South Carolina Law Review

Volume 64 | Issue 2 Article 4

Winter 2012

Against Employer Dumpster-Diving for Email

Michael Z. Green
Texas Wesleyan University School of Law

AGAINST EMPLOYER DUMPSTER-DIVING FOR EMAIL

Michael Z. Green*

Recent attorney–client-privilege cases offer a modern understanding of reasonable expectations of employee privacy in the digital age. Today, employees are sending an increasing number of electronic mail communications to their attorneys via employer-provided computers or other digital devices with an expectation of privacy and confidentiality. Historically, courts summarily dispensed with these matters by finding that an employer's policy establishing employer ownership of any communications made through employer-provided devices eliminated any employee expectation of privacy in the communications and waived any viable privacy challenges to employer review of those communications. Nevertheless, within the last couple of years, several cases involving employee assertions of attorney–client-privilege protection in emails sent on employer-provided devices suggest new thoughts about reasonable workplace privacy expectations.

As employees must communicate through employer-provided digital devices, day and night, these attorney–client-privilege cases help expose the fallacy of assuming employees cannot reasonably expect that emails will remain private if employers' policies mandate that such communications are not private. These new cases and related ethics opinions about privileged email offer a modern lens through which one may now view employee privacy expectations under a new paradigm that replaces the façade of assuming employees have no expectation of privacy due to employer policies.

Digital-age expectations regarding employee use of "smart" cellular phones, portable laptops, and other employer-provided electronic devices to communicate beyond standard work hours leaves little expectation or reasonable opportunity for employees to communicate privately and confidentially by any other means. As a result, this Article asserts that employer efforts to mine employer-provided devices for employee emails, after disputes arise, comprises a form of electronic dumpster-diving that should not be tolerated by courts, legislatures, or attorney ethics committees.

---

*Professor of Law, Texas Wesleyan University School of Law. I thank Robin Barnes, Huyen Pham, and Paul Secunda for their thoughtful suggestions regarding a prior draft of this Article. I value the many comments I have received from several workshop participants who assessed my thoughts discussed herein at the Fifth Annual Labor and Employment Law Colloquium on September 24, 2010 at Washington University College of Law, the Second Annual John Mercer Langston Workshop held on June 25, 2011 at DePaul College of Law, and the Discussion Group on Privacy at the 64th Annual Southeastern Association of Law Schools (SEALS) Annual meeting on August 2, 2012. I also thank Brad Snyder for reading and commenting on an earlier draft of this Article at the University of Wisconsin Law School's Hastie Reunion Workshop held on April 15, 2011. Margaret Green has inspired me in all that I write and I remain eternally grateful. The support from Patricia Jefferson renews me on a daily basis. I appreciate the financial support provided by the Texas Wesleyan University School of Law, and the student research assistance from Rachel Hale, Amy Herrera, Keena Hilliard, Robyn Trosper-Murrell, Stephanie Rodriguez, Anne Sontag, and Kristen vanBolden.

I. INTRODUCTION: INCREASING MERGER OF PERSONAL AND WORK-RELATED COMMUNICATIONS WITH ATTORNEY–CLIENT PRIVILEGE

Imagine the following scenario:

> Bobbi works for Acme as Vice President for Sales and reports to the President, Henry. Despite her extensive travel schedule, Acme expects Bobbi to remain in contact with her staff, as well as with Henry, on a daily basis, including outside normal work hours, as needed. Bobbi has filed a complaint of sexual harassment against Henry, which will be heard in arbitration. Bobbi communicated with her attorney via emails sent through her employer-provided smart phone, and the emails were downloaded to her company laptop computer. A computer forensics

> expert from Acme searched the laptop computer while Bobbi was at a meeting and found several emails from Bobbi to her attorney. Acme's computer use policy states that all communications found on employer-provided equipment are the property of Acme and Acme may inspect the equipment and communications made on it at any time. Acme's attorneys want to use the emails in the arbitration against Bobbi because they are the property of Acme when found on Acme's computer. However, Bobbi's attorney asserts the emails contain protected, confidential, and attorney–client-privileged communications.[1]

This scenario illustrates the difficult issues that have arisen as technological advances create more opportunities and necessities to merge personal and work-related electronic communications.[2] Whether Bobbi may successfully assert that the emails found on her employer-provided computer are privileged depends on the reasonableness of her belief that the communications were private and confidential. Ultimately, this issue will be decided by comparing the steps Bobbi and her attorney took to keep the communications confidential with whatever steps her employer took to inform her that Acme agents would be accessing and viewing information on the computer.[3]

---

1. Portions of this scenario were derived from the facts presented for a petition for review to the Supreme Court of California. Petition for Review at 2–3, Shanahan v. Superior Court, No. S185493, 2010 WL 3799960 (Cal. Aug. 31, 2010). For a broad discussion of many privacy issues generated by the expansion of technology, see JON L. MILLS, PRIVACY: THE LOST RIGHT (2008); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY (2011); CHARLES J. SYKES, THE END OF PRIVACY (1999). Given the growth of technology, concerns related to the attorney–client privilege have also expanded. *See generally* Anne Klinefelter, *When to Research Is to Reveal: The Growing Threat to Attorney and Client Confidentiality from Online Tracking*, 16 VA. J.L. & TECH. 1, 22–30 (2011) (discussing the expansion of online legal research with respect to attorney–client privilege).

2. *See* William A. Herbert, *The Electronic Workplace: To Live Outside the Law You Must Be Honest*, 12 EMP. RTS. & EMP. POL'Y J. 49, 50 (2008) (describing the merger of personal and work-related electronic communications); *see also* Marian K. Riedy et al., *Managing Business Smartphone Data*, J. INTERNET L., Mar. 2011, at 3, 9 (describing the increasing use of smart phones by employees for both personal and business use and suggesting that employees who use their personal smart phones for business use may have some privacy protection in personal emails used on those phones).

3. In August 2011, the American Bar Association (ABA), in an effort to address the concern that employees may realistically expect to communicate with their attorneys via email and whether those email communications may represent a loss of the attorney–client privilege, issued two ethics opinions. *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011) [hereinafter ABA Opinion 11-459] (discussing a lawyer's duty to protect the confidentiality of email communications with clients); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-460 (2011) [hereinafter ABA Opinion 11-460] (discussing a lawyer's duty when receiving a third party's email communication with counsel). Both opinions establish an attorney's duty to protect the attorney–client privilege by making sure those employees keep email communications confidential and not use employer-provided devices to make those email communications. These ethics opinions seem pragmatic in responding to a potential loss of privilege under various state laws by placing more burdens on attorneys to recognize the risk of email communications from

This Article asserts that the growth of mobile technology in the workplace and the increasing expectation that employees be available electronically supports the position that employees reasonably expect their personal communications—those that are not work-related—will remain private, even if those communications are made and stored on employer-provided electronic devices. Employees would not repeatedly communicate with their attorneys through employer-provided devices if those employees did not reasonably expect that those communications would remain private and confidential. After being forced to spend so much of their time and energy working and communicating through employer-provided digital devices, it is only reasonable to expect that employees will make both personal and private communications through those devices.

The expansion of electronically stored information (ESI) in the digital age has created key issues and demands for employers and employees in investigating and resolving workplace disputes.[4] A 2011 Aberdeen Group study of 415 companies found that 75% of those companies allowed their employees to use personal devices to perform work-related activities.[5] Whether it is reasonable to expect privacy in information that has been disclosed or made available to an employer represents a more difficult question in the digital age. Because of the pervasiveness and ease of sending electronic information, questions about whether members of society have given up privacy rights as an "inevitable" compromise to the expediency of electronic communication have posed knotty dilemmas for the courts.[6] Ultimately, legislative action may have

---

clients. On the other hand, these ethics opinions also highlight how employees expect that email communications made to their attorneys on employer-provided devices will remain private. *See* ABA Opinion 11-459, *supra*; ABA Opinion 11-460, *supra*.

4. *See* James K. Robertson Jr. & Charles F. Corcoran III, *The Discovery of Electronically Stored Information in Arbitration Proceedings*, *in* E-DISCOVERY IN ARBITRATION: LEADING LAWYERS ON RECOVERING ELECTRONIC EVIDENCE, MEETING NEW DISCLOSURE GUIDELINES, AND IMPLEMENTING MEASURES TO STREAMLINE THE PROCESS 7, 8 (2010) ("In 2009, computers [were] the primary medium for the development, maintenance, and communication of information . . . . The vast majority of all business records [were] generated and stored electronically, most never appearing in hard copy."); *see also* Rodney A. Satterwhite & Matthew J. Quatrara, *Asymmetrical Warfare: The Cost of Electronic Discovery in Employment Litigation*, 14 RICH. J.L. & TECH. 9, at 3 (2008), http://law.richmond.edu/jolt/v14i3/article9.pdf (highlighting the difficulties for employers who have "significantly larger volumes of ESI in their possession that may be relevant to the litigation" including "electronic mail messages regarding the employee [which] are more likely to be kept on the employer's server").

5. *See* Dave Zielinski, *Bring Your Own Device: More Employers Are Allowing Employees to Use Their Own Technology in the Workplace*, HR MAG., Feb. 2012, at 71 (citing *Enterprise-Grade BYOD Strategies: Flexible, Compliant, Secure*, ABERDEEN GROUP 1, 1 (Sept. 2011) [hereinafter *Enterprise-Grade*], http://fm.sap.com/data/UPLOAD/files/Enterprise_Grade_BYOD_Strategies__2012.4.11-18.52.49.pdf) (describing the increasing number of employers who are allowing employees to use their own mobile, digital devices to perform work duties).

6. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring in judgment) ("New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not

to address the impact of digital devices on privacy rights.[7] Until any responsible legislative action occurs, this Article asserts that courts should recognize that employees do reasonably expect privacy in email communications, especially those made to their attorneys. This expectation of privacy does not change even if the employer has provided the digital device used or the employer clearly has access to review the communications on that device.

Attorney–client-privilege law offers a modern lens through which one can analyze employee expectations in digital communications.[8] When an attorney becomes involved in the investigation of a legal matter, ethical rules guide the attorney's conduct in deciding whether to use inadvertently discovered electronic communications.[9] If an employee chooses to communicate with the employee's lawyer through a work computer, the question arises as to whether that communication remains protected by the attorney–client privilege or whether the privilege has been waived because the employee used a device the employer can access to review those communications.[10] When an attorney receives an

---

welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.").

7. *Id.* at 962–63 ("Concern about the new intrusions on privacy may spur the enactment of legislation to protect against these intrusions" similar to what occurred "with respect to wiretapping," a subject to which "Congress did not leave it to the courts" but "promptly enacted a comprehensive statute.").

8. *See generally* Louise L. Hill, *Gone but Not Forgotten: When Privacy, Policy and Privilege Collide*, 9 NW. J. TECH. & INTELL. PROP. 565, 572–81 (2011) (describing attorney–client issues related to workplace expectations of privacy in email communications from employees to attorneys). *But see* Edward J. Imwinkelried, *The Dangerous Trend Blurring the Distinction Between a Reasonable Expectation of Confidentiality in Privilege Law and a Reasonable Expectation of Privacy in Fourth Amendment Jurisprudence*, 57 LOY. L. REV. 1, 22–28 (2011) (asserting that key distinctions exist between confidentiality expectations under privilege law and expectations of privacy under the Fourth Amendment—the analysis for one area of expectations should not be confused with the other).

9. *See* Louise L. Hill, *Emerging Technology and Client Confidentiality: How Changing Technology Brings Ethical Dilemmas*, 16 B.U. J. SCI. & TECH. L. 1, 21–45 (2010); Robert J.A. Zito, *Stop! The Lawyer's Ethical Duty on Discovery of Inadvertently Disclosed Confidential Information*, N.Y. L.J., May 12, 2008, at S6–S7, S10; *see also* John D. Comerford, Note, *Competent Computing: A Lawyer's Ethical Duty to Safeguard the Confidentiality and Integrity of Client Information Stored on Computers and Computer Networks*, 19 GEO. J. LEGAL ETHICS 629, 630 (2006) (citing Ariz. State Bar Ass'n, Comm. on the Rules of Prof'l Conduct, Formal Op. 05-04 (2005)) (arguing that the Arizona Opinion "offers a solid framework for lawyers and law firms seeking advice regarding their ethical responsibilities in this area").

10. *See* Hill, *supra* note 8, at 565 (finding that "jurisdictions are divided about whether employees give up the protection of attorney-client privilege when they use a company-issued computer to send or receive e-mails"); *see also* Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 438–43 (N.Y. Sup. Ct. 2007) (finding an employee's emails to an attorney were not privileged communications when sent from employer-owned computers where the corporation banned personal use of employer provided devices, the company monitored the use of the employee's computer and email, and the employee was aware of the use and monitoring policies of the company). *But see* Stengart v. Loving Care Agency, Inc., 973 A.2d 390, 402 (N.J. Super. Ct. App. Div. 2009) (finding that an employee's communications to her attorney on her personal email account were protected by the attorney–client privilege even though they were made using the

inadvertent disclosure of information and can clearly see that it was not intended to be disclosed because it represents a confidential communication between an opposing party and an attorney, the receiving attorney may have different obligations depending upon the ethical rules in that jurisdiction.[11] The receiving attorney could certainly ask a court to rule that any attorney–client privilege has been waived under the circumstances.

Neither the law nor ethical rules clearly discourage diving into dumpsters[12] to retrieve confidential communications between an opposing party and that party's attorney.[13] If the communications could have been easily protected from disclosure before going in the trash, a court may disregard the dumpster-diving retrieval and find the privilege was waived.[14] The American Bar Association

---

employer's computer and with knowledge of the company's computer use policy), *aff'd as modified*, 990 A.2d 650 (N.J. 2010).

11. *See* Paula Schaefer, *The Future of Inadvertent Disclosure: The Lingering Need to Revise Professional Conduct Rules*, 69 MD. L. REV. 195, 206–08 (2010).

12. Dumpster-diving, as that term is used in this Article, refers to attempts to obtain private and confidential information clearly not intended to be viewed by others. The term encompasses physically searching trash receptacles as well as electronically searching email files that may be accessible for some reason other than for the purpose of being searched—like being stored on a company-owned computer or server or being accessed through a company-owned computer or server. *See* Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 316–17 (2011) ("'Dumpster diving'" is "a rather drastic form of employee monitoring" where "employers physically search through employees' trash and recycled materials, looking for information" that employees have not shredded or destroyed.); Jason Fitterer, Comment, *Putting a Lid on Online Dumpster-Diving: Why the Fair and Accurate Credit Transactions Act Should Be Amended to Include E-mail Receipts*, 9 NW. J. TECH. & INTELL. PROP. 591, 597 (2011) ("Today's [d]umpster is the Internet, and the amount of personal information that litters the information superhighway is incredible." (quoting Drew Voros, *Your Online Privacy Slips Through Web's Cracks*, OAKLAND TRIB., Oct. 19, 2010, *available at* NewsBank, Rec. No. 16378229) (internal quotation marks omitted)).

13. *See* Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 255–56, 260–61 (N.D. Ill. 1981) (finding that a party, who searched the trash dumpsters of a competitor for evidence of price discrimination and found several drafts of letters intended by the competitor to be confidential communications to attorneys, could use those communications because any privilege was waived by not taking simple precautions to protect the confidentiality of the communications when placing them in the trash dumpster); *see also* Harry Wingo, Comment, *Dumpster Diving and the Ethical Blindspot of Trade Secret Law*, 16 YALE L. & POL'Y REV. 195, 213–15 (1997) (arguing that industrial espionage and dumpster-diving by digging into a competitor's trash receptacles to discover confidential information should represent unethical and "sleazy" behavior even if these activities receive little condemnation in the courts); Sasha Smith, *Spying: How Far Is Too Far? What You Should Know Before Diving in a Dumpster or Cracking a Safe*, FORTUNE SMALL BUS., June 1, 2001, *available at* http://money.cnn.com/magazines/fsb/fsb_archive/2001/06/01/304095/index.htm (referring to the act of dumpster-diving as "unseemly" while noting that the practice is not illegal in most states).

14. *Suburban Sew 'N Sweep*, 91 F.R.D. at 260 ("The likelihood that third parties will have the interest, ingenuity, perseverance and stamina, as well as risk possible criminal and civil sanctions, to search through mounds of garbage in hopes of finding privileged communications, and that they will then be successful, is not sufficiently great to deter open attorney-client communication. . . . [I]f the client or attorney fear such disclosure, [the disclosure] may be prevented by destroying the documents or rendering them unintelligible before placing them in a

(ABA) Model Rules of Professional Conduct (Model Rules) and ABA ethics opinions also do not clearly prohibit an attorney from dumpster-diving for written or electronic communications.[15] Nor do the Model Rules require that an attorney wait to have a court rule that any privilege attached to the communications has been waived before using the communications.[16]

Further, the ethics rules appear more concerned with defining responsibilities when information has been inadvertently disclosed[17] rather than when an employer goes trawling through the garbage or emails of an employee in an attempt to find private and privileged communications.[18] Accordingly, when an employee accesses his own private email service and makes privileged communications, it does not appear to be an inadvertent disclosure when an employer later accesses those communications by examining an employer-provided device.[19] When employers search an employee's computer and find attorney–client privileged or other private communications made by employees,

---

trash dumpster."). *But see* Mendenhall v. Barber-Greene Co., 531 F. Supp. 951, 955 n.8 (N.D. Ill. 1982) (suggesting the question of whether privilege has been waived should focus on the motives of the party whose information was retrieved to determine whether the information was intended to be disclosed—a position contrary to the holding in *Suburban Sew 'N Sweep*).

15. *See, e.g.*, ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 06-442 (2006), *reprinted in* ABA/BNA LAWYERS' MANUAL ON PROFESSIONAL CONDUCT: ETHICS OPINIONS 2006–2010, at 1301:101 (2006) [hereinafter ABA Opinion 06-442] ("The Model Rules of Professional Conduct do not contain any specific prohibition against a lawyer's reviewing and using embedded information in electronic documents, whether received from opposing counsel, an adverse party, or an agent of an adverse party. A lawyer [can readily remove any concerns about this form of dissemination] by 'scrubbing' metadata [(the embedded information)] from documents or by sending a different version of the document without the embedded information."); *see also infra* Part IV.E–F (discussing ABA Opinion 11-459 and ABA Opinion 11-460). A majority of states that have adopted ethics opinions regarding the use of metadata have not agreed with the ABA and, instead, have found that an employer's attorney may not look at the metadata. *See Metadata Ethics Opinions Around the U.S.*, AM. BAR ASS'N, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/resources/charts_fyis/metadatachart.html (last visited Oct. 21, 2012) (tracking jurisdictions that have issued ethics opinions regarding the use of metadata similar to ABA Opinion 06-442 and finding seventeen jurisdictions with decisions—nine jurisdictions have found it unethical for the attorney to mine the metadata and use it (Alabama, Arizona, Florida, Maine, New Hampshire, New York, North Carolina, Washington, D.C., and West Virginia), six jurisdictions have agreed that attorneys may mine and use the metadata (Colorado, Maryland, Oregon, Vermont, Washington, and Wisconsin), and two jurisdictions have refused to establish a bright line rule (Minnesota and Pennsylvania)). *But see* Michael B. de Leeuw & Eric A. Hirsch, *Time to Revisit the Ethics of Metadata*, N.Y. L.J., Mar. 19, 2012, at S10 (quoting ROY D. SIMON, SIMON'S NEW YORK RULES OF PROFESSIONAL CONDUCT ANNOTATED 220 (2012)) (asserting that New York lawyers are disadvantaged by the New York rule not being consistent with the ABA Model Rules and contending that New York should adopt the ABA's approach to the use of document metadata).

16. *See* MODEL RULES OF PROF'L CONDUCT R. 4.4(b) & cmt. 2 (2011).

17. *See id.*

18. *Id.* ("[T]his Rule does not address the legal duties of a lawyer who receives a document that the lawyer knows or reasonably should know may have been wrongfully obtained . . . .").

19. *See* ABA Opinion 11-460, *supra* note 3, at 3 (citing MODEL RULES OF PROF'L CONDUCT R. 1.6 (2011)).

the law should apply the understanding that employees still expect that these communications, whether to their attorneys or others, will not be divulged. This approach faces the realities of the modern, digital workplace by recognizing that these communications are private and intended to be kept confidential, even if it is possible for an employer's forensics expert to later retrieve the information.[20]

Although employees may know, or should know, that people can easily listen to their cell phone conversations or hack into their computers to retrieve private communications that go over wireless networks, employees still expect that those communications will remain private and protected when made to their attorneys or to others. To some extent, ethical opinions describing the scope of the attorney–client privilege initially agreed with that privacy expectation.[21] Even if employers extract information embedded in digital devices provided to their employees and find communications to attorneys, that extraction and its potential use does not change the employees' intent or expectation that those communications will be kept private and confidential. With this understanding, the analysis can focus on whether there was a reasonable basis for the intrusion, instead of encouraging a form of electronic dumpster-diving.

In Part II, this Article examines the current workplace use of digital communication devices, how those devices have blurred the distinction between work-related and private communications, and what employees reasonably expect regarding the privacy of their non-work-related communications. Part III examines the current status of workplace privacy protections for employees when they use employer-provided equipment, given the current expansion of technological advances. Part IV explores the analysis that has developed regarding attorney–client privilege when employers discover employee communications with attorneys on employer-provided mobile devices.

Part V of this Article asserts that ongoing issues regarding attorney–client privilege provide an overall framework for the courts, legislatures, and attorney ethics committees to accept a new paradigm where it should be assumed that employees have a reasonable expectation of privacy in their personal and private communications found on employer-provided equipment. This new paradigm shifts the focus of workplace privacy claims away from whether the employee had an expectation of privacy and moves toward answering the more important

---

20. One might consider it unusual for employers to hire computer forensics experts to look through employee communications on employer-provided devices as part of litigation, but the number of cases involving these actions appears to be increasing. *See* Hill, *supra* note 8, at 578–79 (citing Curto v. Med. World Commc'ns, Inc., 99 FEP Cases 298 (E.D.N.Y. 2006); Kaufman v. SunGard Inv. Sys., No. 05-CV-1236(JLL), 2006 WL 1307882 (D.N.J. May 10, 2006); Banks v. Mario Indus. of Va., Inc., 650 S.E.2d 687 (Va. 2007)) (describing three separate cases where employers, in preparing for litigation, hired a computer forensics expert to restore emails and portions of files created by a former employee).

21. ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413 (1999), *reprinted in* ABA/BNA LAWYERS' MANUAL ON PROFESSIONAL CONDUCT: ETHICS OPINIONS 1996–2000, at 1101:181 (1999) [hereinafter ABA Opinion 99-413] ("[L]awyers have a reasonable expectation of privacy when communicating by e-mail maintained by an [online service provider].").

question of whether the employer's intrusion upon that private information was reasonable. Part VI concludes that courts, legislatures, and attorney ethics committees must presume that employees can have expectations of privacy in certain communications made on employer-provided devices and that employer policies on the use of such devices only help explain the reasonableness of any intrusion upon employee privacy. This result reflects the existing realities in worker electronic privacy cases in that it emphasizes whether it was necessary and reasonable for the employer to access and use the private information in a particular case, rather than assuming an employee had no expectation of privacy or consented to waive that expectation of privacy because of an employer's policy.

II. EMPLOYEE PRIVACY REALITIES IN THE DIGITAL AGE WORKPLACE

> *More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.*
>
> —Justice Sonia Sotomayor, United States Supreme Court[22]

Technological advancements have long created concerns for employees and their lack of privacy protections.[23] However, recent technological advances in electronic communication devices have also led to the "decentralization of the workplace, with some employees integrating their personal computer equipment with their employer's equipment."[24] Because of this integration of information and decentralization of the workplace, resulting from the use of mobile digital communication devices, employers can maximize the efficient use of their employees without the restriction of work hours or work location.[25]

---

22. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citations omitted).

23. *See generally* Rod Dixon, *With Nowhere to Hide: Workers Are Scrambling for Privacy in the Digital Age*, 4 J. TECH. L. & POL'Y 1, para. 9–10 (1999), http://jtlp.org/vol4/issue1/dixon.html (providing excellent detail and analysis of the "growing presence of surveillance technology" and the lack of protection for employees' privacy); *see also* David Beckman & David Hirsch, *Security or Snooping? Monitoring Staff E-mail Is Easy Now, but Privacy May Suffer*, 87 A.B.A. J. 72, 72–73 (2001) (recognizing the need for employer monitoring but suggesting a balance so that employee privacy is still protected).

24. Herbert, *supra* note 2, at 50; *see also* Zielinski, *supra* note 5, at 71 (citing *Enterprise-Grade*, *supra* note 5) (supporting the proposition that many companies have begun to allow employees to use their personal equipment in the workplace).

25. Herbert, *supra* note 2, at 50; *see also* Riedy et al., *supra* note 2, at 3 (providing examples that show how employers can maximize employee productivity without restricting work hours or work location); Zielinski, *supra* note 5, at 71 (stating that offering choices in work technology can "[b]oost productivity and satisfaction levels of most employee generations").

Nevertheless, the merger of work and personal digital communication devices has not shifted employees' reasonable expectations that their personal communications will remain private.[26]

Despite employees' expectation of privacy, the nature of electronic monitoring of employees has become pervasive. A 2001 American Management Association (AMA) study found that 77.7% of employers technologically monitor their employees' emails, phone calls, and computer files.[27] Similarly, a 2007 AMA study found that "66% of employers monitor Internet connections," 12% of employers monitor blogs, "10% monitor social networking sites," and 8% use global positioning systems (GPS) to monitor company vehicles.[28] Another study indicates that "of those employees 'who regularly use e-mail or Internet access at work,' fourteen million 'are under continuous surveillance.'"[29] Moreover, yet another commentator, referring to a 2005 AMA study, noted that 76% of employers are monitoring their employees' web activity.[30]

The Internet has played a major role in how we all view issues pertaining to electronic communication, including the expectation of privacy.[31] With the

---

26. Herbert, *supra* note 2, at 51 (citing Elaine Ki Jin Kim, Comment, *The New Electronic Discovery Rules: A Place for Employee Privacy?*, 115 YALE L.J. 1481, 1485 (2006)); *see also* Dionne Searcey, *Some Courts Raise Bar on Reading Employee Email*, WALL ST. J., Nov. 19, 2009, at A17 ("Employees often assume their communications on personal email accounts should stay private even if they are using work-issued computers or smart phones."); Matthew J. Schwartz, *CIOs See Smartphones as Data Breach Time Bomb*, INFORMATIONWEEK (Nov. 19, 2010, 12:35 PM), http://www.informationweek.com/hardware/handheld/cios-see-smartphones-as-data-breach-time/228300244 (last visited Oct. 23, 2012) (quoting Graham Titterington, principal analyst for Ovum, for the statement that "[e]mployees will want to use their devices, no matter who owns them, for both their work and personal lives" and because "[i]t is unrealistic to delineate between these uses for employees who are mobile and working out of the office for a large part of their time."). Approximately "70% of employees can currently use corporate-owned computing devices for personal activities." *Id.* (citing Graham Titterington, *Enterprises Cautiously Embrace Mobile Devices*, OVUM STRAIGHT TALK IT, Q4 2011, at 9, *available at* http://ovum.com/wp-content/uploads/2011/10/ST-IT-4Q11.pdf).

27. *See* Ariana R. Levinson, *Industrial Justice: Privacy Protection for the Employed*, 18 CORNELL J.L. & PUB. POL'Y 609, 616 (2009) (quoting Matthew W. Finkin, *Information Technology and Workers' Privacy: The United States Law*, 23 COMP. LAB. L. & POL'Y J. 471, 474 (2002)) (citing AM. MGMT. ASS'N ET AL., ELECTRONIC POLICIES AND PRACTICES: SUMMARY OF KEY FINDINGS 1 (2001), *available at* http://www.epolicyinstitute.com/survey2001Summary.pdf).

28. *Id.* (quoting AM. MGMT. ASS'N & EPOLICY INST., 2007 ELECTRONIC MONITORING & SURVEILLANCE SURVEY: EXECUTIVE SUMMARY (2008), *available at* http://www.epolicyinstitute.com/survey2007Summary.pdf).

29. *Id.* (quoting Finkin, *supra* note 27, at 474) (citing PRIVACY FOUND., THE EXTENT OF SYSTEMATIC MONITORING OF EMPLOYEE E-MAIL AND INTERNET USE 1 (2001), *available at* http://65.98.26.50/internetmonitoring.pdf).

30. Mindy C. Calisti, Note, *You Are Being Watched: The Need for Notice in Employer Electronic Monitoring*, 96 KY. L.J. 649, 650 (2008) (citing AM. MGMT. ASS'N & EPOLICY INST., 2005 ELECTRONIC MONITORING & SURVEILLANCE SURVEY: EXECUTIVE SUMMARY (2005), *available at* http://www.epolicyinstitute.com/survey2005Summary.pdf).

31. *See* Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 611–19 (2011) (focusing on privacy concerns over the Internet but only when viewed by humans, as opposed to being disclosed to automated systems).

expansive growth of the information superhighway, employers and employees have to navigate electronic information issues in the increasingly digital workplace. In particular, with the pervasive use of laptops, personal digital assistants (PDAs), pagers, cellular phones, and other mobile devices, an increasing number of employers are requiring that their employees become electronically connected beyond just a normal nine-to-five work day.[32] Also, communications via mobile electronic devices have spread with the proliferation of "[s]ocial networking [w]eb sites allow[ing] registered users to upload profiles, post comments, join 'networks,' and add 'friends'" which gives "users the opportunity to form 'links' between each other, based on friendships, hobbies, personal interests, and business sector or academic affiliations."[33]

As the increasing mandate to be electronically available places more working demands on employees, this availability requirement also creates concerns about whether employees have any reasonable expectation of privacy in the ESI on mobile devices provided by employers. Furthermore, as the nine-to-five culture of communicating about and performing work matters solely at the office and limiting private and non-work-related communications to places and times outside the workplace erodes under the weight of the broad use of mobile digital devices, any assumptions about an employee's expectation of privacy must also be reevaluated in light of the technological changes.[34] Accordingly, the ability to protect employee expectations of privacy, when dealing with merged work and non-work communications, must address the new realities of the mobile, digital workplace.

III. LEGAL EXPECTATIONS OF PRIVACY IN EMPLOYER-PROVIDED DEVICES

In addressing the new realities of the mobile digital workplace, the current legal limitations on employee privacy protections must be explored. The overall history on how the law has allowed employers to diminish employees' expectations of privacy is quite expansive.[35] Employees have little bargaining

32. *See* Herbert, *supra* note 2, at 50 ("Inherent in this technologically based decentralization is the blurring of the lines between the workplace and home and between work and rest."); Marjorie J. Peerce & Daniel V. Shapiro, *The Increasing Privacy Expectations in Employees' Personal Email*, J. INTERNET L., Feb. 2010, at 1, 1 ("Mobile email devices and remote access have lengthened the working day and further blurred the distinction between business and personal time.").

33. Steven C. Bennett, *Ethics of Lawyer Social Networking*, 73 ALB. L. REV. 113, 115 (2009) (citing Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 845–46 (W.D. Tex. 2007)).

34. *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring in judgment) ("Recent years have seen the emergence of many new devices that permit [tracking]. . . . The availability and use of these and other new devices will continue to shape the average person's expectations about [privacy].").

35. *See, e.g.*, Lisa Smith-Butler, *Workplace Privacy: We'll Be Watching You*, 35 OHIO N.U. L. REV. 53, 60–79 (2009) (describing the nature of employer monitoring of employees and the lack of privacy protections); 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, 111–23

power and are subjected to the employment at will doctrine, which is essentially a default contractual expectation for employees without definite terms of employment that allows employees to be terminated for good reason, bad reason, or no reason at all.[36] Professor Ariana Levinson has asserted that "[s]cholars generally agree that the law in the United States fails to adequately protect . . . employees from technological monitoring by their employers."[37] Furthermore, it is unlikely that employee-friendly legislation will be passed in Congress any time in the near future.[38] Some scholars have argued that more state laws protecting employees' legal off-duty activities might provide some form of protection from privacy intrusions by employers.[39]

(2008) (describing the lack of workplace privacy protections for employees related to email and cell phones).

36. *See* MARK A. ROTHSTEIN ET AL., EMPLOYMENT LAW 139 (4th ed. 2009); *see also* Nicole B. Porter, *The Perfect Compromise: Bridging the Gap Between at-Will Employment and Just Cause*, 87 NEB. L. REV. 62, 66–70 (2008) (describing the expansiveness of the at-will employment doctrine); Michael Selmi, *Privacy for the Working Class: Public Work and Private Lives*, 66 LA. L. REV. 1035, 1036 (2006) (noting that at-will employment relationships make resolving workplace privacy issues difficult). This at-will employment concept is believed to have gained credence in the United States based upon a treatise written by Horace Wood. *See* Mayer G. Freed & Daniel D. Polsby, *The Doubtful Provenance of "Wood's Rule" Revisited*, 22 ARIZ. ST. L.J. 551, 551–55 (1990) (discussing, H.G. WOOD, A TREATISE ON THE LAW OF MASTER AND SERVANT § 134, at 271–74 (1877), and the cases relied on therein to validate the rule of at-will employment in the United States).

37. Ariana R. Levinson, *Carpe Diem: Privacy Protection in Employment Act*, 43 AKRON L. REV. 331, 334 (2010); *see also* Finkin, *supra* note 27, at 503–04 ("The law does not perceive of one's conduct on the job as a 'private' matter."); Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 294–304 (2002) (noting the failure of common law and statutory law in the United States to guarantee and adequately protect electronic privacy in the workplace); S. Elizabeth Wilborn, *Revisiting the Public/Private Distinction: Employee Monitoring in the Workplace*, 32 GA. L. REV. 825, 838 (1998) (describing the "scholarly energy" that has been invested in exposing the lack of legal protection for employee privacy).

38. *See* Kesan, *supra* note 37, at 304–07 (highlighting the difficulties in pursuing legislation to address workplace privacy concerns given the United States' unique definition of privacy); *see also Jones*, 132 S. Ct. at 964 (Alito, J., concurring in judgment) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. . . . To date, however, Congress and most States have not enacted statutes . . . .") (citation omitted); Michael Z. Green, *Reading* Ricci *and* Pyett *to Provide Racial Justice Through Union Arbitration*, 87 IND. L.J. 367, 370 n.12 (2012) (describing initial efforts during President Barack Obama's administration to enact employee-friendly legislation and the unlikely prospects that such legislation will pass any time in the near future).

39. *See, e.g.*, Marisa Anne Pagnattaro, *What Do You Do When You Are Not at Work?: Limiting the Use of Off-Duty Conduct as the Basis for Adverse Employment Decisions*, 6 U. PA. J. LAB. & EMP. L. 625, 680–82 (2004) (arguing that an off-duty conduct protection statute should be enacted to protect employees from employer intrusions); Jean M. Roche, Note, *Why Can't We Be Friends?: Why California Needs a Lifestyle Discrimination Statute to Protect Employees from Employment Actions Based on Their Off-Duty Behavior*, 7 HASTINGS BUS. L.J. 187, 198–204 (2011) (providing examples of states that have adopted statutes to protect privacy related to legal off-duty conduct and urging California to adopt a similar statute); *see also* Monique Garcia, *Quinn Signs Social Network Password Law*, CHI. TRIB., Aug. 2, 2012, § 1, at 5, *available at* http://articles.chicagotribune.com/2012-08-01/news/chi-quinn-signs-socalled-facebook-bill-into-law-20120801_1_

With the growth, in the past few years, of electronic mail and the development of social and professional networking through the Internet, colleges, employers, and litigators are frequently checking individuals' social network pages and blogs to determine if there are items to be discovered.[40] Admittedly, employers face potential liability when attempting to access employee information classified as private.[41] Nevertheless, employers have legitimate reasons to want information about their employees, including the need to address concerns about harassment, theft, protection of trade secrets, and efficient performance of duties.[42] Sometimes employers may need to investigate and review an employee's ESI either as part of the employer's duties to act responsibly under law or as an attempt to protect itself in litigation.[43] Accordingly, courts are struggling with issues relating to the use of electronic communications and how employers have responded.[44]

---

social-media-passwords-pat-quinn-illinois-employers (describing new Illinois legislation that prohibits employers from asking employees for social media passwords to investigate an employee or applicant's online social media profile that is password protected).

40. *See* Karen L. Stevenson, *What's on Your Witness's MySpace Page?*, LITIG. NEWS, March 2008, at 4, 4; *see also* Kathrine Minotti, Note, *The Advent of Digital Diaries: Implications of Social Networking Web Sites for the Legal Profession*, 60 S.C. L. REV. 1057, 1057–61 (2009) (describing how courts are increasingly issuing decisions allowing access to social network site information, emails, and text messages as part of litigation process); Lisa Thomas, Comment, *Social Networking in the Workplace: Are Private Employers Prepared to Comply with Discovery Requests for Posts and Tweets?*, 63 SMU L. REV. 1373, 1395–1401 (2010) (discussing workplace problems that may arise as a result of social networking use).

41. *See* Pietrylo v. Hillstone Rest. Grp., No. 06-5754 (FSH), 2009 WL 3128420, at *2–3 (D.N.J. Sept. 25, 2009) (citing 18 U.S.C. § 2701(c)(2) (2006)) (affirming that the employer violated the Stored Communications Act when it repeatedly accessed a password-protected employee discussion forum on MySpace.com); Nat'l Econ. Research Assocs. v. Evans, No. 04-2618-BLS2, 2006 WL 2440008, at *1–2, *5 (Mass. Super. Ct. Aug. 3, 2006) (denying plaintiffs' motion to compel, preventing employer's access to employee communications, stored as "screen shots," where the employee visited the web site to send emails on a password-protected email site that the employer discovered through the use of a computer forensics expert, and rejecting the employer's argument of waiver because it would be difficult to have a privileged email conversation with an attorney if "a traveling employee" would be forced to bring both a company and a personal computer); Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010) ("[U]nder the circumstances, Stengart could reasonably expect that e-mail communications with her lawyer through her personal account would remain private, and that sending and receiving them via a company laptop did not eliminate the attorney–client privilege that protected them.").

42. Selmi, *supra* note 36, at 1042–43; *see also* Doe v. XYC Corp., 887 A.2d 1156, 1160–67 (N.J. Super. Ct. App. Div. 2005) (discussing a third party lawsuit in which the parties were seeking to establish employer liability because the employer established its right to monitor electronic communications made by employees and one of those employees used the employer's computer to access child pornography and send pictures of one of the plaintiff's children to child pornography web sites). *But see* Blakey v. Continental Airlines, Inc., 751 A.2d 538, 552 (N.J. 2000) (finding that an employer does not have a duty to monitor an employee's private electronic communications).

43. *See* Peerce & Shapiro, *supra* note 32, at 1, 14 (discussing potential liability coincident with the "legal need to review" an employee's material on company computers when involved in "an internal investigation, employment dispute, or civil litigation").

44. *See* Karen L. Stevenson, *Courts Confront Admissibility of Text and Instant Messages*, LITIG. NEWS, Mar. 2008, at 4, 4–5.

The implementation of an Internet or device-usage policy provides an opportunity for employers to defend against workplace privacy claims more directly. Often, pointing to the language of the Internet or device-usage policy serves as validation for the employer's actions and refutes any other related claims.[45] However, employees may look to the law as developed under the Fourth Amendment, common law, and statutory law to understand whatever limited privacy protections may exist when the issue involves communications stored on employer-provided devices.[46]

A. Fourth Amendment Employee Privacy Protections: Ortega *and* Quon

Although a governmental employer's accessing an employee's ESI raises issues of constitutional rights that do not apply directly in the private sector, cases involving public employees may be helpful in understanding workplace matters in the private sector. Specifically, the Court's interpretation of privacy issues involving employees under the Fourth Amendment[47] has implications for other areas of privacy law.[48] The Supreme Court addressed the issue of the

---

45. *See, e.g.*, Najee-Ullah v. N.Y.C. Dep't of Educ., No. 05CV6202(GBD), at *1 n.2, *4 (S.D.N.Y. Mar. 31, 2008) (dismissing plaintiff's claims for violation of the Fair Labor Standards Act and New York Labor Law because the "defendant . . . provided a legitimate non-retaliatory reason for the alleged adverse employment actions"—a violation of the employer's Internet policy); Rizzo v. PPL Serv. Corp., Nos. 03-5779, 03-5780, 03-5781, 2005 WL 913091, at *10, *11 (E.D. Pa. Apr. 19, 2005) (rejecting claims based on age discrimination while noting that the company's dismissal was founded on violations of email policy rather than discrimination).

46. Privacy law consists of much more than tort law. *See* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1434 (providing support for the claim that privacy law cannot be easily defined because it consists of five "species" or interrelated areas: (1) torts; (2) the Fourth Amendment; (3) the First Amendment; (4) the Fourteenth Amendment; and (5) state constitutional law). Further, there are state and federal statutes that address privacy implications as well. *See, e.g.*, Stored Communications Act, 18 U.S.C. §§ 2701–2711 (2006) (providing privacy for electronically stored information); Roche, *supra* note 39, at 198–202 (providing examples of states that have adopted statutes to protect privacy in legal off-duty activity, termed "lifestyle discrimination"); Garcia, *supra* note 39, at 5 (describing recent Illinois legislation dealing with privacy law protection from employer efforts to obtain social network passwords).

47. *See generally* Dieter C. Dammeier, *Fading Privacy Rights of Public Employees*, 6 HARV. L. & POL'Y REV. 297, 297 (2012) (describing the erosion of privacy rights of public sector employees under the Fourth Amendment); Paul M. Secunda, *Privatizing Workplace Privacy*, 88 NOTRE DAME L. REV. (forthcoming 2012) (describing Fourth Amendment privacy concerns and proposing stronger public sector employee protection from Fourth Amendment privacy intrusions by employers by requiring probable cause to obtain a warrant before conducting any form of investigatory workplace search).

48. *See* Marc Jonathan Blitz, Stanley *in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like that of the Fourth*, 62 HASTINGS L.J. 357, 373 (2010) (citing City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010)) (admiring the Court's analysis of Fourth Amendment privacy concerns in *Quon* as encompassing a broad acknowledgement of an employee's right to privacy in their own cell phones and Internet accounts and suggesting expansion of that doctrine to First Amendment jurisprudence).

Fourth Amendment's privacy protection for public employees in its 1987 decision, *O'Connor v. Ortega*.[49]

In *Ortega*, a plurality composed of Justices O'Connor, White, Powell, and Chief Justice Rehnquist found that a two-step inquiry applied to determine whether a public employee had a Fourth Amendment protection based upon a reasonable expectation of privacy in items stored in his workplace desk: (1) a court must consider the "operational realities of the workplace" to assess whether the employee had a legitimate expectation of privacy in his workplace items; and (2) if the employee had a legitimate expectation of privacy in his workplace items, then the focus shifts to whether the "public employer intrusions on the constitutionally protected privacy interests of government employees for noninvestigatory, work-related purposes, as well as for investigations of work-related misconduct," were "reasonable[] under all the circumstances."[50] On the other hand, in an opinion concurring in the judgment, Justice Scalia rejected the operational realities component of the plurality decision and argued that, as a general principle, public employees have an expectation of privacy in their employer-provided desks; however, "government searches [of those desks] to retrieve work-related materials or to investigate violations of workplace rules" are reasonable intrusions that "do not violate the Fourth Amendment."[51]

More recently, the issue of privacy expectations in the workplace—under the Fourth Amendment—arose in *City of Ontario v. Quon*.[52] In *Quon*, a police officer's employer-provided pager was searched to review text messages.[53] The City of Ontario, California Police Department (OPD) issued pagers to its police officers to improve communications and provide more efficient responses by the police force.[54] The service provider for the pagers was Arch Wireless Operating Company, who, for a set monthly fee, provided a limited number of text characters that could be sent and received each month on each pager.[55] Messages in excess of the character limit would result in additional charges to be paid by the officers to prevent the OPD from having to audit the texts each month to determine if the overage was due to personal text messages.[56] When the OPD first issued the pagers to the police force, the officers were told that text messages on the pagers would be treated like emails and were therefore subject to the OPD's "Computer Usage, Internet and E-mail Policy" (Computer Use Policy).[57] The Computer Use Policy stated that the OPD "reserves the right to monitor and log all network activity including e-mail and Internet use, with or

49. 480 U.S. 709 (1987).
50. *Id.* at 711–12, 717, 725–26.
51. *Id.* at 730, 732 (Scalia, J., concurring in judgment).
52. 130 S. Ct. 2619 (2010).
53. *Id.* at 2624.
54. *Id.* at 2625.
55. *Id.*
56. *Id.*
57. *Id.*

without notice," and that "[u]sers should have no expectation of privacy or confidentiality when using these resources."[58]

Shortly after the pagers were issued, Quon began to regularly acquire overage charges for which he paid the OPD.[59] After some time, the lieutenant in charge of the OPD's contract with Arch Wireless told his Chief that he was "tired of being a bill collector" for the overages.[60] As a result, the Chief decided that the OPD should determine if the character limit on the text messages was too low for the police officers or if the excessive charges were due to personal messages.[61] The OPD requested two months of text transcripts from Arch Wireless, which indicated that "many of the messages sent and received on Quon's pager were not work-related, and some were sexually explicit."[62] The matter was handed over to OPD's internal affairs department, and the officer in charge of the internal review first pulled out all of the messages that were sent from Quon's pager during his non-working hours so the review could focus on only those messages sent or received while Quon was working.[63] The investigator determined that during one month of transcripts only fifty-seven of the 456 messages sent and received were work-related.[64] As a result, Quon was disciplined.[65]

Quon challenged the OPD's disciplinary action in federal court and argued, among other things, that the OPD violated Quon's rights under the Fourth Amendment by searching through his messages on his employer-provided pager.[66] The United States District Court for the Central District of California determined that the OPD's audit of Quon's text messages was reasonable.[67] However, the United States Court of Appeals for the Ninth Circuit reversed in part, agreeing with the district court that Quon had a reasonable expectation of privacy in his text messages but determining that the search, though legitimately work-related, was unreasonable in scope.[68] The court of appeals determined that the OPD could have found a less intrusive way to meet the business needs of the department.[69]

---

58. *Id.* (quoting Appendix to Petition for Writ of Certiorari at 152a, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332), 2009 WL 1155423, at *4).

59. *Id.* at 2625–26.

60. *Id.* at 2626 (quoting Joint Appendix at 91, City of Ontario v. Quon, 130 S. Ct. 2619 (2010) (No. 08-1332), 2010 WL 546073, at *91).

61. *Id.*

62. *Id.*

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

67. *Id.* at 2626–27 (citing Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116, 1146 (C.D. Cal. 2006), *aff'd in part, rev'd in part*, 529 F.3d 892 (9th Cir. 2008), *rev'd and remanded sub nom.*, City of Ontario v. Quon, 130 S. Ct. 2619 (2010)).

68. *Id.* at 2627 (citing *Quon*, 529 F.3d at 908).

69. *Id.* (citing *Quon*, 529 F.3d at 909).

While resolving the privacy issues on other grounds,[70] the Supreme Court in *Quon* expressed concern about delineating the scope of privacy expectations in digital devices provided by employers:

> Before turning to the reasonableness of the search, it is instructive to note the parties' disagreement over whether Quon had a reasonable expectation of privacy. The record does establish that OPD, at the outset, made it clear that pager messages were not considered private. The City's Computer [Use] Policy stated that "[u]sers should have no expectation of privacy or confidentiality when using" City computers. . . . The Court must proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer. The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear. . . . It is not so clear that courts at present are on so sure a ground. Prudence counsels caution before the facts in the instant case are used to establish far-reaching premises that define the existence, and extent, of privacy expectations enjoyed by employees when using employer-provided communication devices.[71]

Despite Justice Scalia's objections, the Court in *Quon* did offer some powerful statements about an employee's reasonable expectation of privacy in employer-provided equipment when Justice Kennedy, in dicta, noted:

> Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior. As one *amici* brief notes, many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency. Another *amicus* points out that the law is beginning to respond to these developments, as some States have recently passed statutes requiring employers to notify employees when monitoring their electronic communications. At present, it is uncertain how workplace norms, and the law's treatment of them, will evolve. . . . Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-

---

70. *See id.* at 2629–33 (deciding that, even if Quon had a reasonable expectation of privacy, the search was reasonable because it was not excessive in scope and was motivated by a legitimate work-related purpose).

71. *Id.* at 2629 (second alteration in original) (quoting Appendix to Petition for Writ of Certiorari, *supra* note 58, at 152a, 2009 WL 1155423, at *4).

> expression, even self-identification. That might strengthen the case for an expectation of privacy.[72]

Accordingly, Justice Kennedy's comments in *Quon* provide a key framework to make the case that employees do have reasonable expectations of privacy in employer-provided devices.

However, Justice Kennedy also acknowledged the dilemma the Court faced in *Quon* when he suggested that employees may have legitimate alternatives to make their communications without using employer-provided devices and that employer policies do play some role in the reasonableness of an employee's expectations:

> On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated. A broad holding concerning employees' privacy expectations vis-à-vis employer-provided technological equipment might have implications for future cases that cannot be predicted. It is preferable to dispose of this case on narrower grounds.[73]

In evading the expectation of privacy question and moving to the reasonableness of the employer's intrusions, the Court in *Quon* decided that the scope of the OPD's search was appropriate because it was an efficient way to determine if the overages were due to work-related messages.[74] The scope was reasonable in that the OPD looked only at two months of text messages—and eliminated all messages sent during Quon's off-duty time—rather than searching the entire period the pagers were in use.[75] Furthermore, Quon was told that the pagers were subject to auditing, and as a member of the police force, he should have suspected the OPD might have an occasional operational need to look at the text messages in an emergency situation.[76] The Court clarified that, just because

---

72. *Id.* at 2629–30 (citations omitted).

73. *Id.* at 2630. Justice Scalia, in his concurring opinion, criticized the Court's "[t]he-times-they-are-a-changin'" refusal to address the expectation-of-privacy analysis as being a "feeble excuse for disregard of duty." *Id.* at 2635 (Scalia, J., concurring in part and concurring in judgment). Even more, Justice Scalia expressed his indignation about the Court's assertion that it was "agnostic" about the expectation-of-privacy analysis while at the same time offering "a heavy-handed hint," which will result in "bombarding lower courts with arguments about employer policies, how they were communicated, and whether they were authorized, as well as the latest trends in employees' use of electronic media." *Id.*

74. *Id.* at 2631 (majority opinion).

75. *Id.*

76. *Id.*

"OPD could have performed [a] search that would have been less intrusive, it does not follow that the search as conducted was unreasonable."[77]

Although the OPD had a Computer Use Policy in place providing that "[u]sers should have no expectation of privacy or confidentiality when using" the Internet or sending emails on OPD-owned computers and prohibiting "inappropriate, derogatory, obscene, suggestive, defamatory, or harassing language in the e-mail system,"[78] the policy made no explicit reference to pagers.[79] Nevertheless, most employers believe they can safely institute such policies, impose them on employees as a condition of employment, and protect themselves from privacy challenges by asserting that the policies remove or lower any expectation of privacy.[80] These policies also operate as a form of consent to search the employer-provided electronic equipment by getting the employee to agree ahead of time that the employer owns the equipment and any information on it.[81] The argument is that "[c]onsent negates liability provided that the invasion does not exceed the scope of the consent."[82] In contrast,

---

77. *Id.* at 2632.

78. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 896 (9th Cir. 2008), *rev'd and remanded sub nom.*, City of Ontario v. Quon, 130 S. Ct. 2619 (2010)).

79. *Quon*, 130 S. Ct. at 2625.

80. *See* Steven C. Bennett, *Civil Discovery of Social Networking Information*, 39 SW. U. L. REV. 413, 424 (2010); Amanda J. Lavis, Note, *Employers Cannot Get the Message: Text Messaging and Employee Privacy*, 54 VILL. L. REV. 513, 533 (2009) (suggesting a general understanding that an employee has no expectation of privacy if the employer's policy explicitly states that the information is owned by the employer and is not for personal use); *see also* Herbert, *supra* note 2, at 67–70 (describing cases where employers' Internet policies have been found to establish that the employee did not have a reasonable expectation of privacy); Cicero H. Brabham, Jr., Note, *Curiouser and Curiouser: Are Employers the Modern Day Alice in Wonderland? Closing the Ambiguity in Federal Privacy Law as Employers Cyber-Snoop Beyond the Workplace*, 62 RUTGERS L. REV. 993, 1015 n.172 (2010) (describing jurisdictions that have held that employees have no reasonable expectation of privacy in their work computers); 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, 343 (2004) (asserting that an employee's knowledge of the employer's ability to capture and store email may warrant consent and authorization to look at the emails while removing concerns about privacy).

81. *See* Brabham, *supra* note 80, at 995, 996–1014 (describing how courts have implied consent to intrusions and searches from employee knowledge that employers can monitor the information and analyzing whether "the current, broad interpretation of 'consent,' which enables employers to monitor internal electronic communications under the Wiretap Act, should equally apply to 'authorization' in cases involving external electronic storage brought under the Storage Act"); *see also* Bennett, *supra* note 80, at 424 n.67 (collecting cases finding employee had no reasonable expectation of privacy). *But see* Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 561 (S.D.N.Y. 2008) (finding employer's policy failed to establish consent even where the employee's login information to a private email account was stored on the employer's computer).

82. Andrew F. Caplan & Robert J. Donovan, *The Ethical Investigation of Fidelity Claims: Protecting Privacy*, 10 FIDELITY L.J. 63, 83–84 (2004) (citing Tracy B. Holton, *Cause of Action to Recover Damages for Invasion of Private Sector Employee's Privacy*, 18 CAUSES OF ACTION 2d 87 § 3–6 (2003), *superseded by article*, Richard E. Kaye, *Cause of Action to Recover Damages for Invasion of Private Sector Employees' Privacy by Intrusion upon Seclusion*, 42 CAUSES OF ACTION

Europe's data protection scheme does "not condition protection on an expectation of privacy" and protects even data that is publicly available.[83] This Article asserts that the Court should eventually find that employees, whether public employees covered by the Fourth Amendment or private employees covered by federal, local, and common law privacy protections, do have a reasonable expectation of privacy in electronic information stored on employer-provided mobile devices and that the expectation cannot be waived through employer policies imposed as a condition of employment.[84]

B. Tort-Based Employee Privacy Expectations

Employees in the private sector often look to the "Intrusion Upon Seclusion" section of the Restatement (Second) of Torts[85] as a remedy against employer invasion of privacy.[86] This privacy tort developed from the common law.[87] However, the concept of privacy rights probably originated in Judge Thomas Cooley's 1880 treatise expressing the power of the "right to be let alone."[88]

2d 255 § 6 (2009)); *see also* Wal-Mart Stores, Inc. v. Lee, 74 S.W.3d 634, 648–49 (Ark. 2002) (asserting that signed consent to search was coercive and achieved through duress which made it reasonable for a jury to consider the consent invalid when looking at the employer's invasion of the employee's privacy).

83. *See* Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 1025 (2011).

84. *But see* Leading Cases, 124 HARV. L. REV. 179, 179–80 (2010) (asserting that "[t]he Court [in *Quon*] should have ruled that public employees do not enjoy a reasonable expectation of privacy when sending text messages from government-issued devices").

85. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

86. *See* Leonard Court & Courtney Warmington, *The Workplace Privacy Myth: Why Electronic Monitoring Is Here to Stay*, 29 OKLA. CITY U. L. REV. 15, 33 (2004).

87. Many have traced the development of this legal protection from invasion of privacy to the landmark article, Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Dean William Prosser agreed that the Warren and Brandeis article played a significant role in the development of privacy protection under the common law. *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 383–89 (1960) (describing the impact of the Warren and Brandeis article). In the employment setting, the American Law Institute (ALI) recently approved a privacy section of its ongoing project, a Restatement of Employment Law, which may become a source for addressing workplace privacy protections. *See* RESTATEMENT (THIRD) OF EMP'T LAW: EMP. PRIVACY AND AUTONOMY § 7.01, (Tentative Draft No. 5, (2012), *available at* http://www.ali.org/00021333/Employment_Law_TD5_online.pdf. The ALI Council approved Chapter 7 of this Restatement in January 2012, subject to discussion and final editing. *Restatement Third, Employment Law*, ALI PUBLICATIONS CATALOG, http://www.ali.org/index.cfm?fuseaction=publications.ppage&node_id=31 (last visited Dec. 27, 2012). Chapter 7 was approved by the ALI membership on May 22, 2012 at its annual meeting. *See Updates*, ALI 2012 ANN. MEETING, http://2012am.ali.org/updates.cfm?startrow=31 (last visited Dec. 27, 2012).

88. *See* Stall v. State, 570 So.2d 257, 265 (Fla. 1990) (citing THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT 29 (1st ed. 1880)).

Samuel Warren and Louis Brandeis expanded that concept in their landmark 1890 law review article, "The Right to Privacy."[89]

The next major expansion of this tort occurred when Dean William Prosser addressed it in his landmark 1960 law review article, *Privacy*.[90] According to Dean Prosser, "[w]hat has emerged from the [common law] decisions is . . . not one [invasion of privacy] tort, but a complex of four."[91] Those four types of invasion of privacy torts are: (1) "Intrusion upon a [person's] seclusion or solitude, or into [the person's] private affairs"; (2) "Public disclosure of embarrassing private facts about the [person]"; (3) "Publicity which places the [person] in a false light in the public eye"; and (4) "Appropriation" by a person, for that person's advantage, of the "name or likeness" of another person.[92] Dean Prosser's analysis of the invasion of privacy tort was incorporated into the Restatement (Second) of Torts, which identifies these four different types of invasion of privacy torts in their shortened form as: "Intrusion upon Seclusion";[93] "Appropriation of Name or Likeness";[94] "Publicity Given to Private Life";[95] and "Publicity Placing Person in False Light."[96]

A classic example and application of the invasion of privacy tort in the employment setting occurred in *Smyth v. Pillsbury Co.*[97] Therein, an employee who sent an email to his supervisor criticizing his employer was terminated despite being told that his communications would be kept private.[98] The court, while considering various legal concerns, looked at the invasion of privacy tort pursuant to the Restatement (Second) of Torts section 652B, which establishes a claim for invasion of privacy based upon unreasonable intrusion upon the seclusion of an individual.[99] Under that section of the Restatement (Second) of Torts, liability for invasion of privacy can occur when there is an unreasonable intrusion that is substantial and would be offensive to a reasonable person.[100] However, after applying the section 652 provisions for invasion of privacy based upon unreasonable intrusion upon seclusion, the court in *Smyth* concluded that there is no "reasonable expectation of privacy in e-mail communications . . . notwithstanding any assurances that such communications would not be intercepted by management."[101]

---

89. *See* Warren & Brandeis, *supra* note 87.
90. *See* Prosser, *supra* note 87, at 389–410.
91. *Id.* at 389.
92. *Id.*
93. RESTATEMENT (SECOND) OF TORTS § 652B (1977).
94. *Id.* § 652C.
95. *Id.* § 652D.
96. *Id.* § 652E.
97. 914 F. Supp. 97 (E.D. Pa. 1996).
98. *Id.* at 98–99 & n.1.
99. *Id.* at 100–01.
100. *Id.* at 100 (citing Borse v. Piece Goods Shop, Inc., 963 F.2d 611, 620 (3d Cir. 1992)).
101. *Id.* at 101.

Specifically, the court noted that when "communications [were] voluntarily made by an employee to his supervisor over the company e-mail system . . . apparently utilized by the entire company, any reasonable expectation of privacy was lost."[102] Then, the court found that even if there was a reasonable expectation of privacy, the employer's interception of the employee's email communications could not invade the employee's privacy interests because they could not be considered "a substantial and highly offensive invasion of his privacy."[103] According to the court in *Smyth*, the employer had a legitimate, work-related interest in "preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system [that] outweighs any privacy interest the employee may have in those comments."[104] One commentator has asserted that the 1996 holding in *Smyth* was extremely important in limiting the ability of employees to pursue tort-based invasion of privacy claims because the decision made it "more difficult to argue . . . that such an expectation [of privacy in workplace email communications] is reasonable."[105] Nevertheless, because "most American employees believe that their e-mails are private,"[106] the law should expand to recognize this belief.

Unfortunately, other cases addressing invasion of privacy under the Restatement (Second) of Torts still suggest that courts may not be willing to expand the expectation of privacy in employee emails through tort law. In an unpublished opinion, *McLaren v. Microsoft Corp.*,[107] the employee asked the court to determine, pursuant to Texas law, that an "employer's review and dissemination of [an employee's email] stored in a 'personal folders' application on [the employee's] office computer" involved an invasion of privacy tort for intruding upon his seclusion.[108] In an unpublished opinion, the court rejected McLaren's tort claim.[109] McLaren was suspended pending an investigation regarding accusations of sexual harassment made against him.[110] While the investigation was pending, McLaren requested access to his office computer to

---

102. *Id.*
103. *Id.*
104. *Id.*
105. *See* Peter J. Isajiw, Comment, *Workplace E-mail Privacy Concerns: Balancing the Personal Dignity of Employees with the Proprietary Interests of Employers*, 20 TEMP. ENVTL. L. & TECH. J. 73, 75 (2001) (citing *Smyth*, 914 F. Supp. at 101).
106. *Id.* at 79–80; *see also* Paul E. Hash & Christina M. Ibrahim, *E-mail, Electronic Monitoring, and Employee Privacy*, 37 S. TEX. L. REV. 893, 894 & n.5 (1996) (noting that the controversy over employer access to private email files "stems from the diametrically opposite views held by employers and employees regarding the ownership of E-mail" because "[e]mployees consider their E-mail messages to be their private property") (quoting Larry O. Natt Gantt, II, *An Affront to Human Dignity: Electronic Mail Monitoring in the Private Sector Workplace*, 8 HARV. J.L. & TECH. 345, 349 (1995)).
107. No. 05-97-00824-CV, 1999 WL 339015 (Tex. Ct. App. May 28, 1999).
108. *Id.* at *1.
109. *Id.*
110. *Id.* at *5.

disprove the allegations and asked that "no one tamper with his [office computer]."[111]

After his termination, McLaren filed an invasion of privacy suit against his employer for "breaking into" his work computer to review files stored in a "personal" folder and then disseminating the information in those files to third parties.[112] McLaren had restricted access to the folder by creating and using a personal password.[113] McLaren's employer, Microsoft, argued: "[t]he common law of Texas does not recognize any right of privacy in the contents of electronic mail systems and storage that are provided to employees by the employer as part of the employment relationship."[114]

The trial court in *McLaren* agreed with the employer[115] and, on appeal, the appellate court explained that Texas does recognize four kinds of torts for invasion of privacy: "(1) [i]ntrusion upon the plaintiff's seclusion or solitude into his private affairs; (2) [p]ublic disclosure of embarrassing private facts about the plaintiff; (3) [p]ublicity which places the plaintiff in a false light in the public eye; [and] (4) [a]ppropriation, for the defendant's advantage, of the plaintiff's name or likeness."[116] The court also found that because the employer provided the computer to the employee for the purpose of storing work-related items, not personal items, these emails were not the employee's "personal property."[117] Also, even though the employee moved and saved his emails to a private folder which was password-protected, the fact that emails traveled over the company's network and were accessible by the employer at some point suggested there had been no reasonable expectation of privacy.[118] Further, even if the employee had such an expectation, the court found that Microsoft's interception of the communications was not a highly offensive invasion because of the company's interest in preventing illegal and unprofessional activity over its email system.[119]

---

111. *Id.* at *1.
112. *Id.*
113. *Id.*
114. *Id.* (alteration in original) (internal quotation marks omitted).
115. *Id.* at *2.
116. *Id.* at *3 (citing Indus. Found. of the S. v. Tex. Indus. Accident Bd., 540 S.W.2d 668, 682 (Tex. 1976), *cert denied*, 430 U.S. 931 (1977)); *see also* Brabham, *supra* note 80, at 1015 n.176 (asserting that three of the invasion of privacy torts apply to employee monitoring: "(1) the unreasonable intrusion into the 'private affairs or concerns' of another"; "(2) the unreasonable disclosure of 'matter concerning the private life of another'"; and "(3) 'publicity [that unreasonably places another] in a false light'" (quoting RESTATEMENT (SECOND) OF TORTS §§ 652B, D, & E (1977))).
117. *McLaren*, 1999 WL 339015, at *4.
118. *Id.*
119. *Id.* at *5.

C. *Stored Communications Act*

The Stored Communications Act (SCA)[120] establishes criminal and civil liability for someone who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility" when the action involves "access to a wire or electronic communication while it is in electronic storage in such system."[121] The SCA provides a major vehicle for employer liability when an employer accesses ESI.[122] In one key case, an employee, who sued her employer for sexual harassment, discovered during litigation that her supervisor retrieved emails from her personal email account through an employer-provided computer.[123] The Fourth Circuit Court of Appeals found no error in the district court's punitive damages award for her claim that the supervisor's actions violated the SCA.[124]

In another case, an employer attempted to circumvent the SCA by asking two employees, who had access to another employee's created web site, to provide the employer their passwords so that the employer would have authorized access to the password-protected web site.[125] Other employers have sought to obtain or have required that employees provide passwords to social media web sites.[126] But, some states have responded negatively to these acts by

---

120. 18 U.S.C. §§ 2701–2711 (2006).

121. *Id.* § 2701. For a more detailed discussion of the SCA, see 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 (2004) (providing a comprehensive review of the SCA).

122. *See, e.g.*, Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 552 (S.D.N.Y. 2008) (describing SCA claim where an employer accessed a former employee's Hotmail account and used a password sent to that account to discover and access the former employee's Gmail account as well). The employee was able to prevail in the SCA claim based upon the employer's access of the two email accounts. *See* Pure Power Boot Camp, Inc. v. Warrior Fitness Boot Camp, LLC, 759 F. Supp. 2d 417, 429 (S.D.N.Y. 2010).

123. Van Alstyne v. Electronic Scriptorium, Ltd., 560 F.3d 199, 202 (4th Cir. 2009); *see also* Searcey, *supra* note 26, at A17 (describing how, in the *Van Alstyne* case, a supervisor obtained access to an employee's private AOL email account, which she sometimes used for business purposes on her employer-provided computer, and the supervisor continued to read her personal email account even after the employee stopped working for the employer).

124. *Van Alstyne*, 560 F.3d at 209. The case, however, was remanded to the district court to reevaluate the merits in light of the court's ruling that proof of actual damages must be present for Van Alstyne to recover statutory damages. *Id.*

125. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 872–73 (9th Cir. 2002). The Ninth Circuit reversed the district court's grant of summary judgment as to the SCA claim, reasoning that "we must assume that neither [employee] was a 'user' of the website at the time he authorized [the employer] to view it." *Id.* at 880.

126. *See, e.g.*, Pietrylo v. Hillstone Rest. Grp., No. 06-5754(FSH), 2009 WL 3128420, at *3, *6 (D.N.J. Sept. 25, 2009) (rejecting employer's argument that an employee gave verbal consent to allow the employer to access a password-protected online chat forum, suggesting that the jury could have believed that the employee did not authorize the access and was instead improperly coerced to give up the password, and upholding a jury verdict along with punitive damages for an SCA violation).

making it illegal for employers to demand passwords to electronic sites from employees or applicants.[127]

In the intermediate appellate court decision that led to the Supreme Court's decision in *Quon*, the United States Court of Appeals for the Ninth Circuit found a violation of the SCA.[128] In a part of the decision that was not challenged to the Supreme Court, the Ninth Circuit held that Arch Wireless violated the SCA when it knowingly turned over pager text transcripts to the City of Ontario Police Department, which was not an intended recipient or an addressee of the messages.[129]

D. Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA)[130] appears to create criminal liability for an employer who attempts to gain unauthorized access to an employee's personal electronic device and provides for civil liability as well when the unauthorized access causes damages exceeding $5,000.[131] The law was originally designed to respond to juvenile hackers by prohibiting them from attacking the federal government's computers.[132] However, the CFAA has also been used to deter industrial espionage efforts related to the hacking of a business computer to obtain trade secrets.[133] In a recent case, Chief Judge Kozinski of the United States Court of Appeals for the Ninth Circuit asked whether the CFAA also extends to situations where employees exceed the limitations created by employer electronic use policies: "Many employers have adopted policies prohibiting the use of work computers for nonbusiness purposes. Does an employee who violates such a policy commit a federal crime? How about someone who violates the terms of service of a social networking website? This depends on how broadly we read the [CFAA]."[134] However, the

---

127. *See* Garcia, *supra* note 39, at 5 (Illinois); Kevin Rector, *Maryland Becomes First State to Ban Employers from Asking for Social Media Passwords*, BALT. SUN (Apr. 10, 2012, 10:15 PM), http://articles.baltimoresun.com/2012-04-10/news/bs-md-privacy-law-20120410_1_facebook-password-social-media-bradley-shear (Maryland).

128. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 903 (9th Cir. 2008), *cert. denied on SCA issue sub nom.*, USA Mobility Wireless v. Quon, 130 S. Ct. 1011 (2009) (mem.), *and rev'd on other grounds sub nom.*, City of Ontario v. Quon, 130 S. Ct. 2619 (2010).

129. *Id.* at 900, 903.

130. 18 U.S.C. § 1030 (2006).

131. *Id. See generally* Andrew T. Hernacki, Comment, *A Vague Law in a Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. REV. 1543, 1551–74 (2012) (citations omitted).

132. Hernacki, *supra* note 131, at 1546 (citing Sarah Boyer, Note, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 RUTGERS J.L. & PUB. POL'Y 661, 665 (2009)).

133. *See* United States v. Nosal, 676 F.3d 854, 856–63 (9th Cir. 2012) (citations omitted) (discussing the extent and possible interpretations of the CFAA). In *Nosal*, employees of a company violated their company's use policy and transferred confidential records to a third party. *Id.* at 856. The Ninth Circuit found that the CFAA does not apply to internal violations of a company's policies. *Id.* at 863.

134. *Id.* at 856.

Ninth Circuit refused to extend the CFAA—which covers hacking into a computer to obtain unauthorized access to data—to acts involving employee misuse of authorized access to data.[135] While employer-provided devices do not seem to pose a problem of unauthorized access under the CFAA, employers who allow employees to use their personal devices and later attempt to access those devices without, or beyond the scope of, the employee's permission may face CFAA concerns.[136]

IV. ATTORNEY–CLIENT PRIVILEGE: A NEW INDICATOR OF PRIVACY EXPECTATIONS

On September 13, 2009, a *New York Times* article identified that there are "thousands of blogs and so many lawyers online," and the "collisions between the freewheeling ways of the Internet and the tight boundaries of legal discourse are inevitable—whether they result in damaged careers or simply raise eyebrows."[137] A recent study indicated that "86 percent of lawyers ages 25 to 35 are members of social networks like Facebook, LinkedIn and MySpace."[138] The article also provided a number of recent examples regarding the ethical problems that lawyers have faced when dealing with cyberspace communications.[139] One example was a situation where an attorney who made hostile comments on a blog about a judge he had appeared in front of received sanctions and an ethical reprimand for such communications.[140]

All of these cyberspace collisions with attorney ethics issues may also provide a window into the realities of employee privacy expectations when dealing with the significant technological growth in electronic communications through the development of various digital devices. Joining concepts of employee privacy and ethics is not new. In 1993, Frank Cavico identified a merger of these issues with respect to the ethics of secretly monitoring

---

135. *Id.* at 857, 863 (refusing to "transform the CFAA from an anti-hacking statute into an expansive misappropriation statute").

136. *See* GARRY G. MATHIASON ET AL., THE "BRING YOUR OWN DEVICE" TO WORK MOVEMENT: ENGINEERING PRACTICAL EMPLOYMENT AND LABOR LAW COMPLIANCE SOLUTIONS 13–16 (2012), *available at* http://www.littler.com/files/press/pdf/TheLittlerReport-TheBringYourOwnDeviceToWorkMovement.pdf (describing CFAA concerns for employers when employees are allowed to use their personal electronic devices at work).

137. John Schwartz, *A Legal Battle: Online Attitude Vs. Rules of the Bar*, N.Y. TIMES (late ed.), Sept. 13, 2009, at 1.

138. *Id.* (citing LEADER NETWORKS, 2009 NETWORKS FOR COUNSEL STUDY: A GLOBAL STUDY OF THE LEGAL INDUSTRY'S ADOPTION OF ONLINE PROFESSIONAL NETWORKING, PREFERENCES, USAGE AND FUTURE PREDICTIONS 10 (2009), *available at* http://www.leadernetworks.com/documents/Networks_for_Counsel_2009.pdf).

139. *Id.*

140. *Id.*; *see also* Debra Cassens Weiss, *Too Much Information: Blogging Lawyers Face Ethical and Legal Problems*, A.B.A. J. (Sept. 14, 2009, 9:52 AM), http://www.abajournal.com/news/article/too_much_information_blogging_lawyers_face_ethical_and_legal_problems/ (describing a reprimand for an attorney who described a judge as an "evil, unfair witch" in a blog post).

employees.[141] More recently, in 2010, Gregory Sisk and Nicholas Halbur suggested that employee privacy issues in the workplace may also raise concerns regarding attorney–client-privilege ethics.[142] Specifically, concerns about privacy and confidentiality of communications made by employees to their attorneys on employer-provided equipment have resulted in ethical challenges based upon violations of attorney–client privilege.[143] These ethical challenges, and the actions of the employers and employees involved, help to identify the parameters of employee expectations of privacy and confidentiality.[144]

The ABA Model Rules for attorney ethics were amended in 2002 to include Model Rule 4.4(b), which provides "that a receiving lawyer who 'knows or reasonably should know that [a] document was inadvertently sent shall promptly notify the sender.'"[145] A comment to this Model Rule provides that "[w]hether the [receiving] lawyer is required to take additional steps, such as returning the document or electronically stored information, is a matter of law beyond the

---

141. *See* Frank J. Cavico, *Invasion of Privacy in the Private Employment Sector: Tortious and Ethical Aspects*, 30 HOUS. L. REV. 1263, 1265–67 (1993) (asserting that there is an "immense new array of sophisticated technology . . . available to the employer . . . to engage in surveillance, monitoring, and testing of employees" that makes secret supervision possible). For a modern discussion of using social media and digital technology as a form of surveillance of employees and the attorney ethical implications, see Allison Clemency, Comment, *"Friending," "Following," and "Digging" up Evidentiary Dirt: The Ethical Implications of Investigating Information on Social Media Websites*, 43 ARIZ. ST. L.J. 1021, 1029–35 (2011) (describing ethical committee decisions regarding an attorney's access of social media).

142. *See* Gregory C. Sisk & Nicholas Halbur, *A Ticking Time Bomb? University Data Privacy Policies and Attorney–Client Confidentiality in Law School Settings*, 2010 UTAH L. REV. 1277, 1278; *see also* Richard L. Marcus, *The Electronic Lawyer*, 58 DEPAUL L. REV. 263, 293–98 (2009) (describing how the expanded use of email, laptops, and other handheld computer devices has resulted in problems maintaining attorney–client confidences).

143. *See* Sisk & Halbur, *supra* note 142, at 1278.

144. *See* 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, 367–81 (2008); *see also* John Gergacz, *Employees' Use of Employer Computers to Communicate with Their Own Attorneys and the Attorney–Client Privilege*, 10 COMPUTER L. REV. & TECH. J. 269, 286 (2006) ("Employees' privilege assertions are most at risk if their communications violated company computer-use policy, the employee[] understood that [she was] doing so, and the policy contained a monitoring provision."); Hill, *supra* note 8, at 572–82 (describing privacy expectations and attorney–client-privilege cases); Meir S. Hornung, Note, *Think Before You Type: A Look at Email Privacy in the Workplace*, 11 FORDHAM J. CORP. & FIN. L. 115, 128 (2005) (citing RESTATEMENT (SECOND) OF TORTS § 652B (1977)); Adam C. Losey, Note, *Clicking away Confidentiality: Workplace Waiver of Attorney-Client Privilege*, 60 FLA. L. REV. 1179, 1184 (2008) (suggesting that courts should adopt a rebuttable presumption of waiver of attorney–client privilege to establish "predictability in workplace waiver cases"); Searcey, *supra* note 26, at A17 (describing cases related to privacy challenges resulting from employer decisions to retrieve employee information from an employer-provided device).

145. Schaefer, *supra* note 11, at 205 (quoting MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2011)). This Model Rule was amended at the ABA House of Delegates Annual Meeting in August 2012 to add "electronically stored information" to the inadvertently sent inquiry. *See* ABA COMM'N ON ETHICS 20/20, REVISED RESOLUTION 105A, at 5 (2012) [hereinafter 20/20 RESOLUTION], *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf.

scope of these Rules, as is the question of whether the privileged status of a document or electronically stored information has been waived."[146] Another comment to Rule 4.4 notes that a lawyer may return inadvertently disclosed information unread, even if the attorney has no legal obligation to do so.[147]

One commentator recently noted the implications for attorneys in dealing with inadvertent disclosures under Model Rule 4.4:

> Thirty-two states have adopted Model Rule 4.4(b) or a substantially similar provision. Eight states and the District of Columbia have adopted their own professional conduct rules that require receiving counsel to take one or more steps beyond notification. In thirty-nine of these forty-one jurisdictions with a professional conduct rule addressing the issue, the receiving attorney has no obligation unless he or she determines opposing counsel sent the document "inadvertently." In the remaining ten states, no professional conduct rule addresses the recipient's ethical obligations. Regardless of whether a state has or has not adopted an inadvertent disclosure rule, recipients of inadvertent disclosure should research the jurisdiction's ethics opinions and case law that may provide additional authority, conflicting authority, or the only authority regarding counsel's obligations. Finally, attorneys should proceed with caution when practicing in a jurisdiction that has not definitively addressed the issue, as their case may be the one in which the jurisdiction announces its expectations for counsel.[148]

Model Rule 4.4(b) does not clearly prohibit use of an inadvertent communication prior to a waiver ruling.[149] However, some jurisdictions have expanded their ethical requirements to find that the attorney must either refrain from reviewing such materials or review them only to the extent required to determine how to proceed appropriately.[150] Upon completing that review, the attorney should notify the adversary's lawyer that such materials are in the possession of the attorney and should either follow instructions of the adversary's lawyer with respect to the disposition of the materials or refrain from using the materials until a definitive resolution as to the proper disposition of the materials is obtained from a court.[151] A few recent cases, along with recent state

---

146. MODEL RULES OF PROF'L CONDUCT R. 4.4 cmt. 2 (2012), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_4_4_respect_for_rights_of_third_persons/comment_on_rule_4_4.html.

147. *Id.* R. 4.4 cmt. 3; Schaefer, *supra* note 11, at 205.

148. Schaefer, *supra* note 11, at 206–08 (footnotes omitted).

149. *Id.* at 225.

150. *See, e.g.*, Utah State Bar Ethics Advisory Op. Comm., Op. No. 99-01 (1999), *available at* http://www.utahbar.org/rules_ops_pols/ethics_opinions/op_99_01.html (discussing ABA ethics advisory opinions).

151. *Id.* ("[T]he best course of action [is] for the receiving attorney to advise opposing counsel . . . and then either return the documents or seek assistance from the court in determining

and ABA ethics opinions, highlight this merger of ethical attorney–client-privilege concerns with concerns about employees' expectations of privacy in email communications.

A. Stengart v. Loving Care Agency, Inc.

In *Stengart v. Loving Care Agency, Inc.*,[152] the New Jersey Supreme Court reviewed the realities of employee expectations of privacy and confidentiality in communications made on an employer-provided device to an attorney.[153] After resigning from her employment, Marina Stengart filed a lawsuit against her former employer, Loving Care Agency, Inc. (Loving Care), alleging constructive discharge, retaliation, and harassment among other things.[154] Before Stengart's employment with Loving Care ended, she sent several emails to her attorney from her personal Yahoo account on a company-provided laptop in which she complained about how her employer had treated her.[155] Stengart never saved her personal email password on the computer and never sent an email to her attorney from the company provided email system.[156] However, unbeknownst to Stengart, all of her personal emails were saved to the hard drive of the laptop.[157] After Stengart tendered her resignation and filed suit, Loving Care employed a computer forensic specialist to preserve Stengart's laptop hard drive.[158] The computer forensic specialist obtained access to the emails in question by reviewing cached web site pages saved on the laptop after Stengart visited those pages to access her private email account.[159]

Stengart was unaware that Loving Care had obtained the emails until discovery when Loving Care's attorneys used information from the emails to reply to Stengart's first set of interrogatories.[160] Stengart's attorney, asserting attorney–client privilege, sought return of the emails and applied for an order to

---

the appropriate course of action under the particular facts at hand."); *see also* N.H. RULES OF PROF'L CONDUCT R. 4.4(b) (2010) (requiring the additional duty to not examine documents that the attorney knows were inadvertently sent under the New Hampshire rule as compared to the Model Rule). More recently, Federal Rule of Evidence 502 was enacted as a result of the growth of electronic data and the need to guard against potentially harmful effects if privileged information was inadvertently disclosed though electronic discovery. Klinefelter, *supra* note 1, at 28–30 (describing events leading to the enactment of Federal Rule of Evidence 502 and how that Rule strikes a balance regarding inadvertent disclosure through electronic discovery by looking at factors such as "whether [the] lawyer [took] reasonable precautions against inadvertent disclosure and whether overall fairness would be better served by waiver or maintenance of the privilege" under the circumstances at issue).

152. 990 A.2d 650 (N.J. 2010).
153. *Id.* at 655.
154. *Id.*
155. *Id.* at 656.
156. *Id.*
157. *Id.* at 655–56.
158. *Id.* at 656.
159. *Id.*
160. *Id.*

show cause, which the trial court converted to a motion and thereafter denied.[161] The appellate court reversed the trial court and directed Loving Care's attorneys to return the emails and delete any record of them.[162] Loving Care appealed, and the issue before the New Jersey Supreme Court was whether an employee has a reasonable expectation of privacy in emails between her and her attorney when the employee sent the emails from a company-owned laptop but only used the employee's personal, password-protected email account.[163]

On appeal to the New Jersey Supreme Court, Loving Care argued that either Stengart had waived any privacy and attorney–client-privilege rights pursuant to Loving Care's computer use policy when she sent the emails while using the company laptop or the privilege had never attached.[164] Loving Care's computer use policy: (1) reserved for Loving Care the right to review, intercept, audit, etc., any matters on the "company's media systems and services at any time," (2) declared emails, voicemails, Internet use, etc., would be considered company property, but (3) allowed "occasional personal use."[165] The policy also expressly prohibited certain criminal uses, but the policy failed to disclose that personal emails would be saved on the hard drive.[166] Stengart, in turn, argued that she was not given notice that emails from her personal, password-protected email account would be subject to the policy.[167] The court examined two key issues: (1) "the adequacy of the notice provided by the [p]olicy" and (2) the public policy concern with preserving the attorney–client privilege.[168]

The court found the scope of the policy "not entirely clear."[169] First, the policy used general language and failed to define the terms "media systems and services."[170] Also, the policy failed to mention personal email and did not warn the employees that any emails would be saved to the hard drive.[171] Furthermore, the court noted that it would be unreasonable to assert that merely because a client emailed her attorney from a company computer, the client waived the privilege.[172] The court continued its analysis by referring to section 652B of the Restatement (Second) of Torts and to treatment of this issue by other courts.[173]

After noting that the computer policy did not place Stengart on notice that her employer would retrieve her personal emails, the court examined Stengart's

161. *Id.* at 656–57.
162. *Id.* at 657.
163. *Id.* at 655.
164. *Id.* at 658.
165. *Id.* at 657.
166. *Id.*
167. *Id.* at 658.
168. *Id.* at 659.
169. *Id.*
170. *Id.*
171. *Id.*
172. *See id.* at 660, 664.
173. *Id.* at 660–63.

actions to protect the communications.[174] The court acknowledged that Stengart was careful not to send messages from the company email account and that she never saved her Yahoo password or username on the laptop.[175] The court found under these circumstances, where the policy did not place her on notice and she attempted to protect the communications, Stengart could not be held to have waived her privacy rights.[176] Finally, the New Jersey Supreme Court explained that every email situation does not always warrant privacy protection for employees.[177] Employers can ban personal use, expressly tell employees that personal emails will be logged and reviewed, or discipline employees for inappropriate use of electronic communications consistent with a properly disclosed Internet policy.[178] Therefore, merely asserting ownership of an electronic device and its contents, without more, does not remove employee expectations of privacy.[179] Thus, in this case, Loving Care should have immediately notified its adversary of its possession of the emails.[180]

B. Holmes v. Petrovich Development Co.

In *Holmes v. Petrovich Development Co.*,[181] Gina Holmes filed suit against her former employer alleging sexual harassment, intentional infliction of emotional distress, wrongful termination, retaliation, and violation of her right to privacy.[182] Holmes started her employment as an executive assistant in early June 2004.[183] The next month, Holmes told her employer that she was pregnant, the baby would be due the first week of December, she was planning to work up to her due date, and she would be out for six weeks of maternity leave following her pregnancy.[184] On August 6, 2004, after her employer expressed the need to find and train Holmes's temporary replacement, Holmes notified her employer that she would need her maternity leave to start in mid-November instead of December and would require four months of maternity leave instead of six weeks.[185]

Holmes's employer responded shortly thereafter inquiring as to how far along in her pregnancy Holmes really was when she interviewed for the position and asserted that he felt deceived.[186] Holmes responded with a long email

174. *Id.* at 663.
175. *Id.*
176. *Id.* at 665.
177. *Id.*
178. *Id.*
179. *See id.*
180. *Id.* at 666.
181. 119 Cal. Rptr. 3d 878 (Ct. App. 2011).
182. *Id.* at 882.
183. *Id.* at 883.
184. *Id.* at 884.
185. *Id.*
186. *Id.*

describing her problems with prior pregnancies and asked her employer if he wanted her to quit.[187] The employer asserted that he still wanted to employ Holmes but needed honesty from all employees.[188] By August 10, 2004, they agreed to move forward.[189] However, Holmes later became upset when she learned that her employer had forwarded her email to other employees.[190] On the same day she told her employer that they should move forward in "a positive direction," Holmes used her company computer to send emails to an attorney.[191] She resigned the next day, and in September 2005, she filed a lawsuit against the employer.[192]

As part of her claim for violation of privacy, Holmes asserted that her employer had illegally disseminated her "highly personal" emails to other employees.[193] Further, Holmes alleged that the emails she sent to her attorney from the company computer were protected under the attorney–client privilege.[194] The employer filed a motion for summary judgment asserting that Holmes had failed to state a claim because the emails sent on the company computer were not private.[195] The trial court denied the motion, but at trial, a verdict was entered in favor of the employer.[196] On appeal, Holmes contended that the trial court erred by: (1) denying her demand for the return of the emails between her and her attorney; (2) permitting the employer to introduce the emails at trial; and (3) "giving a limiting instruction that undermined her [claim] for invasion of privacy."[197]

The appellate court in *Holmes* referenced the employer's computer policy, which "direct[ed] employees that the company's technology resources should be used only for company business and that employees are prohibited from sending or receiving personal e-mails."[198] Further, the court highlighted that "the handbook warns that '[e]mployees who use the Company's Technology Resources to create or maintain personal information or messages have no right of privacy with respect to that information or message.'"[199] As a result, the court concluded that Holmes had no expectation of privacy in her emails because the computer policy placed her on notice that the emails could be accessed by the employer.[200]

---

187. *Id.* at 884–85.
188. *Id.* at 885–86.
189. *Id.* at 886.
190. *Id.*
191. *Id.*
192. *Id.* at 887.
193. *Id.*
194. *Id.* at 893–94.
195. *Id.* at 887.
196. *Id.* at 888.
197. *Id.* at 893.
198. *Id.* at 883.
199. *Id.* (alteration in original).
200. *Id.* at 896.

As a final highlight, the court in *Holmes* used a tantalizing analogy to explain its ruling. The court compared Holmes's use of the company computer to communicate with her attorney through emails as similar to "consulting her attorney in one of defendants' conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by [her employer] would be privileged."[201] Pursuant to the same reasoning it used to find that Holmes had no reasonable expectation of privacy, the court rejected Holmes' other related privacy claims, Holmes's jury instruction challenge, and Holmes' request for sanctions.[202]

C. Convertino v. United States Department of Justice

In *Convertino v. United States Department of Justice*,[203] the United States District Court for the District of Columbia found that although Jonathan Tukel, an Assistant United States Attorney, had used his employer's computer and his work email in making communications to his private attorney, those email communications were still subject to attorney–client-privilege protection.[204] According to the court, the employee "reasonably expected" that his emails would be confidential because he was unaware of the fact that his employer would be reviewing emails sent from his account.[205] Moreover, the court found that the employer, the Department of Justice, had a policy of allowing personal use of an employee's email account.[206] As evident from the different rulings in *Stengart*, *Holmes*, and *Convertino*, case law on the issue of accessing attorney–client communications stored on employer computers is split. These cases have not yielded a clear rule, and the appropriate analysis appears to depend on the specific facts in each case.[207]

---

201. *Id.* It is the author's view that the court's analogy in *Holmes* about consulting an attorney in one of the employer's conference rooms has merit when assessing the reality of employee privacy expectations regarding emails to an attorney found on an employer-provided device. *See infra* Part VI. But the court's application of this analogy in *Holmes* was wrong when it injected hyperbole about speaking in "a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by [her employer] would be privileged." *Holmes*, 119 Cal. Rptr. 3d at 896; *see infra* Part VI.

202. *Holmes*, 119 Cal. Rptr. 3d at 893–900.

203. 674 F. Supp. 2d 97 (D.D.C. 2009).

204. *Id.* at 110.

205. *Id.*

206. *Id.*

207. Of these cases, the *Stengart* decision may suggest more of a concern given it involved access by an employer of an employee's private email system as compared to an employee's use of the employer's own email system. *See Holmes*, 119 Cal. Rptr. 3d at 896 (distinguishing *Stengart* on the basis that *Stengart* involved use of a personal, web-based email of an employee, not the use of the employer's own email system).

D. California Ethics Opinion No. 2010-179: Attorneys Beware and Protect

Given the concerns about protecting the attorney–client privilege relating to cyberspace communications, it is not surprising that jurisdictions are starting to address this issue through ethics opinions. Unfortunately, the efforts have been aimed at placing more burdens on attorneys to defend against hackers, snoops, scavengers, and electronic dumpster-divers rather than protecting the communications despite offensive efforts to obtain the information.[208] The State Bar of California Committee on Professional Responsibility and Conduct issued Formal Opinion No. 2010-179[209] to address an attorney's ethical duties when accessing public wireless networks while using a company-provided computer. The opinion states that attorneys, pursuant to their duty of confidentiality and competence, "should consider the following before using a specific [wireless] technology": (1) "[t]he attorney's ability to assess the level of security afforded by the technology"; (2) "[w]hether reasonable precautions may be taken when using the technology to increase the level of security"; (3) the limitations on third party access and monitoring; (4) the legal ramifications of a third party accessing information under privacy and wiretap laws; (5) the level of sensitivity of the information involved; (6) the potential level of detriment to the client from inadvertent disclosure through the technology; (7) the urgency of the need to use the technology in question; and (8) whether specific client instructions were violated.[210] At a minimum, the California Ethics opinion suggests that lawyers should ensure that they have some type of encryption-protected Wi-Fi if they intend to access confidential client work files while using laptops and other digital devices when at home or in the general public.[211]

Despite imposing increased expectations on attorneys to protect the confidentiality of cyberspace communications, the opinion also acknowledges the existence of attorney–client privileges even when there is a general understanding that wireless communications may be viewed by outsiders—a position supported by a 1999 ABA ethics opinion.[212] Nevertheless, this California ethics opinion matches a trend of requiring attorneys to take on more

---

208. *See, e.g.*, Cal. State Bar Comm. on Prof'l. Responsibility & Conduct, Formal Op. 2010-179 (2010) [hereinafter Cal. Formal Ethics Op. 2010-179], *available at* http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=837 (addressing the issue of whether "an attorney violates the duties of confidentiality and competence . . . by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties").

209. *See id.*

210. *Id.* at 3–6 (citations omitted).

211. *See id.* at 7; Eric B. Evans et al., *California Bar Clarifies Rules Governing Wireless Network Use*, MAYER BROWN (Feb. 9, 2011), http://www.mayerbrown.com/publications/California-Bar-Clarifies-Rules-Governing-Wireless-Network-Use-02-09-2011/.

212. *See* Cal. Formal Ethics Op. 2010-179, *supra* note 208, at 3–4 ("[A]ttorneys have a reasonable expectation of privacy in email communications, even if unencrypted, 'despite some risk of interception and disclosure.'" (quoting ABA Opinion 99-413, *supra* note 19, at 1101:188)).

responsibility to protect the confidentiality of cyberspace communications without addressing the realistic expectations of their clients, who desire to communicate via electronic devices.[213] Therefore, this opinion makes it slightly more difficult for those seeking to expand the privacy rights of employees who use an employer-provided digital device to make and receive what should be confidential and privileged communications over wireless networks.

E. ABA Ethics Opinion 11-459: More Burdens on Attorneys to Protect Confidentiality of Email Communications

In 1999, the ABA Committee on Ethics and Professional Responsibility concluded that sending unencrypted emails via the Internet between an attorney and client did not violate the attorney's ethical duty to maintain client confidentiality.[214] On August 4, 2011, the ABA issued two additional formal opinions discussing the ethical responsibilities of attorneys with respect to protecting client confidences when communicating with a client by email[215] and when receiving email communications between a third party and their attorney.[216] With the concern that employers may access an employee's email communications, ABA Opinion 11-459 recommends that an attorney "should instruct the employee-client to avoid using a workplace device or system for sensitive or substantive communications, and perhaps for any attorney-client communications, because even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications."[217]

ABA Opinion 11-459 takes no position as to the substantive law question of whether electronic communications made through a workplace device to an attorney by an employee can be protected by the attorney–client privilege.[218] However, ABA Opinion 11-459 does place the ethical obligation on the employee's attorney to "assume that an employer's internal policy allows for access to the employee's e-mails sent to or from a workplace device or

---

213. *See* Cal. Formal Ethics Op. 2010-179, *supra* note 208, at 7.

214. *See* ABA Opinion 99-413, *supra* note 21, at 1101:181 ("[T]he mode of transmission for unencrypted emails affords a reasonable expectation of privacy from a technological and legal standpoint."); *see also* Comerford, *supra* note 9, at 636 n.53 (stating the same finding as in ABA Opinion 99-413 that lawyers "may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct . . . because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint"); Hill, *supra* note 9, at 21 (citing ABA Opinion 99-413, *supra* note 21, at 1101:181; Del. State Bar Ass'n Comm. on Prof'l Ethics, Op. 2001-2 (2001); Me. Prof'l Ethics Comm'n, Op. 194 (2008)) (describing the ABA's conclusion in Opinion 99-413).

215. *See* ABA Opinion 11-459, *supra* note 3.

216. *See* ABA Opinion 11-460, *supra* note 3.

217. *See* ABA Opinion 11-459, *supra* note 3, at 3.

218. *See id.* ("[W]e express no view on whether, and in what circumstances, an employee's communications with counsel from the employee's workplace device or system are protected by the attorney-client privilege.").

system."[219] Additionally, this opinion places an ethical obligation on the attorney representing an employee to "ascertain . . . whether there is a significant risk that the client will use a business e-mail address for personal communications or whether the employee's position entails using an employer's device."[220]

ABA Opinion 11-459 not only requires that the attorney counsel the employee–client against using workplace devices and work email to communicate with the attorney, but it also demands that the attorney cease email communications with the client if the client appears to have not adhered to the attorney's advice.[221] It is understandable that the ABA would give such guidance, as it is attempting to protect the attorney–client privilege in an area where state law obligations have resulted in uncertainty as to the expectation of privacy in email communications on employer-provided devices. However, ABA Opinion 11-459 may place an employee's attorney in an antagonistic relationship with the attorney's client if the client has to jump through unrealistic hoops to communicate with the attorney without using an employer-provided device as demands on employees to be digitally available all day for communication with their employers have expanded significantly.

F. ABA Ethics Opinion 11-460: Employer Retrieval of Employee Emails to Their Attorney Is Not Inadvertent Disclosure

In an effort to specifically address an employer's review of an employee's email communications with an attorney, the ABA's Standing Committee on Ethics and Professional Responsibility issued Opinion 11-460.[222] Specifically, the opinion addresses the following hypothetical scenario:

> After an employee files a lawsuit against her employer, the employer copies the contents of her workplace computer for possible use in defending the lawsuit, and provides copies to its outside counsel. Upon review, the employer's counsel sees that some of the employee's e-mails bear the legend "Attorney-Client Confidential Communication." Must the employer's counsel notify the employee's lawyer that the employer has accessed this correspondence?[223]

---

219. *Id.*

220. *Id.*

221. *Id.* at 4 n.7 ("Of course, if the lawyer becomes aware that a client is receiving personal e-mail on a workplace computer or other device owned or controlled by the employer, then a duty arises to caution the client not to do so, and if that caution is not heeded, to cease sending messages even to personal e-mail addresses.").

222. *See* ABA Opinion 11-460, *supra* note 3.

223. *Id.* at 1.

According to ABA Opinion 11-460, Model Rule 4.4(b)—which addresses an attorney's obligation to notify the sender of an inadvertent disclosure—does not apply to this scenario because "a document is not 'inadvertently sent' when it is retrieved by a third person from a public or private place where it is stored or left."[224] Although one might imply a duty of the employer's attorney to notify the employee or the employee's attorney of the receipt of email communications between the employee and the employee's attorney—even under the scenario discussed—and some courts have made such a finding,[225] ABA Opinion 11-460 interprets Model Rule 4.4(b) as creating a limit on the circumstances when an attorney has a duty to notify the opposing attorney of the "inadvertent" communications.[226] Because the scenario where an employer retrieves emails sent to an employee's attorney from an employer-provided device does not involve an inadvertent communication according to Opinion 11-460, the opinion further concludes that Model Rule 4.4(b) cannot apply.[227] Instead, Opinion 11-460 makes clear that any duties regarding the handling of the employee's emails to the employee's attorney that are provided by the employer to its attorney must be determined by state law.[228]

However, Opinion 11-460 goes even further by addressing the duties of the employer's attorney who operates in a jurisdiction where the legal duty to report the retrieval of the employee's email is unclear.[229] According to Opinion 11-460, the employer's attorney may have an ethical obligation to not report the retrieval of the employee's email pursuant to Model Rule 1.6(a), which states that "information relating to the representation of [the] client" must be kept confidential unless there is an exception to the confidentiality requirement or the client gives "informed consent" to make a disclosure.[230] Model Rule 1.6(b) does allow the employer's attorney to reveal the retrieval of the employee's emails to the employee's attorney if the employer's attorney reasonably believes disclosure is "necessary . . . to comply with other law or a court order."[231]

But, according to ABA Opinion 11-460, if there is no clear law that applies, the employer's attorney will have to keep the retrieval of the employee's emails confidential unless the employer consents to disclosing the retrieval.[232] The opinion does note that it may be advantageous to the employer to communicate

224. *Id.* (quoting MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2011)).

225. *See id.* at 1–2 (quoting Chamberlain Grp., Inc. v. Lear Corp., 270 F.R.D. 392, 398 (N.D. Ill. 2010)) (citing Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 666 (N.J. 2010)).

226. *Id.* at 2–3 (citing ABA Comm. on Prof'l Responsibility, Formal Op. 06-440 (2006), *reprinted in* ABA/BNA LAWYERS' MANUAL ON PROFESSIONAL CONDUCT: ETHICS OPINIONS 2001–2005, at 1201:174, :175 (2006) [hereinafter ABA Opinion 06-440]; ABA Opinion 06-442, *supra* note 15, at 1301:103); MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2011)).

227. *Id.* at 3.

228. *Id.*

229. *Id.*

230. *Id.* (quoting MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2011)).

231. *Id.* (quoting MODEL RULES OF PROF'L CONDUCT R. 1.6(b)(6) (2011)).

232. *Id.*

the retrieval of the employee's emails to a court so that it may rule on the admissibility of the emails and whether they may be used by the employer and the employer's attorney.[233] While also recognizing that a court's discovery disclosure requirements may require an employer's attorney to notify the employee's attorney of the retrieval of the employee's emails, ABA Opinion 11-460 makes clear that the Model Rules do not require such a notification.[234]

G. The Overall ABA Ethics Approach and Its August 2012 Changes

ABA Opinions 11-459 and 11-460 continue a conservative trend by the ABA in adopting ethics opinions regarding electronic data communications that place the host of ethical burdens on the employee's attorney to prevent the technical mining of this data. Further, the approach of these opinions seems to countenance employer attempts to use advanced technology and computer forensics experts to dumpster-dive and sift through data to find confidential communications never intended to be communicated to the employer. Initially, the ABA had been quite liberal about protecting electronic communications when it found, in 1999, that unencrypted attorney–client emails were protected, confidential communications even if they could be hacked and discovered by outsiders.[235] But in 2006, the ABA started to become more conservative about protecting electronic communications when it decided that an attorney could ethically mine electronic documents to find confidential communications that might be disclosed inadvertently through embedded metadata and placed the ethical burden on the employee's attorney to prevent any disclosure.[236]

Under ABA Opinion 11-460 and ABA Opinion 11-459, the employee's attorney now has an even greater ethical duty and technical obligation to protect the confidentiality of email communications. The attorney must even confront an employee client and discontinue communicating with that client if email communications from the client have come from an employer-provided device, regardless of the client's desires or ability to communicate with the attorney through any other means.[237] In contrast to the obligations of the employee's attorney under the ABA's recent ethical approach to protecting electronic communications, the employer's attorney has no ethical obligation to notify the employee's attorney of the retrieval of the employee's emails or seek a court determination of the admissibility before using the emails.[238] Rather, the employer's attorney is limited only by other legal restraints in the jurisdiction

---

233. *Id.*

234. *Id.*

235. *See* ABA Opinion 99-413, *supra* note 21, at 1101:181 to :182 (identifying an expectation of privacy in email communications between attorneys and clients).

236. *See* ABA Opinion 06-442, *supra* note 15, at 1301:104.

237. ABA Opinion 11-459, *supra* note 3, at 3–4.

238. ABA Opinion 11-460, *supra* note 3, at 2–3 (citing ABA Opinion 06-440, *supra* note 226, at 1201:175; MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2011)).

involved.[239] Absent clarity regarding legal requirements on disclosure, the ABA's ethics opinions even go to the opposite extreme by implying that it may be an ethical violation for the employer's attorney to disclose the retrieval of the employee's emails.[240] Accordingly, this Article calls for states and their attorney ethics committees to adopt a new paradigm that employee emails—if clearly intended to be kept confidential, such as when made to an attorney—should be presumed private and confidential communications even if retrieved by an employer from an employer-provided device.

At its August 2012 meeting, the ABA continued its conservative approach of placing more burdens on the attorney representing an employee regarding technology advances as opposed to the attorney representing an employer who dumpster-dives and mines for data intended to be kept confidential. Specifically, based upon recommendations from its Commission on Ethics 20/20, the ABA adopted changes to the Model Rules by creating a new Rule 1.6(c) to require that a lawyer "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[241] While it is reasonable to expect that an attorney have competency in technology, the changes do not address attorney efforts to mine for confidential data or dumpster-dive. The following language added to comment 18 for Model Rule 1.6(c) does recognize that an attorney may not be able to prevent some disclosures and that actions intended to prevent disclosures that would "adversely affect the lawyer's ability to represent clients" should be considered:

> The unauthorized access to, or the inadvertent or unauthorized disclosure of, [confidential] information . . . does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).[242]

---

239. *Id.* at 3 (citing ABA Opinion 06-442, *supra* note 15, at 1301:103).

240. *Id.* (citing MODEL RULES OF PROF'L CONDUCT R. 1.6(a), (b)(6) (2011)).

241. *See* MODEL RULES OF PROF'L CONDUCT R. 1.6(c) (2012), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information.html (amended by 20/20 RESOLUTION, *supra* note 145, at 4).

242. *Id.* cmt. 18, *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6.html.

Further, the ABA changed the language in Model Rule 4.4(b) to include "electronically stored information"[243] and "metadata"[244] as part of the information that could be inadvertently disclosed and would require the receiving attorney to notify the sending attorney if such information was clearly sent inadvertently.[245] While recognizing that ABA Opinion 06-442 fails to place any burdens on an attorney regarding an obligation to refrain from mining for metadata or dumpster-diving and to return any data discovered in this fashion despite findings by other jurisdictions to the contrary, the 20/20 Commission continued the ABA's refusal to address and deter the behavior of employers—by increasing the ethical obligations on their attorneys—when they electronically dumpster-dive and obtain private and confidential data through forensics experts.[246] Only courts, legislatures, and attorney ethics committees can address employer electronic dumpster-diving for private and confidential employee emails and other electronic information given that the ABA has chosen to sidestep the matter in its rules and ethics opinions.

V. ASSUMING EXPECTATION OF PRIVACY AS A NEW PARADIGM

When an employer accesses ESI that an employee has placed in a mobile digital device provided to the employee by his or her own employer, concerns abound about whether the employer has invaded the employee's privacy.[247] Most employers use some form of an electronic communications policy as an attempt to circumvent the invasion of privacy legal concern by getting

---

243. *See* MODEL RULES OF PROF'L CONDUCT R. 4.4(b) (2012), *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_4_4_respect_for_rights_of_third_persons.html.

244. *See id.* cmt. 2, *available at* http://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_4_4_respect_for_rights_of_third_persons/comment_on_rule_4_4.html.

245. *See* 20/20 RESOLUTION, *supra* note 145, at 5–6.

246. *See* JAMIE S. GORELICK & MICHAEL TRAYNOR, ABA COMMISSION ON ETHICS 20/20, REPORT 105A 6 (2012), *available at* http://www.abanow.org/wordpress/wp-content/files_flutter/1340913956_31_1_1_9_resolution_summary.doc ("The new language about metadata [in comment 2 to Rule 4.4(b)] does not resolve a more controversial question: whether a lawyer should be permitted to look at metadata in the absence of consent or court authority to do so. . . . The Commission's proposal does not resolve this issue.").

247. *See* Zielinski, *supra* note 5, at 71–72 (describing legal concerns for employers related to employee personal use of electronic devices); Dave Zielinski, Editorial, *Don't Overlook Legal, Privacy Issues*, HR MAG., Feb. 2012, *available at* http://www.shrm.org/Publications/hrmagazine/EditorialContent/2012/0212/Pages/0212techa.aspx (describing legal problems including data confidentiality, security, and privacy issues); *see also* MATHIASON ET AL., *supra* note 136, at 8–9 (citing ETHICS RES. CTR., 2011 NATIONAL BUSINESS ETHICS SURVEY: WORKPLACE ETHICS IN TRANSITION 30 (2012), *available at* http://www.ethics.org/nbes/files/FinalNBES-web.pdf) (describing legal concerns for employers when employees merge their electronic devices for personal use with work use and how expectations of privacy and the moral attitudes of workers change regarding use of those devices depending on whether they are more frequent users of social media).

employees to consent to any invasions that may occur and by purportedly removing their expectation of privacy by obtaining employee agreement that the electronic communications on the employer-provided devices are owned by the employer.[248] But, the employer may get into legal trouble by gathering ESI that the employee has left on an employer-provided device and using that information to access the employee's communications on private systems. For example, finding an employee's personal email address and password on a company computer and using that information to access the employee's private email suggests illegal and improper action.[249]

Instead of addressing employee expectations on a case-by-case basis—as the *Ortega* plurality suggests—for Fourth Amendment matters, courts, legislatures, and attorney ethics committees should adopt a general understanding about an employee's expectation of privacy in email communications.[250] This understanding assumes that if employers provide employees with mobile, electronic devices and expect those employees to use those devices while outside the workplace, employees will expect to also make some private communications on those devices.[251] As *Quon* suggests, employers cannot just rely on clearly defined policies; they must also consistently apply those policies.[252] The façade effectuated by adhesion policies—regarding device use—that attempt to suggest employees have no expectation of privacy in communications found on employer devices and have also consented to

---

248. *See Computer Software Tracking and Counting Keystrokes—Do They Violate Employee Privacy Rights?*, EMP'T L. UPDATE (Rutkowski & Associates Inc., Evansville, Ind.), Dec. 2011, at 4, *available at* Westlaw, 25 No. 12 EMP. L. UPDATE 4 (2011); *see also* Zielinski, *supra* note 247 (advising employers to use an electronic communication policy to circumvent privacy issues).

249. Peerce & Shapiro, *supra* note 32, at 16–17 (citing Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 552–56 (S.D.N.Y. 2008); Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 656–64 (N.J. 2010)). In *Pure Power Boot Camp*, the United States District Court for the Southern District of New York found that an employer's access of a former employee's private email by using a password left on employer's computer and use of that information to access the former employee's personal email, as well as his email at his new place of employment, was a violation of the SCA. *Pure Power Boot Camp*, 587 F. Supp. 2d at 556. Likewise, in *Stengart*, the Supreme Court of New Jersey found that a privilege violation resulted when the employer's attorney reviewed cached web pages of the former employee's communications with her attorney on her personal email account, which were left on the employer's computer, and that the employee had a reasonable expectation of privacy in those communications. *Stengart*, 990 A.2d at 663.

250. This approach adheres to the conclusion that Justice Scalia reached in the first step of his analysis as described in his opinion in *Ortega*. O'Connor v. Ortega, 480 U.S. 709, 732 (1987) (Scalia, J., concurring in judgment).

251. *See* Philip M. Berkowitz, *Legal Challenges Arise to 'Bring Your Own Device' Policies*, N.Y. L.J., July 12, 2012, at 4 (describing how many employers "have adopted formal policies that permit employees to use their personal mobile devices to create, store, and transmit work-related data"); *see also* MATHIASON ET AL., *supra* note 136, at 6–7 (referring to a cost–benefit approach that has led many employers to allow employees to use their personal devices at work).

252. *See* Justin Conforti, Comment, *Somebody's Watching Me: Workplace Privacy Interests, Technology Surveillance, and the Ninth Circuit's Misapplication of the* Ortega *Test in* Quon v. Arch Wireless, 5 SETON HALL CIRCUIT REV. 461, 485 (2009).

employer searches for employee communications found on those devices as a legal paradigm should now be clearly rejected. In following the approach of Justice Scalia in *Ortega*, the legal paradigm applicable to this analysis should represent a categorical acceptance of the employee's expectation of privacy in email communications even if made and found on employer-provided devices.[253] This understanding should apply in both constitutional and private sector analysis. Then the real analysis can focus on whether the intrusion into the private aspects and information that an employee may reasonably expect to be kept private is a reasonable intrusion under the circumstances. Although the question of what framework should be employed to address the reasonableness of any employer intrusion upon employee expectations of privacy in email communications found on employer-provided devices is beyond the scope of this Article, employer intrusions conducted to investigate sexual harassment claims or determine appropriate costs in using devices, when narrowly tailored, would appear to be reasonable intrusions. On the other hand, employer attempts to access private communications, stored on employer-provided equipment, to advance a position in a lawsuit would not appear to be reasonable intrusions.

Using *Stengart* as the template for defining the expectation of privacy, courts can apply a broad acceptance of employee expectations of privacy when analyzing communications from employees on employer-provided mobile devices.[254] As a result, the analysis of cases involving privacy expectations can focus on whether the employer's actions in intruding upon the employee's privacy expectations were reasonable.[255] Any employee will certainly be concerned about the consequences of using a digital device provided by an employer. These employees will also be concerned about whether they can try to keep communications made on that device private and confidential.[256] Merging privacy protections for public employees and private employees into a

253. *See, e.g.*, *id.* at 474, 491 (citing *Ortega*, 480 U.S. at 729–30 (Scalia, J., concurring in judgment)) (referring to case-by-case approach in *Ortega*'s plurality and rejection of Scalia's categorical approach as a methodology that courts have applied to allow employers to diminish employees' privacy rights). A categorical acceptance of an expectation of privacy that cannot be diminished through a device-use policy would not preclude a finding that an expectation of privacy in a particular case was not reasonable on other grounds, such as when communications involve a tort. *See, e.g.*, CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997) (finding that unauthorized and unsolicited email communications constituted the tort of trespass to chattels by damaging the reputation and goodwill of a business with its customers).

254. *See* Brabham, *supra* note 80, at 1020 (citing Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010)) (asserting that *Stengart* represented a more expansive treatment of employee expectations of privacy than had generally been applied in the courts).

255. *Id.* at 1017 (citing City of Ontario v. Quon, 130 S. Ct. 2619, 2630 (2010)) (referring to how the Court in *Quon* sidestepped the reasonable expectation of privacy issue by focusing on the narrower issue of whether the police department had a legitimate business interest in reviewing the employee's text messages).

256. *See* Joseph O. Oluwole, *Teacher Cell Phone Searches in Light of* Ontario v. Quon, 17 RICH. J.L. & TECH. 6, at 21–22 (2010), http://jolt.richmond.edu/v17i2/article6.pdf (discussing privacy concerns of teachers who have been issued cell phones by their school district employers).

coherent paradigm would also represent an important step in the advancement of technology and privacy in the workplace.[257]

VI. CONCLUSION: EMPLOYEE PRIVACY IN COMMUNICATIONS ON EMPLOYER-PROVIDED DEVICES MUST FOCUS ON EMPLOYER REASONABLENESS INSTEAD OF EMPLOYEE EXPECTATIONS

This Article has focused on identifying employees' reasonable expectations of privacy when making personal and private communications even though they are stored on an employer-provided electronic device. The mobile nature of these devices encourages an increasing merger of work-related and private communications. Some employers have started to understand and accept the reality that use of these devices will lead to employees making personal communications that they expect will remain private.

However, the current legal paradigm allows an employer to remove any expectation of privacy or create an assumption that employees have consented to any intrusion by an employer in scenarios where the employer has established a clear policy notifying the employee that the employer may review the information. Unfortunately, that paradigm does not comport with the realities of the increasingly digital workplace. Instead of getting bogged down by the stilted and unrealistic assumption that employees have no expectation of privacy even in an email communication to their own attorneys, the analysis should focus on whether employers in a particular situation had a legitimate reason to access the email information and whether they utilized that access in a reasonable fashion. Attorney–client-privilege analysis has suggested a new paradigm where after the employer and its attorney recognize that an email communication is intended as a private and confidential communication, such as a communication to the employee's attorney, the employer should not be able to use the communication unless a court determines the communication was not privileged and confidential.

Most cases, from a constitutional analysis of the Fourth Amendment to an analysis of statutes and common law invasion of privacy torts, permit an employer to access its own digital equipment without liability when acting reasonably. Accordingly, reasonable employer intrusions are always protected, even if the circumstances suggest an employee clearly had a reasonable expectation of privacy in information stored on an employer's electronic device. The law should not encourage an employer to dumpster-dive for electronic communications obviously intended to be confidential and private communications under the guise of asserting that employee privacy rights have been subsumed by the mandates of employer policies. Given the realities of the

257. *See* Laura B. Pincus & Clayton Trotter, *The Disparity Between Public and Private Sector Employee Privacy Protections: A Call for Legitimate Privacy Rights for Private Sector Workers*, 33 AM. BUS. L.J. 51, 81–82 (1995).

digital workplace, the new paradigm should also include an expansion of ethics law to place obligations on employers and their attorneys to disregard these communications and return them immediately to employees, absent a court finding to the contrary.

Using the development of attorney–client-privilege analysis as a tool to address the growing merger of private and work-related communications on employer-provided devices supports the approach of assuming that employees still have reasonable expectations of privacy regarding information left on these devices. Broadly applying this approach will remove the current paradigm and the assertion of the resulting sham that employees have actually consented when an employer imposes, as a condition of employment, the obligation to let an employer search digital devices and acknowledge that the employer owns all information on that device.

Instead, the analysis of privacy protections in the workplace should presume reasonable intent and expectations of the employee, as occurs with attorney–client-privilege analysis. This analysis assumes, as a matter of law, that employees would not leave private communications on their employer-provided electronic devices without having some expectation of privacy in those communications. Then, the focus of the analysis would shift to whether the employer's actions in accessing and reviewing private, non-work-related information, left by an employee on an employer-provided device, was reasonable and necessary under the circumstances. The assumption would be that such an intrusion would not be reasonable simply because the employer required the employee to agree to a computer-use policy that grants the employer the authority to make the intrusion. Therefore, an employer would not be so easily encouraged to dumpster-dive for private and confidential employee communications embedded on employer-provided devices. The expansive demands of technological innovations and the increasing expectation that an employee be available to communicate through these employer-provided devices as a job duty supports the general expectation that employees will also use those devices to make personal and private communications.

Furthermore, incorporating attorney–client-privilege analysis only helps to support the expansive nature of employee communications made through these devices. Recent ABA ethics opinions represent a new privacy hurdle to overcome. These opinions place additional burdens on an employee's attorney to protect against employer mining of the data while making it more advantageous for the employer and the employer's counsel to dumpster-dive for this information. As a result, states, legislatures, and their attorney ethics committees must adopt a new paradigm that recognizes an expectation of privacy and confidentiality in emails to attorneys even when found on, or made with, employer-provided devices.

In concluding, it is helpful to return to the scenario discussed at the beginning of the Article where Bobbi has made email communications to an

attorney who represents her in an arbitration involving sexual harassment charges against her supervisor.[258] In *Holmes*, the California appellate court suggested an employee's email communications to an attorney on the employer's computer were analogous to an employee meeting with her attorney in one of the employer's conference rooms.[259] That part of the *Holmes* analogy works well for Bobbi, who will likely use her employer's conference room to meet with her attorney as she is still employed there and her attorney is representing her in an arbitration proceeding in which her employer might even be paying her attorney's fees.[260]

Unlike the hyperbole used in applying the conference room analogy in *Holmes*, which suggested that the employee had opened the door to the employer's conference room and yelled when communicating via email on the employer's computer, a more realistic application of the conference room analogy should be employed. When an employee must constantly be available to communicate via email, through employer-provided computers and other electronic devices, and the employee uses the employer's conference room (analogous to the employer-provided electronic device) for both work-related and private communications, the conference room could be viewed as having a glass window where the employer can certainly see into the room. In looking through that conference room window, the employer can clearly see that the employee is communicating with her attorney. Similarly, when analogizing the electronic device to the conference room, upon viewing titles and an overview of electronic file information, the employer can clearly see what information is not work-related and involves private, personal, and even attorney–client-privileged communications.

Also, if desired, the employer could attempt to listen to what the employee is communicating to her attorney inside the conference room, whether it is yelled or not. But when the employer sees through the window (the title of messages, to whom the messages are addressed, whether an attorney is involved in the communication, or if a privilege is identified) and realizes that the employee is meeting with her own attorney in that conference room, the employer will know

---

258. *See supra* Part I.

259. *See* Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 896 (Ct. App. 2011) (finding that Holmes was aware that the employer-provided computer was not private and was accessible to her employer, and by still using the computer to communicate with her attorney, her actions were "akin to consulting her attorney in one of defendants' conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard [by the employer] would be privileged").

260. It may appear unusual to suggest that an employer would enter into an agreement with an employee to arbitrate any disputes while also funding the employee's legal counsel, but a number of companies do agree to these transactions. *See, e.g.*, Michael Z. Green, *Ethical Incentives for Employers in Adopting Legal Service Plans to Handle Employment Disputes*, 44 BRANDEIS L.J. 395, 409–13 & n.105 (2006) (describing a specific legal service plan that was offered to employees to obtain legal counsel for arbitration proceedings and referring to other companies providing for such an arrangement).

that those communications are private, confidential, and privileged. The law should not encourage the employer to spy or electronically dumpster dive to mine for email information that the employer would normally not be allowed to use because it is clearly intended to be private and confidential.[261]

Further, the employer will know that although it might be able to stand near the door of the conference room and listen to those communications, the employer's attorney has an ethical obligation to not listen to those communications when it knows they are privileged and protected. Bobbi is not opening the door to that conference room; nor is she yelling. She is merely using the employer's conference room to have her private communication with her attorney. The realities of the current digital workplace provide Bobbi with little opportunity to communicate with her lawyer or have sufficient private communications off the employer's premises—without using the employer-provided digital device.

By applying the conference room analogy in this way, the analysis of Bobbi's problem at the beginning of this Article will shift to a focus on whether it was reasonable for the employer to extract the communications sent to her attorney from the employer-provided laptop. The question of whether Bobbi had a reasonable expectation of privacy will not arise because that expectation is presumed within the analytical paradigm asserted in this Article. By accomplishing this shift in the analysis, the dispute will center on the realities of the digital workplace and not on an employer-induced removal of an expectation of privacy through an Internet communication or employer-provided-device usage policy.

Consequently, employers will be limited in their insistence that employees use employer-provided devices to communicate at all times while also mandating successfully that none of the employees' communications can be protected as private. Under this analysis, employers will no longer be encouraged to dumpster-dive for confidential and private employee email communications on an employer-provided device once a dispute arises. As soon as the employer can clearly see that the communications were intended to be private and confidential, such as emails to an attorney, and there is no reasonable justification to intrude upon the privacy of the employee or to assert that the employee waived any privacy expectations, the employer must refrain from using an employee's private email communications.

---

261. *See* Wingo, *supra* note 13, at 215 ("Because dumpster diving is an unethical and destructive practice, [the] owners [of the information] should not be abandoned to protect themselves exclusively through security measures such as guards, electronic surveillance and paper shredders[, as this abandonment and focus on one's own private protection] is the moral equivalent of abandoning homeowners to private protection against burglary. Society should make the moral statement that dumpster diving is wrong and will not be tolerated . . . .").