

CLICKING AWAY CONFIDENTIALITY: WORKPLACE WAIVER  
OF ATTORNEY-CLIENT PRIVILEGE

*Adam C. Losey\**

I.	INTRODUCTION: BARBARA HALL AND HER DAUGHTERS . . .	1180
II.	THE EVOLUTION OF ATTORNEY-CLIENT PRIVILEGE . . . . .	1185
	A. <i>The Traditional Approach</i> . . . . .	1185
	B. <i>The Modern Approach</i> . . . . .	1185
	C. <i>Possible Chilling Effects</i> . . . . .	1187
	D. <i>Intersection with the Work Product Doctrine</i> . . . . .	1189
III.	CHAOS IN THE COURTS . . . . .	1190
	A. <i>The Employer's Policies Regarding Computer Use         and Monitoring</i> . . . . .	1191
	B. <i>Employee Use of a Password-Protected E-mail         Account</i> . . . . .	1193
	C. <i>Common Usage of Personal E-mail on Company         Computers</i> . . . . .	1194
	D. <i>Employee Attempts to Delete Privileged Material</i> . . . . .	1195
	E. <i>Employer Enforcement of any Existing Policies</i> . . . . .	1196
	F. <i>The Location of the Computer</i> . . . . .	1197
	G. <i>The Forensic Method Used to View an Employee's         E-mails</i> . . . . .	1198
	H. <i>Fairness and Public Policy</i> . . . . .	1199
IV.	MAKING SENSE OF IT ALL . . . . .	1201
	A. <i>The Knowledge Gap</i> . . . . .	1201
	B. <i>Modern vs. Traditional Approach to Attorney-Client         Privilege</i> . . . . .	1202
V.	THE WORKPLACE WAIVER PRESUMPTION . . . . .	1202
	A. <i>The Bright-Line Fallacy</i> . . . . .	1202
	B. <i>Distillation of Logically Pertinent Variables</i> . . . . .	1203
VI.	CONCLUSION: ADOPTION OF THE WORKPLACE WAIVER PRESUMPTION . . . . .	1204

---

\* J.D. expected May 2009, University of Florida College of Law. For my mother and father, whom I love and admire more than any other two people in the world, and whose wisdom, guidance, and many sacrifices made everything possible for me. Thanks also to the editorial staff of the *Florida Law Review* for all their hard work.

## I. INTRODUCTION: BARBARA HALL AND HER DAUGHTERS

Barbara Hall, an administrative assistant, often arrives at work an hour and a half early solely to check her personal e-mails<sup>1</sup> on her employer's computer.<sup>2</sup> Afterwards, "[i]n the grand tradition of Chekhov, or perhaps 'Days of Our Lives,' Barbara Hall carries on a dialogue throughout the workday with her two daughters, both of whom work at an event-planning company in Cleveland and use its e-mail system for such exchanges."<sup>3</sup> When she gets home from work, Barbara continues to use her workplace e-mail account to send personal e-mails.<sup>4</sup>

Barbara Hall and her daughters are not alone. The average employee is estimated to spend nearly an hour a day on personal Internet use.<sup>5</sup> While this behavior at work may be economically detrimental,<sup>6</sup> "[v]ery few companies today have a rule against all personal use of electronic communication . . . . Employers are becoming more realistic about people's need to send an occasional personal message from work."<sup>7</sup> Few companies will fire an employee solely for sending a personal e-mail from

1. "The abbreviated version of 'electronic mail' has been written as 'email,' 'Email,' or 'E-mail'" yet "dictionaries have not taken a position" on which abbreviation is correct. Elaine R. Firestone & Stanford B. Hooker, *Careful Scientific Writing: A Guide for the Nitpicker, the Novice, and the Nervous*, 48 SOC'Y FOR TECH. COMM. 505, 506 (2001). The Supreme Court has repeatedly used both "email" and "e-mail" within the same opinion. See *United States v. Williams*, 128 S. Ct. 1830, 1845 (2008) (using email and e-mail interchangeably); compare *Fed. Election Comm'n v. Wis. Right to Life, Inc.*, 127 S. Ct. 2652, 2669 (2007) (using email), with *id.* at 2698 (using e-mail). "Newly coined nonce words of English are often spelled with a hyphen, but the hyphen disappears when the words become widely used. For example, people used to write 'non-zero' and 'soft-ware' instead of 'nonzero' and 'software'; the same trend has occurred for hundreds of other words. Thus it's high time for everybody to stop using the archaic spelling 'e-mail.'" Donald E. Knuth, Email (let's drop the hyphen), <http://www-cs-faculty.stanford.edu/~knuth/email.html> (last visited Sept. 27, 2008).

2. Katie Hafner, *Putting All Your E-Mail in One Basket*, N.Y. TIMES, June 26, 2003, at G1.

3. *Id.*

4. "'I don't even bother with my home account any more,' [Barbara] said. 'When I'm home, I log onto the work e-mail because everyone has my work e-mail address. It's just easier.'" *Id.*

5. *Is That Work Related?*, 24 NO. 5 LEGAL MGMT., Sept.–Oct. 2005, at 8, 8.

6. "It's estimated that 'cyberslacking' is responsible for up to a 40% loss in employee productivity and can waste up to 60% of a company's bandwidth!" Jay P. Kesan, *Cyber-Working or Cyber-Shirking?: A First Principles Examination of Electronic Privacy in the Workplace*, 54 FLA. L. REV. 289, 290 (2002).

7. Larry Keller, *Monitoring Employees: Eyes in the Workplace*, CNN.com, Jan. 2, 2001, <http://archives.cnn.com/2001/CAREER/trends/01/02/surveillance/>; see also Nathan Watson, Note, *The Private Workplace and the Proposed "Notice of Electronic Monitoring Act": Is "Notice" Enough?*, 54 FED. COMM. L.J. 79, 96 (2001) ("Many people take care of personal business on company time and, for the most part, many employers do not mind this behavior as long as it is within reason.").

work,<sup>8</sup> and the modern corporate attitude toward personal e-mail in the workplace is one of begrudged tolerance coupled with surveillance.<sup>9</sup>

From 1996 to 2006, the percentage of employers monitoring of employee Internet use skyrocketed by more than 45%.<sup>10</sup> As of 2006, 80% of employers regularly monitor employee Internet use.<sup>11</sup> “[Employer computer] monitoring takes various forms, with 36% of employers tracking content, keystrokes, and time spent at the keyboard. Another 50% store and review employees’ computer files. Companies also keep an eye on e-mail, with 55% retaining and reviewing messages.”<sup>12</sup> While an estimated 90% of companies that monitor employee communications notify their employees about the possibility of monitoring,<sup>13</sup> many employees are oblivious to the fact that a permanent record may exist of their Internet and e-mail use at work.<sup>14</sup>

This ignorance has resulted in serious consequences for employee litigants. At risk are the communications between attorney and client that have been extended special legal protections throughout history.<sup>15</sup> This Note discusses workplace monitoring of these privileged communications.

---

8. However, many companies are firing employees for e-mail misuse. “Increasingly, employers are fighting back by firing workers who violate computer privileges. Fully 26% of employers have terminated employees for e-mail misuse.” 2006 AMA Survey: Workplace E-Mail, Instant Messaging & Blog Survey; *see also* Kim Zetter, *Employers Crack Down on Personal Net Use*, PC WORLD, Aug. 25, 2006, *available at* <http://www.pcworld.com/article/id,126835/article.html>.

9. “[W]hile [companies] may not fire people for sending personal e-mail messages, they keep reading them.” Keller, *supra* note 7.

10. Ericka Chickowski, *Monitoring Employee Internet Usage*, PROCESSOR, Apr. 14, 2006, at 29, 29.

11. *Id.*

12. 2005 AMA Survey: Electronic Monitoring & Surveillance Survey.

13. Kyle Schurman, *E-mail & Your Legal Rights*, SMART COMPUTING, July 2001, at 140, 140–41.

14. “‘Many people are unaware that a permanent record exists of their Internet and e-mail use at work,’ says Max Messmer, Chairman of Accountemps. ‘Most organizations actively monitor Web use by employees to ensure it complies with established corporate policy.’” *Is That Work Related?*, *supra* note 5, at 8.

15. *See* Max Radin, *The Privilege of Confidential Communication Between Lawyer and Client*, 16 CAL. L. REV. 487, 488 (1927–1928) (“Advocates equally from very ancient times could not be called as witnesses against their clients while the case was in progress. Cicero in prosecuting the Roman governor of Sicily regrets that he cannot summon the latter’s *patronus*, Hortensius . . . .”); Ken M. Zeidner, Note, *Inadvertent Disclosure and the Attorney-Client Privilege: Looking to the Work-Product Doctrine for Guidance*, 22 CARDOZO L. REV. 1315, 1320 (2001) (“The notion that an attorney may not give testimony against his client is deeply rooted in Roman law.”).

Generally, American<sup>16</sup> courts have held that employers are free to monitor<sup>17</sup> employee computer use,<sup>18</sup> and even government employers and supervisors can monitor employee computer usage without probable cause.<sup>19</sup> Accordingly, employees who e-mail an attorney from the workplace, or from a workplace e-mail account,<sup>20</sup> often lose the evidentiary protections of attorney-client privilege.<sup>21</sup> This loss of privilege subsequently allows an employer to forensically recover<sup>22</sup> a current or former employee's otherwise privileged e-mails to use against the employee in litigation.<sup>23</sup> This disclosure is particularly devastating to the employee, as these types of e-mails are often damning.<sup>24</sup> The employee's

---

16. Most European employees enjoy greater workplace privacy protections than their American counterparts. *See generally* Kesan, *supra* note 6, at 307–11 (outlining workplace privacy protections in the United Kingdom, France, Germany, and Italy).

17. Or not to monitor. Employers choose to monitor their employees for a variety of reasons, but it should be noted that they normally need not do so. *See, e.g.*, *Doe v. XYZ Corp.*, 887 A.2d 1156, 1162 (N.J. Super. Ct. App. Div. 2005) (“The duty to monitor employee’s internet activities does not exist.”).

18. For a critical discussion of employer-employee privacy law in the United States, see generally Rafael Gely, *Distilling the Essence of Contract Terms: An Anti-Antiformalist Approach to Contract and Employment Law*, 53 FLA. L. REV. 669 (2001), which criticizes “[t]he argument, which according to employers has become a truism, . . . [that] since employers ‘buy’ the time of employees, employers presumptively have the right to control all aspects of the employees’ life while at work, and at times even outside of work.”

19. *See United States v. LeBlanc*, 490 F.3d 361, 365 (5th Cir. 2007) (noting that the Supreme Court has held that “government employers and supervisors may conduct warrantless, work-related searches of employees’ desks and offices without probable cause . . .”).

20. “[S]ending a message over [a company’s] e-mail system [is] like placing a copy of that message in the company files.” *In re Asia Global Crossing, Ltd.*, 322 B.R. 247, 259 (Bankr. S.D.N.Y. 2005).

21. When a federal question is being litigated in the federal courts, the attorney-client privilege is a question of federal common law. *See* FED. R. EVID. 501. When a claim or defense is governed by state law (*e.g.*, in a diversity action) state privilege law is applicable. *Id.* For the purposes of this Note, due to the sparsity of case law on the subject, cases from all jurisdictions will be similarly considered.

22. Computer forensics is defined as “the art and science of applying computer science to aid the legal process.” CHRISTOPHER L.T. BROWN, *COMPUTER EVIDENCE: COLLECTION AND PRESERVATION* 3 (2006). “The primary focus of many computer forensics investigations is the extraction of digital evidence . . .” *Id.* at 127. Deleting an e-mail, or a file, generally does not make it inaccessible to a skilled computer forensics expert. For the purposes of this Note, the reader need be aware that if the user of a computer views or composes an e-mail, a forensic expert may be able to recover the e-mail regardless of whether the e-mail was intentionally saved on the computer.

23. *See* FED. R. EVID. 801(d)(2)(A) (stating the party admission exemption to the definition of hearsay).

24. Good examples of the types of communications involved in workplace waiver cases are

(1) a draft memorandum from Plaintiff to [a corporate officer], prepared by Plaintiff and her counsel; (2) a ‘chronology of events’ describing events

lawyer may even be vulnerable to a malpractice lawsuit for failing to advise the employee on how to take precautions to avoid waiver.<sup>25</sup>

The typical workplace waiver situation involves an employee, using an employer-owned computer, communicating with an attorney regarding an action adverse to the employer.<sup>26</sup> The employer usually has some sort of written policy providing notice to employees that their computer use is subject to monitoring.<sup>27</sup>

---

underlying many of Plaintiff's claims, prepared by Plaintiff and her counsel; (3) drafts of Plaintiff's EEOC complaint prepared by Plaintiff and her counsel; and (4) various e-mails sent amongst Plaintiff and her counsel.

*Curto v. Med. World Commc'ns, Inc.*, No. 03-CV-6327, 2006 WL 1318387, at \*2 (E.D.N.Y. May 15, 2006).

25. See Audrey Rogers, *New Insights on Waiver and the Inadvertent Disclosure of Privileged Materials: Attorney Responsibility as the Governing Precept*, 47 FLA. L. REV. 159, 189 & n.160 (1995).

26. See, e.g., *Long v. Marubeni Am. Corp.*, No. 05-Civ.-639, 2006 WL 2998671, at \*1 (S.D.N.Y. Oct. 19, 2006) (describing employees Kevin Long and Ludvic Presto using their employer's computers "that were issued to them to perform their respective work assignments, to send and receive e-mail messages to each other and to their attorney" regarding a civil rights action against their employer); *Curto*, 2006 WL 1318387, at \*1-2 (noting that employee Curto used an assigned company-owned laptop to frequently e-mail her attorney concerning an EEOC complaint against her employer); *Kaufman v. SunGard Inv. Sys.*, No. 05-CV-1236, 2006 WL 1307882, at \*1 (D.N.J. May 10, 2006) ("Kaufman and OSI, a financial software company owned by Kaufman, initiated suit action against SunGard, alleging, among other claims, breach of contract in connection with SunGard's acquisition of OSI's assets and hiring of Kaufman as a senior executive . . . [E-mails related to the litigation] were sent from and received on SunGard's e-mail system during Kaufman's employment with SunGard."); *Nat'l Econ. Research Assocs. v. Evans*, No. 04-2618-BLS2, 2006 WL 2440008, at \*1 (Mass. Super. Ct. Aug. 3, 2006) (using his employer's computer, employee Evans contacted an attorney for advice regarding his leaving the company and working with a competitor); *Banks v. Mario Indus. of Va., Inc.*, 650 S.E.2d 687, 695 (Va. 2007) (describing how employee Cook used his employer's computer to prepare, print, and delete a privileged document to send to his attorney regarding legal action adverse to his employer).

27. See, e.g., *Long*, 2006 WL 2998671, at \*1 (noting that the employee handbook stated that personal use of company computers was prohibited, and that employees "'have no right of personal privacy in any matter stored in, created, received, or sent over the e-mail, voice mail, word processing, and /or internet systems provided' by [the employer]"); *Curto*, 2006 WL 1318387, at \*1 ("Employees should not have an expectation of privacy in anything they create, store, send, or receive on the computer system. The computer system belongs to the company and may be used only for business purposes. Employees expressly waive any right of privacy in anything they create, store, send, or receive on the computer or through the Internet or any other computer network. Employees consent to allowing personnel of [MWC] to access and review all materials employees create, store, send, or receive on the computer or through the Internet or any computer network. Employees understand that [MWC] may use human or automated means to monitor use of computer resources."); *Kaufman*, 2006 WL 1307882, at \*4 ("SunGard policy . . . provided that all emails were subject to monitoring. SunGard warned: The Company has the right to access and inspect all electronic systems and physical property belonging to it. Employees should not expect that any items created with, stored on, or stored within Company property will remain private. This

In these workplace waiver cases, a schism is quietly developing. Some courts are discreetly (and perhaps inadvertently) abandoning the traditionally accepted narrow interpretation of attorney-client privilege in favor of a broad protective approach on public policy grounds. Others continue to adhere to traditional doctrine. A clash between these two schools of thought may be inevitable. The universal application of a rebuttable presumption that an employee has waived attorney-client privilege could avert a direct collision between these two schools of thought and establish a semblance of predictability in workplace waiver cases.

Part II points out the growing and unspoken abandonment of traditional approaches in these non-traditional cases. Part III describes the hodgepodge of emerging case law on the subject. Part IV attempts to identify the underlying source of difficulty in these abstruse cases. Part V teases the logically pertinent variables out of existing case law, and uses these variables as building blocks to construct a workplace waiver presumption. Finally, Part VI advocates the universal adoption of this workplace waiver presumption.

Barbara Hall's e-mail conversations with her daughters "range from the mundane business of trading recipes to the more textured landscape of family illness and romantic relationships[,]""<sup>28</sup> and would not be protected by attorney-client privilege.<sup>29</sup> Yet, Barbara might be surprised to learn that if she were to e-mail an attorney to ask if she might be fired for sending personal e-mails on company time,<sup>30</sup> her otherwise privileged e-mail could likely be used against her by her employer in any future litigation.<sup>31</sup> She would then find herself out of work, and finally forced to use a personal e-mail account for personal e-mail.

---

includes desk drawers, even if protected with a lock; and computer files and electronic mail, even if protected with a password."); *Evans*, 2006 WL 2440008, at \*2-3 (listing a series of provisions in the employer's policies and procedures manual stating that employee e-mails are subject to monitoring); *Banks*, 650 S.E.2d at 695 (noting that the "employee handbook provided that there was no expectation of privacy regarding [company computers]").

28. Hafner, *supra* note 2.

29. Unless, of course, one or both of her daughters happened to be an attorney, and Barbara contacted that daughter for legal advice.

30. To which the attorney should respond "yes." See *supra* note 8. If the attorney Barbara consulted was also her husband, she might also be able to seek the protections of the spousal privilege. See *Sprenger v. Rector & Bd. of Visitors of Va. Tech.*, 2008 WL 2465236, at \*2-3 (W.D. Va. June 17, 2008) (discussing employee spousal privilege in the workplace, and noting that "[t]he attorney-client privilege is similar to the [spousal] privilege").

31. See FED. R. EVID. 801(d)(2)(A) (stating the party admission exemption to the definition of hearsay).

## II. THE EVOLUTION OF ATTORNEY-CLIENT PRIVILEGE

### A. *The Traditional Approach*

Attorney-client privilege protects from discovery confidential communications made between an attorney and client for the purpose of obtaining legal assistance.<sup>32</sup> The purpose behind the attorney-client privilege is to “encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice.”<sup>33</sup>

Yet, as discovery is intended to be broad and inclusive,<sup>34</sup> the Supreme Court noted in 1947 that the “privilege limitation must be restricted to its narrowest bounds.”<sup>35</sup> In 1961, Professor Wigmore stated that

[the privilege’s] benefits are all indirect and speculative; its obstruction is plain and concrete . . . . It is worth preserving for the sake of a general policy, but it is nonetheless an obstacle to the investigation of the truth. It ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle.<sup>36</sup>

Thus, the traditional viewpoint is that when the privilege is in question “[a] court must balance the possibility that the privilege indirectly promotes free and honest communication with the policy of liberal discovery to enhance the search for truth[,]”<sup>37</sup> with the court’s thumb on the scale favoring waiver. In workplace waiver cases, application of the traditional approach involves balancing the possible chilling effect of admitting the employee’s communications against the truth-seeking value of the communications, while construing the privilege as narrowly as possible.

### B. *The Modern Approach*

When Wigmore and the Supreme Court originally advocated the narrow construction of attorney-client privilege, personal computers and

---

32. See Bryan S. Gowdy, Note, *Should the Federal Government Have an Attorney-Client Privilege?*, 51 FLA. L. REV. 695, 697 (1999) (citing Dean Wigmore’s definition of the attorney-client privilege).

33. *Upjohn Co. v. United States*, 449 U.S. 383, 389 (1981).

34. The Court often references “the broad discovery authorized by the Federal Rules of Civil Procedure . . . .” *Codd v. Velger*, 429 U.S. 624, 638 (1977).

35. *Hickman v. Taylor*, 329 U.S. 495, 506 (1947).

36. 8 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2291 (John T. McNaughton ed., rev. ed. 1961).

37. *Suburban Sew’N Sweep, Inc. v. Swiss-Bernina, Inc.*, 91 F.R.D. 254, 257 (N.D. Ill. 1981).

e-mail did not exist.<sup>38</sup> Technology has since revolutionized interpersonal communications,<sup>39</sup> and attorney-client communication now regularly occurs in a manner and form that would be completely alien to Wigmore. E-mail combines the accountability of a pen-and-ink letter with the convenience of a phone call.<sup>40</sup> It can be instantly accessed from a computer anywhere in the world, and it has forever blurred the line between formal correspondence and casual communication.

Hence, antiquated legal rubrics may not apply to modern legal questions involving e-mail. In an attempt to honor the policies behind attorney-client privilege, some courts have deemed it necessary to break with tradition and interpret the privilege broadly.<sup>41</sup> This broad interpretation has created a judicial bulwark protecting employees against what some judges view as an unfair practice by employers. If this broad interpretation is adopted in workplace waiver cases, employers would still be permitted to monitor employee communications, but they would be prevented from using these communications against an employee in litigation. Although no court has explicitly articulated this broadened approach, at least one court has undoubtedly adopted it.<sup>42</sup> Another court attempted to finesse the traditional approach through explanation, while the court's reasoning suggested application of the broad approach.<sup>43</sup>

This broad approach to attorney-client privilege is not unprecedented. "Historically, the attorney-client privilege subordinates the need for information to determine truth to the need for a sphere of

---

38. While e-mail has arguably been around since the late 1960s, e-mail did not exist in its modern form until 1972, when an engineer named Ray Tomlinson chose the "@" symbol for e-mail addresses and wrote software to send the first network e-mail. Barry M. Leiner et. al., *A Brief History of the Internet*, <http://arxiv.org/html/cs/9901011v1>.

39. See Stephen J. Snyder & Abigail E. Crouse, *Applying Rule 1 in the Information Age*, SEDONA CONF. J., Fall 2003, at 165, 167 ("Computers have revolutionized the way people live and do business . . . and email has revolutionized the way people communicate.").

40. Just as a phone call can be made from any phone hooked up to a telephone service provider, e-mail can be sent with ease from any computer in the world with an Internet connection and a web browser. There are approximately one billion such computers in the world today, and by 2015 that number will double. See Siobhan Chapman, *PC Numbers Set to Hit One Billion*, COMPUTERWORLDUK, June 12, 2007, <http://www.techworld.com/news/index.cfm?NewsID=9119>. As in correspondence by letter, a permanent record exists of an e-mail communication. Some argue that the existence of these two qualities in a single method of communication is risky, stating that "email is more like a dangerous power tool than like a harmless kitchen appliance [and] many, perhaps most, of us have suffered the equivalent of burns, lost fingers, electric shocks, and bone fractures." Janet Malcolm, *Pandora's Click*, N.Y. REV. OF BOOKS, Sept. 27, 2007, at 8, 8 (book review).

41. See, e.g., *Sims v. Lakeside Sch.*, No. C06-1412RSM, 2007 WL 2745367, at \*2 (W.D. Wash. Sept. 20, 2007) ("[P]ublic policy dictates that [privileged] communications shall be protected to preserve the sanctity of communications made in confidence.").

42. See *supra* note 41 and accompanying text.

43. See *In re Teleglobe Commc'ns Corp.*, 493 F.3d 345, 361 n.13 (3d Cir. 2007).

autonomy . . . .”<sup>44</sup> Courts have been slowly backing away from the traditional approach in certain situations since “the privilege carries through policy purposes—encouraging attorney-client communication to enhance compliance with the law and facilitating the administration of justice. . . .”<sup>45</sup>

### C. Possible Chilling Effects

If courts apply the traditional, narrow view of attorney-client privilege, it is unclear whether employees would be discouraged from speaking with counsel while at work. Nothing prevents an employee in the workplace or at home from communicating with an attorney on a personally owned computer,<sup>46</sup> or via another medium of communication.<sup>47</sup> Yet courts in workplace waiver cases have used the argument that “personal communications with attorneys were exchanged at the office out of necessity arising from the long business hours at [the employee’s workplace]”<sup>48</sup> to tie the exclusion of evidence to the purpose of the privilege. While one court ignored this argument for procedural reasons,<sup>49</sup> another court used essentially the same reasoning to justify its decision to protect privileged e-mails.<sup>50</sup>

It is clear that an overworked employee could bring a personal computer into work and e-mail his attorney from his personal e-mail

---

44. Bryan T. Camp, *Tax Administration as Inquisitorial Process and the Partial Paradigm Shift in the IRS Restructuring and Reform Act of 1998*, 56 FLA. L. REV. 1, 131 (2004).

45. *In re Teleglobe*, 493 F.3d at 360 (citation omitted).

46. This observation assumes that the employee owns a personal computer, and has Internet access. Approximately 90% of American families with an annual household income more than \$50,000 in 2003 owned a personal computer with an Internet connection. See U.S. Census Bureau, Computer and Internet Use in the United States: 2003, at 2 (2005), available at <http://www.census.gov/prod/2005pubs/p23-208.pdf>. This number has likely risen since 2003, and will continue to rise. See *supra* note 40. Because an employee consulting an attorney to obtain legal advice is likely to have an annual household income of more than \$50,000, the underlying assumption is reasonable.

47. Phone calls, letters, and face-to-face conversations are not yet antiquated to the point of obsolescence. Moreover, an employee could easily purchase and use a personally owned electronic device capable of sending and receiving e-mail, such as a BlackBerry or iPhone. Ample alternatives to e-mail remain for an employee to privately communicate with his or her attorney.

48. *Kaufman v. SunGard Inv. Sys.*, No. 05-CV-1236, 2006 WL 1307882, at \*4 (D.N.J. May 10, 2006).

49. *Id.*

50. See *Nat’l Econ. Research Assocs. v. Evans*, No. 04-2618-BLS2, 2006 WL 2440008, at \*5 (Mass. Super. Ct. Aug. 3, 2006) (“If [the employer’s] position were to prevail, it would be extremely difficult for company employees who travel on business to engage in privileged e-mailed conversations with their attorneys . . . . Pragmatically, a traveling employee could have privileged e-mail conversations with his attorney only by bringing two computers on the trip—the company’s and his own.”).

account,<sup>51</sup> or could pick up the telephone to speak with his attorney in lieu of sending an e-mail. It is not unusual for an employee to routinely bring a personal computer to work,<sup>52</sup> and some undoubtedly already use the telephone to communicate with their attorney while at work. Still, denying privilege in these cases could significantly chill attorney-client communication.

E-mail is particularly useful for legal communications,<sup>53</sup> and forcing an employee to bring a separate personal computer to work to ensure privacy would be burdensome to the employee and potentially still subject the employee to monitoring.<sup>54</sup> Further, allowing employers to use technologically sophisticated methods to covertly intercept attorney-client communications could allow the employer to fold the protections of privilege into a paper tiger.<sup>55</sup> If an employee's privileged communications with an attorney can be intercepted without the employee's knowledge and used against the employee, the employee has a strong incentive to avoid seeking legal advice. This is the chilling effect the privilege is designed to prevent.

---

51. However, bringing in a personal computer might not be enough to avoid employer surveillance, as the employee would likely be forced to use the employer's Internet connection or network to send e-mail. *See supra* note 20.

52. *See, e.g.*, *United States v. Barrows*, 481 F.3d 1246, 1247 (10th Cir. 2007) ("Mr. Barrows brought his personal computer to work."); *Gernady v. Pactiv Corp.*, No. 02-C-8113, 2005 WL 241472, at \*8 (N.D. Ill. Jan. 24, 2005) ("On January 22, 2001, Gernady brought his personal computer to work even though he had previously been notified that he was not allowed to do so."); *United States v. Murray*, No. NMCCA 200501175, 2007 WL 1704288, at \*1 (N.M. Ct. Crim. App. Jan. 11, 2007) ("The appellant sometimes brought his personal laptop computer to work so that he could listen to music while working."); *Am. Airlines, Inc. v. Geddes*, 960 So. 2d 830, 831 (Fla. 3d DCA 2007) ("The mechanics had begun bringing their personal computers from home, keeping them in a closet area near the break room where the mechanics await their work assignments.").

53. "According to the 2007 ABA Legal Technology Survey Report, more than 99 percent of the ABA members surveyed reported using email in their practices." Joshua Poje, *Sanctions Just a Click Away: Email's Ethical Pitfalls*, THE E-PUBLIC LAWYER, Summer 2008, <http://www.abanet.org/govpub/ePL/summer08/email.html>. However, there are some critics of e-mail. "E-mail is a party to which English teachers have not been invited . . . E-mail has just erupted like a weed, and instead of considering what to say when they write, people now just let thoughts drool out onto the screen[.]" Sam Dillon, *What Corporate America Cannot Build: A Sentence*, N.Y. TIMES, Dec. 7, 2004, at A23 (quoting R. Craig Hogan).

54. *See supra* note 51.

55. "[P]aper tigers [are] fierce in appearance but missing in tooth and claw." Bob Hepple, *Enforcement: The Law and Politics of Cooperation and Compliance*, in SOCIAL AND LABOUR RIGHTS IN A GLOBAL CONTEXT 238, 238 (Bob Hepple ed., 2002).

#### D. Intersection with the Work Product Doctrine

The work product doctrine,<sup>56</sup> now codified in the Federal Rules of Civil Procedure,<sup>57</sup> is derived from the Supreme Court's decision in *Hickman v. Taylor*.<sup>58</sup> The doctrine is distinct from and more expansive than attorney-client privilege.<sup>59</sup> "[I]n [a] civil context, work-product protection is not absolute, but is a 'qualified privilege or immunity'"<sup>60</sup> that protects documents and tangible things otherwise discoverable that are prepared in anticipation of litigation by a party or by the party's representative, unless opposing counsel demonstrates a need for its disclosure.<sup>61</sup>

"The work product doctrine reflects a policy that attorneys should be free to investigate all aspects of his client's case and devise strategy and tactics without the fear that such information can be obtained by opposing counsel through discovery."<sup>62</sup> As the policy rationale behind the work product doctrine differs from the rationale for attorney-client privilege, "[a] split of authority exists as to whether the work-product doctrine should be treated the same as the attorney-client privilege for waiver purposes."<sup>63</sup>

Because some courts treat waiver questions differently when viewed through the lens of attorney-client privilege or work product doctrine,<sup>64</sup> an employee's claim of work product protection might be stronger than the employee's attorney-client privilege claim in a workplace waiver situation.<sup>65</sup> In many cases involving employee waiver of attorney-client privilege, the employee has also claimed that the communications were protected by the work product doctrine.<sup>66</sup>

For example, Martha Stewart's forwarding of a privileged e-mail to her daughter was found to constitute waiver of attorney-client privilege, yet

---

56. Federal law governs issues concerning the work product doctrine in diversity cases in federal courts. *See, e.g.,* *Pyramid Controls, Inc. v. Siemens Indus. Automations, Inc.*, 176 F.R.D. 269, 276 (N.D. Ill. 1997).

57. *See* FED. R. CIV. P. 26(b)(3).

58. 329 U.S. 495, 514 (1947).

59. *See* *United States v. Nobles*, 422 U.S. 225, 238 n.11 (1975).

60. *United States v. Armstrong*, 517 U.S. 456, 474 (1996) (Breyer, J., concurring).

61. *See* FED. R. CIV. P. 26(b)(3).

62. *Rogers, supra* note 25, at 179 n.117.

63. *Id.*

64. *Id.* at 179–80 n.117.

65. This approach has not worked well for employee litigants to date. Generally, courts finding waiver or upholding attorney-client privilege reach the same result in their work product analysis. *See, e.g.,* *Long v. Marubeni Am. Corp.*, No. 05-Civ.-639, 2006 WL 2998671, at \*4 (S.D.N.Y. Oct. 19, 2006) (noting the employees waived attorney-client privilege and work product protections by voluntary disclosure); *Curto v. Med. World Commc'ns, Inc.*, No. 03-CV-6327, 2006 WL 1318387, at \*5–9 (E.D.N.Y. May 15, 2006) (concluding employee is entitled to either or both attorney-client privilege or work product doctrine protections for the same reasons).

66. *See, e.g.,* *Long*, 2006 WL 2998671, at \*2–5; *Curto*, 2006 WL 1318387, at \*2.

was still considered protected under the work product doctrine, because Stewart did not “substantially increase the risk that the Government would gain access to materials prepared in anticipation of litigation.”<sup>67</sup> However, in *Lynch v. Hamrick*,<sup>68</sup> Juanita Lynch’s privileged telephone conversations held in the presence of her daughter received no such protection through application of the work product doctrine.<sup>69</sup> The contrast between these cases illustrates how courts are particularly friendly to litigants who have made a technological blunder.

The *Stewart* court reasoned that, as “[d]isclosure to third persons in no way indicates a party’s intent to allow his adversary access to work product materials, waiver is therefore not warranted.”<sup>70</sup> This rationale could be extended to workplace waiver situations, especially when an employee attempts to remove traces of the privileged materials from the employer’s computer system. However, it is clear that the work product doctrine has taken a backseat to attorney-client privilege. To date, all courts addressing workplace waiver have simply lumped the two concepts together or given work product claims token consideration.<sup>71</sup>

### III. CHAOS IN THE COURTS

Courts have struggled in determining whether an employee waived attorney-client privilege by checking an otherwise privileged e-mail on a company computer.<sup>72</sup> The decisions center around whether the employee-client had an objectively reasonable expectation of privacy when communicating with an attorney.<sup>73</sup> Courts have generally taken a

---

67. *United States v. Stewart*, 287 F. Supp. 2d 461, 469 (S.D.N.Y. 2003).

68. 968 So. 2d 11 (Ala. 2007).

69. *Id.* at 14.

70. *Stewart*, 287 F. Supp. 2d at 469 (quoting Jeff A. Anderson et al., *The Work Product Doctrine*, 68 CORNELL L. REV. 760, 884 (1983)).

71. *See supra* note 65.

72. *Compare* *Long v. Marubeni Am. Corp.*, No. 05-Civ.-639, 2006 WL 2998671, at \*1-3 (S.D.N.Y. Oct. 19, 2006) (refusing to shield communications because employee waived privilege by checking e-mails on company computer), *and* *Kaufman v. SunGard Inv. Sys.*, No. 05-CV-1236, 2006 WL 1307882, at \*1-3 (D.N.J. May 10, 2006) (reasoning that although employee deleted privileged e-mails on company laptop that were later recovered by a computer technician, employee had waived privilege), *and* *Banks v. Mario Indus. of Va., Inc.*, 650 S.E.2d 687, 695-96 (Va. 2007) (preparing an otherwise privileged communication on a company computer waived the employee’s privilege), *with* *Sims v. Lakeside Sch.*, No. C06-1412RSM, 2007 WL 2745367, at \*2 (W.D. Wash. Sept. 20, 2007) (holding that public policy demanded that employee’s privileged communications be protected), *and* *Curto v. Med. World Commc’ns, Inc.*, No. 03-CV-6327, 2006 WL 1318387, at \*4-5 (E.D.N.Y. May 15, 2006) (concluding employee had not waived privilege by leaving traces of privileged e-mails on a company computer, although company policy stated all e-mails viewed on company computer were subject to monitoring), *and* *Nat’l Econ. Research Assocs. v. Evans*, No. 04-2618-BLS2, 2006 WL 2440008, at \*3-5 (Mass. Super. Ct. Aug. 3, 2006) (checking e-mail on company computer did not waive employee privilege).

73. The attorney-client privilege protects from disclosure those

fact-specific approach in determining the objective reasonableness of the employee's belief. The different variables that courts have considered will be discussed in the following subsections.

*A. The Employer's Policies Regarding Computer Use and Monitoring*

Every court addressing workplace waiver has first looked to the employer's policies<sup>74</sup> regarding employee computer use. Some courts have treated policy language indicating that an employee has no expectation of privacy on workplace computers to be a necessary condition to establish waiver, while others have found such language to be in itself sufficient to establish waiver.

An example of this "necessary and sufficient" approach can be seen in *Banks v. Mario Industries of Virginia, Inc.*,<sup>75</sup> in which an employee used an employer-owned computer to prepare a memorandum for his attorney regarding his planned resignation.<sup>76</sup> The employee printed the letter and sent it via non-electronic mail, and then single deleted<sup>77</sup> the electronic copy

---

communications from clients to their attorneys that were part of the clients' efforts to obtain legal advice or assistance. The communication must be confidential for the privilege to apply. A communication is confidential when (1) the client subjectively believes the communication is confidential and (2) that the belief is objectively reasonable.

PAUL R. RICE, *ELECTRONIC EVIDENCE: LAW AND PRACTICE* 132–33 (2005); *see also* *Bogle v. McClure*, 332 F.3d 1347, 1358 (11th Cir. 2003) ("To determine if a particular communication is confidential and protected by the attorney-client privilege, the privilege holder must prove the communication was '(1) intended to remain confidential and (2) under the circumstances was 'reasonably expected and understood to be confidential.'" (quoting *United States v. Bell*, 776 F.2d 965, 971 (11th Cir. 1985))); *United States v. Melvin*, 650 F.2d 641, 645 (5th Cir. 1981) ("A communication is protected by the attorney-client privilege . . . if it is intended to remain confidential and was made under such circumstances that it was reasonably expected and understood to be confidential.").

74. Most employers have some sort of written policy allowing the employer to monitor employee computer use. *See supra* note 27 and accompanying text. In the event that an employer had no such policy language, the lack of a policy would likely be determinative. *See* *Transocean Capital, Inc. v. Fortin*, No. 05-0955-BLS2, 2006 WL 3246401, at \*4 (Mass. Super. Ct. Oct. 20, 2006) (upholding privilege, noting that "[the employer] did not have its own Policies or Procedures Manual or Employment Manual setting forth the Company's policy regarding the review of emails on the Company's network").

75. 650 S.E.2d 687 (Va. 2007).

76. *Id.* at 695.

77. The term "deleted" has a legion of different meanings in the context of electronic discovery. Counter-intuitively, clicking "delete" on a computer file does not actually delete the file. It merely removes the computer's reference mark to the document. Thus, the term "single deleted" or "once deleted" should be used to refer to documents whose reference mark has been removed, and "double deleted" should be used to refer to documents that have actually been overwritten and truly been made inaccessible. *See* RALPH C. LOSEY, *E-DISCOVERY: CURRENT TRENDS AND CASES*

of the letter.<sup>78</sup> The employer later forensically recovered<sup>79</sup> the memorandum, and sought to use it as evidence against the employee.<sup>80</sup> The court held that since “[the employer’s] employee handbook provided that there was no expectation of privacy regarding [the employer’s] computers[,]” and “[the employee] created the pre-resignation memorandum on a work computer located at [the employer’s] office[,]”<sup>81</sup> *ipso facto* attorney-client privilege did not protect the deleted memorandum from discovery.<sup>82</sup>

Most courts, however, have followed a “necessary but not sufficient” approach. An example of this approach can be seen in *Scott v. Beth Israel Medical Center Inc.*<sup>83</sup> In *Scott*, a physician used his employer’s e-mail system to write several e-mails to his attorney regarding a suit against his employer for wrongful termination.<sup>84</sup> While the court found that the employee-physician had waived privilege,<sup>85</sup> it treated the presence of appropriate policy language<sup>86</sup> as an important factor in determining waiver.<sup>87</sup> The court based its decision primarily on the policy language, explaining that the employer’s e-mail policy meant, in effect, that the employer looked over the employee’s shoulder each time he sent an e-mail. Thus, the privileged e-mail could not have been sent in confidence.<sup>88</sup>

The weight given to this variable hinges on the court’s interpretation of the strength of the policy language. What constitutes sufficiently strong language depends largely on the surrounding circumstances. An employer’s blanket statement that an employee is not entitled to any expectation of privacy may be all that is needed in some situations.<sup>89</sup> Yet, in another situation, an employer may need to specifically describe the method used to monitor employees for the court to consider the language sufficient to establish waiver.<sup>90</sup>

---

192–93 (2008). It seems clear that the *Banks* court was referring to single deletion, which is arguably not a reasonable precaution taken to prevent the disclosure of a privileged document. See *Banks*, 650 S.E.2d at 695.

78. *Banks*, 650 S.E.2d at 695.

79. See *supra* note 22.

80. *Banks*, 650 S.E.2d at 695.

81. *Id.*

82. *Id.* at 695–96.

83. 2007 N.Y. Slip Op. 27429 (N.Y. Sup. Ct. Oct. 17, 2007).

84. *Id.* at \*1.

85. *Id.* at \*4–6.

86. For the full text of the policy language, see *id.* at \*2.

87. *Id.* at \*5.

88. *Id.* at \*3.

89. See *Banks v. Mario Indus. of Va.*, 650 S.E.2d 687, 695 (Va. 2007).

90. See discussion *infra* Part III.G.

### B. Employee Use of a Password-Protected E-mail Account

In workplace waiver cases, an employee will often use a personal password-protected e-mail account to e-mail counsel.<sup>91</sup> In *Curto v. Medical World Communications, Inc.*,<sup>92</sup> the Eastern District of New York considered the use of a password to be an appropriate factor in considering whether attorney-client privilege should protect employee data stored on an employer-owned computer.<sup>93</sup> In *National Economic Research Associates, Inc. v. Evans*,<sup>94</sup> the Superior Court of Massachusetts found the existence of a password to be a determinative factor.<sup>95</sup> A California appellate court reasoned that “[b]y proffering evidence that these electronic documents were password-protected and placed in a folder called ‘Attorney’ for the explicit purpose of protecting them from disclosure, defendant satisfied the initial evidentiary burden imposed on privilege claimants.”<sup>96</sup>

While these holdings seem to indicate that password protection equates to privacy, this generalization is not necessarily true. “[An employee] does not have an absolute expectation of privacy in records kept or accessed on his workplace computer, even if password protected.”<sup>97</sup> In *Long v.*

91. See, e.g., *Long v. Marubeni Am. Corp.*, No. 05-Civ.-639, 2006 WL 2998671, at \*1 (S.D.N.Y. Oct. 19, 2006) (“In [the employees’ communicating with their attorney on an employer-owned computer], the [employees] used private password-protected e-mail accounts.”); *Curto v. Med. World Commc’ns, Inc.*, No. 03-CV-6327, 2006 WL 1318387, at \*3 (E.D.N.Y. May 15, 2006) (“Plaintiff did take reasonable precautions to prevent inadvertent disclosure in that she sent the e-mails at issue through her personal AOL account which did not go through the Defendants’ servers.”); *Nat’l Econ. Research Assocs. v. Evans*, No. 04-2618-BLS2, 2006 WL 2440008, at \*1 (Mass. Super. Ct. Aug. 3, 2006) (“Many of these attorney-client communications were conducted by e-mail, with Evans sending and receiving e-mails from his personal, password-protected e-mail account with Yahoo rather than his NERA e-mail address.”). But see *Kaufman v. SunGard Inv. Sys.*, No. 05-CV-1236, 2006 WL 1307882, at \*1 (D.N.J. May 10, 2006) (“These e-mails [between Kaufman and her attorneys] were sent from and received on SunGard’s e-mail system during Kaufman’s employment with SunGard.”).

92. No. 03-CV-6327, 2006 WL 1318387 (E.D.N.Y. May 15, 2006).

93. *Id.* at \*5, \*8.

94. No. 04-2618-BLS2, 2006 WL 2440008 (Mass. Super. Ct. Aug. 3, 2006).

95. The Evans court stated that:

The bottom line is that, if an employer wishes to read an employee’s attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, not the company’s Intranet, the employer must plainly communicate [this] to the employee . . . .

*Id.* at \*5.

96. *People v. Jiang*, 31 Cal. Rptr. 3d 227 (Cal. Ct. App. 2005), *withdrawn* 33 Cal. Rptr. 3d 184, 203 (Cal. Ct. App. 2005)).

97. *Campbell v. Woodard Photographic, Inc.*, 433 F. Supp. 2d 857, 861 n.4 (N.D. Ohio

*Marubeni America Corporation*,<sup>98</sup> the Southern District of New York considered the use of a personal password-protected e-mail account to be irrelevant.<sup>99</sup> The court, referring to language in the employer's policy handbook, held that the employee's erroneous subjective belief that using a personal password-protected e-mail account equated to privacy was inconsequential.<sup>100</sup>

Where an employer has provided in its policies that an employee has no expectation of privacy while using an employer-owned computer,<sup>101</sup> it is unwise to give weight to an employee's erroneous subjective belief of privacy stemming from use of a personal password-protected e-mail account, as doing so would allow and encourage the employee to circumvent the employer's policies.<sup>102</sup> However, password protection may be relevant in analyzing work product claims.<sup>103</sup>

### C. Common Usage of Personal E-mail on Company Computers

In *Curto*, the court determined that widespread use of personal e-mail by various employees in the workplace had bearing on the objective reasonableness of an individual employee's expectation of privacy in using personal e-mail.<sup>104</sup> The court made a specific reference to the fact that "several other MWC employees, including its president, had personal [e-mail] accounts on their work computers."<sup>105</sup>

The fact that personal e-mail accounts are widely used in the workplace does not necessarily mean that those employees expected their communications to be private.<sup>106</sup> This inference of privacy from common

---

2006).

98. No. 05-Civ.-639, 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006).

99. "The plaintiffs contend they used their private password-protected e-mail accounts to communicate with their attorney, and with each other, to protect the confidentiality of their communications. However, when the plaintiffs determined to use MAC's computers to communicate, they did so cognizant that MAC's ECP was in effect . . ." *Id.* at \*3.

100. *Id.*

101. As in all the cases cited in this sub-section. See *Long*, 2006 WL 2998671, at \*1; *Curto v. Med. World Commc'ns, Inc.*, No. 03-CV-6327, 2006 WL 1318387, at \*1 (E.D.N.Y. May 15, 2006); *Jiang*, 31 Cal. Rptr. 3d at 197-98; *Nat'l Econ. Research Assocs. v. Evans*, No. 04-2618-BLS2, 2006 WL 2440008, at \*3 (Mass. Super. Ct. Aug. 3, 2006).

102. This argument presents a slippery slope. Rewarding an employee for attempting to hide evidence seems unwise, as it rewards an employee for what essentially amounts to spoliation.

103. An employee's use of a password protected account arguably decreases the risk that emails would be discovered.

104. *Curto*, 2006 WL 1318387, at \*3 & n.2.

105. *Id.*

106. Many employees may well continue to use personal e-mail accounts at work despite their knowledge that they have no expectation of privacy in their communications, as they have nothing to hide.

use may be rational in exceptional circumstances,<sup>107</sup> but it is questionable whether such an inference is objectively reasonable.<sup>108</sup>

#### D. *Employee Attempts to Delete Privileged Material*

The *Curto* court reasoned that an employee's attempt to single delete<sup>109</sup> privileged files was a reasonable precaution to prevent inadvertent disclosure.<sup>110</sup> The *Evans* court reached a similar conclusion regarding an employee's attempt to double delete privileged files.<sup>111</sup> In both cases, the employer discovered the files.<sup>112</sup>

These attempts to delete information surely created a subjective belief in the mind of the employee that the communication was made inaccessible to the employer.<sup>113</sup> Yet, in light of commonly used technology,<sup>114</sup> that belief was objectively unreasonable. That the employer was able to recover the documents, even when a document was purportedly double deleted<sup>115</sup> illustrates this point.

---

107. The argument is stronger when control-group executives are in the habit of using personal e-mail at work, as in *Curto*. See *supra* note 105 and accompanying text. It would be further strengthened if the employee were instructed by a supervisory employee to use a personal e-mail account for e-mails, such as to send them a work-related file.

108. Where an employee was merely aware that other rank-and-file employees used personal email at work, or where co-workers with no supervisory authority represented to the employee that personal e-mail at work was shielded from surveillance, an inference of privacy would be less reasonable.

109. See *supra* note 77.

110. *Curto*, 2006 WL 1318387, at \*3. Yet, it seems clear that the *Curto* court was referring to single deletion, which is arguably not a reasonable precaution "taken . . . to prevent inadvertent disclosure of [a privileged document] . . ." *Id.*

111. Nat'l Econ. Research Assocs. v. *Evans*, No. 04-2618-BLS2, 2006 WL 2440008, at \*1 (Mass. Super. Ct. Aug. 3, 2006). *Evans* is a great example of a technologically unsophisticated person attempting to double delete a file. The employee deleted all his personal files and ran a disk defragmenter under the false assumption that running the program would prevent recovery of his files. *Id.*

112. See *Curto*, 2006 WL 1318387, at \*1; *Evans*, 2006 WL 2440008, at \*2.

113. Otherwise, why would the employee bother to delete the file? While the employee might argue that the deletion was merely an attempt to eliminate e-mail clutter, this sort of housekeeping deletion would still create the subjective belief that the e-mail was made inaccessible to their employer.

114. Recovery of deleted data from computers through the use of forensic software has been commonplace since the early 1990s. See David W. Hendron, *The Continuing Evolution of Computer Forensics*, L. ENFORCEMENT Q., Winter 2005–2006, at 19, 19–20.

115. With some effort, double deleted data can be recovered.

Even when data on a [computer] disk is deleted and overwritten, a 'shadow' of the data might remain . . . . [This] shadow data [is the] result of the minor imprecision[s] that naturally [occur] when data [is] being written on a disk. The arm that writes data onto a disk has to swing to the correct place, and it is never perfectly accurate. Skiing provides a good analogy. When you ski down a snowy

Further, the employers in both *Curto* and *Evans* made clear that employees had no expectation of privacy while using a work computer.<sup>116</sup> Thus, even if the employees' actions in *Curto* and *Evans* were to be considered reasonable precautions to prevent inadvertent disclosure, an ex post facto measure to prevent disclosure does not automatically equate to a showing of an objectively reasonable expectation of privacy at the time of the communication.<sup>117</sup> The employee's attempted deletion might be more relevant in a work product analysis.<sup>118</sup>

### E. Employer Enforcement of any Existing Policies

In upholding an employee's privilege claims, the *Curto* court considered the frequency of the employer's enforcement of its computer usage policy.<sup>119</sup> The court acknowledged that no other court had previously found this factor to be relevant,<sup>120</sup> but stated that "it goes right to the heart of the overriding question which guides the Court's analysis: was [the employee's] conduct so careless as to suggest that she was not concerned with the protection of the privilege."<sup>121</sup>

The court further stated that prior cases on employee expectations of privacy were not controlling as (1) they did "not address the confidentiality of [an] employee's e-mails and personal computer files with regard to the attorney-client privilege or attorney work product immunity[,] and (2) "none of [the] cases involve[d] an employee working from a *home* office."<sup>122</sup>

*Curto* suggests that consideration of the employer's habitual enforcement would not be appropriate in all situations, and the court's

---

slope, your skis make a unique set of curving tracks. When people ski down behind you, they destroy part of your tracks when they ski over them but they leave small segments. A similar thing happens when data is overwritten on a disk—only some parts of the data are overwritten leaving other portions untouched. A disk can be examined for shadow data in a lab with advanced equipment (e.g. scanning probe microscopes, magnetic force microscopes) and the recovered fragments can be pieced together to reconstruct parts of the original digital data.

EOGHAN CASEY, *DIGITAL EVIDENCE AND COMPUTER CRIME* 240 (2d ed. 2004).

116. See *Curto*, 2006 WL 1318387, at \*1; *Evans*, 2006 WL 2440008, at \*2–3.

117. The objective reasonability of a person's belief that his or her communications are private is determined at the time the communications were made. See, e.g., *United States v. Inigo*, 925 F.2d 641, 657 (3d Cir. 1991); *Coastal States Gas Corp. v. Dep't of Energy*, 617 F.2d 854, 863 (D.C. Cir. 1980).

118. This conclusion follows because an employee's attempt to delete emails likely decreases the risk that the emails would be discovered.

119. *Curto*, 2006 WL 1318387, at \*4–5.

120. *Id.*

121. *Id.* at \*5.

122. *Id.*

explicit limitation of its holding makes this conclusion clear.<sup>123</sup> Moreover, the *Curto* court downplayed the importance of employer enforcement, stating that the factor was “in no way . . . dispositive” and characterizing it “as a ‘sub-factor’ to be examined, along with [other factors] . . . .”<sup>124</sup> *Curto*’s token defense justifying consideration of the frequency of the employer’s enforcement of its computer use policy illustrates its relative unimportance.

#### F. *The Location of the Computer*

The physical location of the computer has logical and legal significance in workplace waiver cases. It is true that an employer-owned computer does not cease to be employer-owned if it is taken into an employee’s home.<sup>125</sup> However, technologically sophisticated surveillance intruding into an individual’s home has been frowned upon by the Supreme Court in other contexts.<sup>126</sup> Allowing an employee to take a computer into his or her home, then later using information stored on that computer against the employee, smacks of a Trojan Horse.<sup>127</sup>

In upholding an employee’s privilege claims, the *Curto* court was careful to note that

[t]he Court’s holding is limited to the question of whether an employee’s personal use of a company-owned computer *in her home* waives any applicable attorney-client privilege or work product immunity that may attach to the employee’s computer files and/or e-mails. It does not purport to address an employee’s right to privacy in an office computer in general.<sup>128</sup>

By limiting its holding in this way, the *Curto* court indicated that a computer’s location can be determinative. Another recent case has cited

---

123. See *infra* note 128 and accompanying text.

124. *Curto*, 2006 WL 1318387, at \*8.

125. The converse is true regarding an employee’s personal computer taken to work. See *supra* notes 51–52 and accompanying text.

126. “The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.” *Kyllo v. United States*, 533 U.S. 27, 34 (2001). *Kyllo* answered this question by placing harsh limitations on the warrantless use of technology to cross the “‘firm line [of privacy] at the entrance to the house.’” *Id.* at 40 (quoting *Payton v. New York*, 445 U.S. 573, 590 (1980)). Although the *Kyllo* case involved the Fourth Amendment and criminal law, the Court’s articulation of its desire to protect the home against invasive technological surveillance implies that the Court would have similar protectionist leanings in workplace waiver cases.

127. The Supreme Court has previously frowned upon “a Trojan horse dressed up in legal form.” *NLRB v. City Disposal Sys., Inc.*, 465 U.S. 822, 844 (1984).

128. *Curto*, 2006 WL 1318387, at \*8 (emphasis added).

*Curto* to “highlight[] the perils” of an employee using an employer-issued computer in the home.<sup>129</sup>

A more interesting question would be posed by an employee accessing a workplace e-mail account<sup>130</sup> from home. It is doubtful that this scenario would be viewed as analogous to using an employer-owned computer at home, as the employee would have had the option to use a personal e-mail account, and thus it would seem less of an employer-set snare.

### G. *The Forensic Method Used to View an Employee’s E-mails*

The *Evans* court took issue with the method used by the employer to monitor its employee’s e-mail usage.<sup>131</sup> The employer in *Evans* used software that routinely took “screen shots”<sup>132</sup> of what the employee was viewing on the employer’s computer.<sup>133</sup> The court was shocked that this surveillance was possible.<sup>134</sup> Yet, the employer stated in its policy manual that “Network administrators can read your [electronic] mail!”<sup>135</sup> While shocking to the court,<sup>136</sup> this particular forensic method may be relatively commonplace.<sup>137</sup>

While stopping short of declaring this method of surveillance per se unacceptable, the *Evans* court stated that:

The bottom line is that, if an employer wishes to read an employee’s attorney-client communications unintentionally stored in a temporary file on a company-owned computer that were made via a private, password-protected e-mail account accessed through the Internet, not the company’s Intranet, the employer must plainly communicate to the employee that:

1. all such e-mails are stored on the hard disk of the company’s computer in a “screen shot” temporary file; and

---

129. *Geer v. Gilman Corp.*, No. 3:06–CV-889, 2007 WL 1423752, at \*4 (D. Conn. Feb. 12, 2007).

130. *See supra* note 20.

131. *Nat’l Econ. Research Assocs. v. Evans*, No. 04-2618-BLS2, 2006 WL 2440008, at \*4 (Mass. Super. Ct. Aug. 3, 2006).

132. “A screen shot is [an electronically] printed [or electronically stored] page depicting the visual images seen on a computer monitor when connected to a web page.” *SCC Commc’ns Corp. v. Anderson*, 195 F. Supp. 2d 1257, 1258 n.4 (D. Colo. 2002).

133. *Evans*, 2006 WL 2440008, at \*4.

134. “This Court does not agree that any reasonable person would have known this information. Certainly, until this motion, this Court did not know of the [possibility of] routine storing of ‘screen shots’ from private Internet e-mail accounts on a computer’s hard disk.” *Id.*

135. *Id.* at \*3.

136. *Id.* at \*4.

137. *See supra* note 12 and accompanying text.

2. the company expressly reserves the right to retrieve those temporary files and read them.

Only after receiving such clear guidance can employees fairly be expected to understand that their reasonable expectation in the privacy of these attorney-client communications has been compromised by the employer.<sup>138</sup>

Such a detailed instruction as to how an employee is being monitored seems unnecessary when the employer's policy manual states "[n]etwork administrators can read your [electronic] mail!"<sup>139</sup> Moreover, forcing an employer to lay out the specific technical procedure used to monitor an employee might aid employees in circumventing the monitoring systems.

However, the *Evans* court's reaction to the employer's method of surveillance seemed ultimately grounded in a concern for fairness.<sup>140</sup> The court's holding stemmed from its belief that the method used was overly invasive and that the employee was not given adequate notice of monitoring.<sup>141</sup> Thus, if a court considers a method of surveillance to be inherently unfair,<sup>142</sup> it may justifiably require a company to take extraordinary steps to ensure notice.<sup>143</sup>

#### H. *Fairness and Public Policy*

The *Curto* court specifically considered the "overarching issue of fairness" as a variable.<sup>144</sup> All courts, whether implicitly or explicitly, have considered issues of fairness and public policy. It may be that all workplace waiver decisions are reverse-engineered to match whatever the court feels is the fair result. The sparsity of case law coupled with rich factual situations has resulted in malleable judicial standards. The danger reliance on a court's interpretation of what is fair or in the interest of

---

138. *Evans*, 2006 WL 2440008, at \*5.

139. *Id.* at \*3.

140. *Id.*

141. *Id.* at \*3-4.

142. Raising the question, what exactly is an "unfair" method of surveillance? Employers use a myriad of methods to keep an eye on employees, running the gamut from peeping over the employee's shoulders to keystroke monitoring and e-mail duplication and review. *See supra* note 12 and accompanying text. Intuitively, the more sophisticated methods of surveillance would be more likely to be deemed unfair as they appear harsh as a natural consequence of their effectiveness.

143. Even if a court determines a method is inherently unfair, the employer could still continue to use that method of surveillance to watch over employees. The employer would simply be unable to use the information gained in litigation.

144. *Curto v. Med. World Commc'ns, Inc.*, No. 03-CV-6327, 2006 WL 1318387, at \*3 (E.D.N.Y. May 15, 2006) (citation omitted).

public policy is that what different judges consider to be “fair” differs wildly.

A good example of a court reverse-engineering a workplace waiver decision based upon what it believes to be in the interest of public policy can be seen in *Sims v. Lakeside School*,<sup>145</sup> in which an employee used his employer’s laptop to communicate with his attorney and the employer later forensically recovered the e-mails.<sup>146</sup> The court stated “that [the employee] was on notice that he did not possess a reasonable expectation of privacy in the contents of his laptop[,]”<sup>147</sup> yet the court held that “[n]otwithstanding defendant Lakeside’s policy in its employee manual, public policy dictates that such communications shall be protected to preserve the sanctity of communications made in confidence.”<sup>148</sup> The only legal support cited by the *Sims* court for deciding the case on public policy grounds was a ninety-two-year-old case that does not once mention attorney-client privilege,<sup>149</sup> thus making the court appear intellectually disingenuous.

While the *Sims* court may well be correct that it is not in the public interest to allow employers to use in litigation information gained from spying on employees, its unilateral imposition of this policy viewpoint with no legitimate legal support illustrates the danger of judicial imposition of public policy judgments. As Justice White said, “[t]he task of defining the objectives of public policy and weighing the relative merits of alternative means of reaching those objectives belongs to the legislature.”<sup>150</sup> While it is important for a court to have the discretion to consider issues of fairness and public policy, it is more important that a court carefully consider the factual circumstances and principles of

---

145. No. C06-1412RSM, 2007 WL 2745367 (W.D. Wash. Sept. 20, 2007).

146. *Id.* at \*1.

147. *Id.*

148. *Id.* at \*2.

149. Although the *Sims* court indicates otherwise in the parenthetical following its citation:

Notwithstanding defendant Lakeside’s policy in its employee manual, public policy dictates that such communications shall be protected to preserve the sanctity of communications made in confidence. *See e.g., United States v. Louisville & Nashville R.R.*, 236 U.S. 318, 336, 35 S.Ct. 363, 369 (1915) (recognizing that the attorney-client privilege is predicated upon the belief that it is in the public interest to encourage free and candid communications between clients and their attorneys, by protecting the confidentiality of such communications).

*Id.*

150. *Lowe v. SEC*, 472 U.S. 181, 213 (1985) (White, J., concurring).

existing law.<sup>151</sup> Widespread judicial application of subjective interpretations of fairness would result in chaos. It would simply be impossible to establish any semblance of uniformity in workplace waiver cases.

#### IV. MAKING SENSE OF IT ALL

##### A. *The Knowledge Gap*

Much of the difficulty in these cases stems from the employee-employer knowledge gap.<sup>152</sup> Most employees have an erroneous belief that e-mail communications made on a company computer are private,<sup>153</sup> even though a person with a moderate technological knowledge base would consider that belief unreasonable. Whether an objectively reasonable person possesses moderate technological knowledge remains an open question.

Judges are put in the unenviable position of trying to determine who should bear the consequences of this knowledge gap.<sup>154</sup> They are forced to decide whether a commonly held incorrect belief is an objectively reasonable belief. This position is made all the more difficult by the fact that few judges have significant experience with technology,<sup>155</sup> and some

---

151. Admittedly, *stare decisis* concerns are particularly weak in workplace waiver cases as they involve application of evidentiary rules. *See, e.g., Payne v. Tennessee*, 501 U.S. 808, 828 (1991) (“Considerations in favor of *stare decisis* . . . [are at their weakest in cases] involving procedural and evidentiary rules.”).

152. “[I]nadequacy in the law [related to employee privacy in the workplace] is primarily based on the fact that many employees do not know the extent of their privacy rights regarding their company-provided e-mail accounts. In fact, many employees operate under the false assumption that personal e-mail messages sent from work are protected from their employer’s scrutiny.” Corey A. Ciocchetti, *Monitoring Employee E-Mail: Efficient Workplaces vs. Employee Privacy*, 2001 DUKE L. & TECH. REV. 26, ¶1 (2001); *see also supra* notes 13–14 and accompanying text.

153. *See supra* notes 13–14 and accompanying text.

154. “Hard cases, it is said, make bad law.” *Ex Parte Long*, 3 W.R. 19 (Q.B. 1854, Lord Campbell, C.J.).

155. According to Judge Posner, “[e]veryone knows that younger people are on average more comfortable with computers than older people . . . .” *Sheehan v. Daily Racing Form, Inc.*, 104 F.3d 940, 942 (7th Cir. 1997). It is also common knowledge that most judges do not typically take the bench until they have practiced law for years. However, a growing number of Federal Judges are being recognized for their technological sophistication and adroitness in handling electronic discovery issues. These judges, including Judge David A. Baker of the Middle District of Florida, Judge Shira A. Shindlin of the Southern District of New York, Judge Paul W. Grimm of the District of Maryland, Judge John M. Facciola of the District of Columbia, Judge David J. Waxse of the District of Kansas, and Judge Rudi M. Brewster of the Southern District of California, have been referred to as electronic discovery “rock stars.” *See* Jason Krause, *Rockin’ Out the E-Law*, 94 A.B.A. J. 48 (2008).

appear to personally identify with technologically unsophisticated employees.<sup>156</sup>

Interestingly, when faced with ambiguity, courts that regularly deal with technological questions rule differently in technology-related cases than courts that do not.<sup>157</sup> This observation suggests that the judge's level of technological sophistication corresponds to the judge's interpretation of what is an objectively reasonable level of technological sophistication.<sup>158</sup>

### B. *Modern vs. Traditional Approach to Attorney-Client Privilege*

Some courts have adopted a modern approach to attorney-client privilege in workplace waiver cases. These courts have broadly interpreted the privilege in an attempt to deal with situations where these courts feel the privilege should be upheld. They may do so either for public policy reasons, or because they feel that the traditional approach is unable to cope with issues involving technology. Other courts have adhered to Wigmore's traditional approach. While it is possible that courts adopting the modern, broad approach have done so unwittingly, the difference of breadth has naturally led to inconsistent holdings and will continue to do so until some uniformity is established.<sup>159</sup>

## V. THE WORKPLACE WAIVER PRESUMPTION

### A. *The Bright-Line Fallacy*

It has been noted that “[t]o date, courts have not developed bright-line approaches for determining when attorney-client privilege protects data

---

156. See *supra* note 134 and accompanying text.

157. See Joseph A. Grundfest & A.C. Pritchard, *Statutes with Multiple Personality Disorders: The Value of Ambiguity in Statutory Design and Interpretation*, 54 STAN. L. REV. 627, 724–25 (2002) (“These findings also suggest that the more frequently judges view technology cases, the more likely they are to adopt pro-defendant interpretations of the statute.”).

158. *Id.*

159. However, this inconsistency may become moot. It is possible that employee privacy rights in the United States will broaden over time to the point that workplace waiver is no longer an issue. Most countries outside the United States offer significantly more privacy rights for employees, and the United States may eventually fall into line with the rest of the world and legislatively establish broader privacy rights for employees in the workplace.

Moreover, business entities within the United States may voluntarily broaden the privacy rights of their employees through widespread revisions to employee policy manuals. The impetus behind this broadening of employee privacy rights may come from upper level management, and other control group employees. Control group employees are often responsible for making decisions regarding employee privacy and employee surveillance, and yet they themselves are employees. Thus, there is a strong incentive for the employee-authors of employee policy manuals to broaden employee privacy rights per the employer's policies.

stored on an employer-issued computer.”<sup>160</sup> Without a bright-line approach, courts will continue to consider a legion of variables, leading to inconsistency. Yet, some variability may be desirable. An attempt to produce clarity through the imposition of a forced bright-line test would cause unnecessary rigidity.

Thus, it would be a mistake for a court, in a workplace waiver case, to hold that either (1) privilege is always waived in the presence of policy language stating that the employee has no expectation of privacy; or (2) privilege is never waived as a matter of public policy. Workplace waiver issues involve sophisticated questions of law and nuanced factual inquiries, and they require an equally nuanced analysis to achieve a just resolution. By teasing the logically pertinent variables out of existing workplace waiver case law, a standardized yet nuanced approach can be developed.

### B. *Distillation of Logically Pertinent Variables*

It is generally accepted that in workplace waiver cases a court should first look to the language of the employer’s policies. If the policies make clear that the employee has no expectation of privacy while using a workplace computer, then it is logical to establish a presumption that privilege has been waived. This presumption could be rebutted if the employee shows that (1) the location of the computer or (2) the actions of the employer rendered this policy language ineffective. Depending on the circumstances, a court might also consider analyzing the issue under the work product doctrine.

However, problems may emerge when considering such variables as (1) use of a personal password-protected e-mail account, (2) other employees’ use of personal e-mail at work, (3) employee attempts to delete or hide files from the employer, (4) the forensic method used by the employer to recover information, or (5) any other technologically related facts where the court is unable to easily determine the objective relevance of the evidence.

Under the traditional, narrow construction of attorney-client privilege, these variables are likely insignificant. Under a modern, broad approach to attorney-client privilege, they might be pertinent. Either way, courts need specialized outside help in these cases. Court-appointed experts,<sup>161</sup> special masters,<sup>162</sup> or even adversarial testimony by the parties’ competing

---

160. Kelcey Nichols, Note, *Hiding Evidence From the Boss: Attorney-Client Privilege and Company Computers*, 3 SHIDLER J.L. COM. & TECH. 6, ¶ 4 (2006), available at <http://www.lctjournal.washington.edu/Vol3/a006Nichols.html>.

161. See FED. R. EVID. 706.

162. See FED. R. CIV. P. 53.

experts<sup>163</sup> could go a long way in assisting in the determination of the objective reasonableness of an employee's belief.

By all accounts, the use of a presumption is the logical first step in workplace waiver cases. Courts should first place the burden on the employer to show language in its policy manual that facially establishes that the employee had no objectively reasonable expectation of privacy. The employee would then be free to rebut that presumption by presenting evidence showing that the employee had an objectively reasonable expectation of privacy despite the language in the employer's policy manual. If the court has any doubt as to whether evidence presented by the employee to rebut the presumption is relevant, then the court should call in specialized outside help.

#### VI. CONCLUSION: ADOPTION OF THE WORKPLACE WAIVER PRESUMPTION

Courts can and should distill existing case law to determine the logically pertinent factual variables in workplace waiver cases, but a jurisprudential clash may be inevitable. Courts that have adopted the broad (modern) approach to attorney-client privilege, and those that have held fast to Wigmore's narrow (traditional) interpretation are on a collision path.

The application of the workplace waiver presumption, described in this Note, is the best way to avert a direct collision between these two schools of thought and to achieve a semblance of predictability in these cases. Adherents to both the modern and traditional approaches would be able to use this presumption without compromising their viewpoints. This presumption would give courts a workable, flexible rubric that would prove invaluable in working through workplace waiver issues. It is clear that the adoption of the workplace waiver presumption is the logical first step in the development of workplace waiver jurisprudence.

---

163. See FED. R. EVID. 702.