BIG BOSS IS WATCHING: CIRCUMSTANCES UNDER WHICH EMPLOYEES WAIVE THE ATTORNEY-CLIENT PRIVILEGE BY USING E-MAIL AT WORK

JANNA FISCHER*

ABSTRACT

When an employee chooses to send an e-mail to her attorney from a work computer, the employee risks waiving the attorney-client privilege because of the possibility that the employer will access the e-mail sent from the work computer. When the employee uses a work e-mail account, the risk is high that a court will say that the employee waived the privilege. But when the employee uses her personal, web-based e-

* Associate at Cooley LLP, Broomfield, Colo. J.D., University of Colorado Law School, 2012. This paper began in Professor Harry Surden's Computers and the Law seminar. The author thanks Professor Surden for his support and advice and Steven Zansberg of Levine Sullivan Koch & Schulz for assigning the research that gave her the idea.

mail account, a court will probably hold that the employee did not waive the attorney-client privilege even if the employer is able to retrieve the messages. This paper explores why this distinction makes sense in light of employees' expectations about personal e-mail and the difference in the way the law treats public e-mail accounts.

INTRODUCTION

Emily wants to file a sexual harassment lawsuit against her employer because her immediate supervisor makes inappropriate comments to her on a daily basis. She faithfully documents every incident in e-mails that she sends to her attorney. Emily's only e-mail account is her work e-mail account, which she accesses through her employer-provided computer at work.[1] Emily deletes every e-mail after she sends it, and only she knows the password she uses to access her work e-mail. She thinks her employer does not have access to her deleted messages.

Jessica similarly is preparing to sue her employer for sexual harassment based on her immediate supervisor's conduct. Just like Emily, she documents every incident in e-mails that she sends to her attorney. But Jessica is careful to only use her personal, web-based e-mail account, not her work e-mail.[2] Jessica's only computer is her employer-provided laptop, which she uses both at home and at work. She uses this laptop to access her personal e-mail account and send e-mails to her attorney. Jessica clears her browser history after she uses her work laptop, and she thinks her employer cannot access the messages she sent using her personal e-mail account and her work computer.

Both Jessica's and Emily's employers retrieve e-mails from the company computers after the two employees file lawsuits. Both employers want to use the e-mails as evidence, and both employees claim that the e-mails are protected by attorney-client privilege. While the court in Emily's case says that Emily waived the privilege because she used her employer's account and must have expected that her employer would be able to access the account, the court in Jessica's case says her e-mails are protected by privilege despite the fact that she sent

1. Emily is loosely based on the facts of Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 898–99 (Cal. Ct. App. 2011). The *Holmes* court held that an employee waived the attorney-client privilege when she used her work e-mail account to communicate with her attorney about her sexual-harassment lawsuit against her employer. *Id.*

2. Jessica is loosely based on the facts of Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010). An employee in *Stengart* used her employer's computer but accessed her personal, web-based e-mail account and used that to exchange messages with her attorney regarding her employment-discrimination lawsuit; the court held that her e-mails were protected by privilege. *Id.*

the e-mails using her employer's computer, which was the employer's property. While both Emily and Jessica used their employers' computers to communicate with their attorneys, only Emily used her work e-mail account. Is that difference enough to account for the opposite outcomes in their cases?

Whether a court finds that an employee's work e-mail is protected by attorney-client privilege depends on a range of factors. Some courts look to the employer's policy on e-mail.[3] Other courts may find that an employee waived the attorney-client privilege by using work e-mail even though the employer had no policy governing e-mail[4] or, conversely, that the employee did not waive the attorney-client privilege precisely because the employer had no clear policy.[5] When the employee uses a personal, web-based e-mail account on a work computer, courts have generally held that the employee did not waive attorney-client privilege by using a work computer.[6]

E-mail is a commonplace form of communication, and many—if not all employees—send personal messages at some point during the workday.[7] While an employee would reasonably be on notice that her employer can access her messages while using her work e-mail account, an employee using her personal, web-based e-mail account would not reasonably expect that her employer has access to her e-mail and therefore should not be deemed to have waived the attorney-client privilege.

3. *See In re* Info. Mgmt. Servs., Inc. Derivative Litig., 81 A.3d 278, 291 (Del. Ch. 2013) (compelling the production of employees' e-mails with attorneys because the employees were aware of the company's policy that it had unrestricted access to company computers and e-mails sent using those computers should not be considered private); Kaufman v. SunGard Inv. Sys., CIV.A.05-CV-1236(JLL), 2006 WL 1307882, at *4 (D.N.J. May 10, 2006) (employee waived the attorney-client privilege because of an employer's policy that it could search and monitor communications at any time); *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (describing four factors in an employer's policy that suggest the employee will not have a reasonable expectation of privacy in his e-mail).

4. *See* Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (employee waived the attorney-client privilege by using work e-mail even though his employer told him that his e-mail would be kept "confidential").

5. Convertino v. U.S. Dept. of Justice, 674 F. Supp. 2d 97, 110 (D.D.C. 2009) (because the employer did not have a policy governing personal use of e-mail and the employee was unaware that his employer would regularly be accessing his work e-mail account, he did not waive attorney-client privilege by using that e-mail).

6. *See, e.g.*, Curto v. Med. World Comm'ns, Inc., 03CV6327 DRH MLO, 2006 WL 1318387, at *1 (E.D.N.Y. May 15, 2006).

7. Two of every five employees use a computer at work, and the most common activities are surfing the Internet and checking e-mail. U.S. DEP'T OF LABOR BUREAU OF LABOR STATISTICS, ECONOMIC NEWS RELEASE: COMPUTER AND INTERNET AT WORK SUMMARY (2005). In general, 92 percent of adults use e-mail each day. Kristen Purcell, *Search and Email Still Top the List of Most Popular Online Activities*, PEW INTERNET & AMERICAN LIFE PROJECT (Aug. 9, 2011), http://pewinternet.org/Reports/2011/Search-and-email.aspx.

Because of this difference in expectations, it does not make sense to treat Emily and Jessica the same. While Emily probably opened herself up to a court's determination that she waived the attorney-client privilege by using her work e-mail account, Jessica took steps to try to keep her employer from reading her e-mail. This paper explores the reasons for this distinction. Part I describes the circumstances under which a client inadvertently waives the attorney-client privilege by exposing the contents of a communication to a third party. Part II describes the circumstances under which an employee generally has a reasonable expectation of privacy in her electronic communications. Part III discusses the current case law involving employees who e-mailed their attorneys on work equipment and whether those employees waived the attorney-client privilege. Part IV discusses the statutory and policy reasons for treating an employee's use of a personal account differently than her use of a work e-mail account.

I. WHEN A CLIENT WAIVES ATTORNEY-CLIENT PRIVILEGE

Attorney-client privilege applies to (1) a communication; (2) made between privileged persons; (3) in confidence; (4) for the purpose of obtaining or providing legal assistance for the client.[8] "Its purpose is to encourage full and frank communication between attorneys and their clients."[9] The privilege recognizes an attorney needs to be fully informed by his client in order to order to give the best advice.[10]

The burden rests with the party asserting the privilege to show that the attorney-client relationship existed, that the communications were made in the course of legal assistance, that the communications were made in confidence, and that the privilege has not been waived.[11] The client (but not the attorney) can waive the privilege if the client discloses to a third party information protected by the attorney-client privilege.[12]

8. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 68 (1998).

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

10. *Id.*

11. *See, e.g.*, Saxholm AS v. Dynal, Inc., 164 F.R.D. 331, 333 (E.D.N.Y. 1996) ("A party who asserts the attorney-client privilege . . . bears the burden of establishing all the essential elements of the privilege."); Nat'l Econ. Research Assocs. v. Evans, CIV.A. 04-2618-BLS2, 2006 WL 2440008, at *2 (Mass. Super. Aug. 3, 2006).

12. *See* United States v. Jacobs, 117 F.3d 82, 91 (2d Cir. 1997) (public disclosures constitute a waiver of the privilege); *see also* Charles Alan Wright et al., *Procedure*, 24 FED. PRAC. & PROC. EVID. § 5507 (1st ed. 2011 update) (Traditionally, the privilege is waived when "the holder of the privilege 'voluntarily discloses or consents to disclosure of any significant part of the [privileged] matter or communication.'"); *see also* 32 AM. JUR. 3D *Proof of Facts* 189 § 8 (1995) ("[A]lthough a client confides the substance of attorney-client

Other circumstances under which the attorney-client privilege can be waived include the following:

> (1) conversations between attorneys and clients in a public place are overheard by others; (2) there is indiscriminate mingling of attorney-client privileged documents with documents which will be subject to routine disclosure to third persons without having taken precautions to protect the privileged documents from disclosure; (3) privileged documents are stolen or taken because they were not adequately protected; (4) privileged documents are kept in file cabinets routinely used by others; and (5) privileged papers are left in places accessible to the public.[13]

A client can waive the attorney-client privilege by exposing a conversation to a third party. For example, when an incarcerated criminal defendant made phone calls to his attorney from prison, the court concluded that he waived the attorney-client privilege.[14] The prison notified inmates at the outset of each call they placed that the calls were being recorded and monitored by prison officers.[15] The defendant's decision to continue with his phone call even after hearing the notification was no different than if he had chosen "to proceed with these conversations notwithstanding the known presence of a third party within earshot of the conversation."[16] Similarly, where a defendant proceeded with a conversation in her attorney's office despite the presence of at least five other people, a court held that the conversation was not protected by attorney-client privilege.[17] And where a telephone operator overheard a conversation between a criminal defendant and his attorney, the conversation was not privileged.[18]

Similarly, when clients do not take steps to protect access to documents, courts may find that the disclosure waived the attorney-client

communications to a brother or a sister with whom the client has historically discussed important personal matters, there is a strong risk that the disclosure would be deemed a waiver of the attorney-client privilege.").

13. McCafferty's, Inc. v. Bank of Glen Burnie, 179 F.R.D. 163, 168 (D. Md. 1998) (citing EDNA S. EPSTEIN, THE ATTORNEY-CLIENT PRIVILEGE AND THE WORK-PRODUCT DOCTRINE 183-90 (3d ed. 1997)).

14. United States v. Lentz, 419 F. Supp. 2d 820, 828 (E.D. Va. 2005).

15. *Id.*

16. *Id.*

17. United States v. Gordon-Nikkar, 518 F.2d 972, 975 (5th Cir. 1975) ("A communication divulged to 'strangers' or outsiders can scarcely be considered a confidential communication between attorney and client."); *see also* Conn. Mut. Life Ins. Co. v. Shields, 18 F.R.D. 448, 451 (S.D.N.Y. 1955) (a claim of privilege was "not supportable" with respect to a conversation at which outside parties were present).

18. Clark v. State, 261 S.W.2d 339, 343 (Tex. Crim. App. 1953), *cert. denied*, 346 U.S. 855.

privilege. For example, the Department of Energy failed to establish that the attorney-client privilege protected communications with the agency's lawyers, and that those documents were therefore not subject to a Freedom of Information Act request, when the agency took no steps to keep the documents confidential.[19] The agency circulated the documents among all of its offices and admitted that it did not know who had access to the documents.[20] The agency argued that because the documents were only circulated within the agency, they were still protected by the attorney-client privilege, but the court rejected its argument because "that would be far too broad a grant of privilege."[21]

However, a disclosure does not operate as a waiver if: "(1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error."[22] The steps that a client takes to preserve the attorney-client privilege do not have to be perfect, just reasonable. For example, where a human resources director tore a memo into sixteen pieces before discarding the pieces in a trashcan, a court concluded that she did not waive the attorney-client privilege even though she threw away the memo.[23] The director received a memo from the attorney who was representing her employer in a sexual-harassment lawsuit, and she revised the memo, sent it back to the attorney, and threw the draft he had sent her in her office trash can after tearing it up.[24] She did not show the draft to anyone else.[25] The janitor emptied her office trashcan, along with many others, into a dumpster in the parking lot, which was marked with a sign stating that the trash was for the exclusive use of the bank.[26] A private investigator working for the plaintiff retrieved the trash from the dumpster and pieced together the memo.[27] When the bank's attorney learned the plaintiff might have the memo, he moved to compel its return.[28] The court determined that the human resources director took reasonable precautions in discarding the memo because she reasonably expected that nobody would see the memo when she discarded it in a place not accessible to the public, she knew that the pieces would be mingled with other trash, and she knew that the trash

19. Coastal States Gas Corp. v. Dep't of Energy, 617 F.2d 854, 863 (D.C. Cir. 1980).

20. *Id.*

21. *Id.* ("If facts have been made known to persons other than those who need to know them, there is nothing on which to base a conclusion that they are confidential.").

22. FED. R. EVID. 502.

23. McCafferty's Inc. v. Bank of Glen Burnie, 179 F.R.D. 163, 169 (D. Md. 1998).

24. *Id*. at 165.

25. *Id.*

26. *Id.*

27. *Id.*

28. *Id.* at 166.

would remain on bank property and was marked with a sign forbidding others' use of the trash.[29] She did not have to take every possible precaution to keep the memo private, just reasonable precautions.[30]

A court cannot infer a waiver simply from the fact that a document did find its way to opposing counsel. For example, where the opposing counsel in an insurance reorganization received two documents from an anonymous source that the plaintiff then sought to protect through attorney-client privilege, the court held that a waiver could not be assumed just from the fact that the anonymous source had the documents.[31] "[A] client may be deemed to have met the burden of establishing that a privilege exists and no waiver has occurred if adequate steps have been taken to ensure a document's confidentiality."[32]

E-mail presents two challenges to maintaining the attorney-client privilege.[33] First, e-mail is susceptible to security breaches during its transmission.[34] Second, e-mail is very easily forwarded and copied to large numbers of people, sometimes by mistake.[35] Despite these two characteristics, courts and the American Bar Association now generally regard e-mail as no less secure than similar forms of communications in which people have a reasonable expectation of privacy.[36] Indeed, at least one federal court of appeals specifically held that people generally have a reasonable expectation of privacy in the contents of their e-mails.[37] While e-mails are probably protected by privilege,[38] sending an e-mail to

29. *Id.* at 169.

30. *Id.*

31. *In re* Reorganization of Elec. Mut. Liab. Ins. Co. (Bermuda), 681 N.E.2d 838, 841 (Mass. 1997) ("Where it can be shown that reasonable precautionary steps were taken, the presumption will be that the disclosure was not voluntary and therefore unlikely that there has been a waiver").

32. *Id.*

33. DAVID. M. GREENWALD ET AL., 1 TESTIMONIAL PRIVILEGES § 1:42 (3d ed. 2010).

34. *Id.*

35. *Id.*

36. *See, e.g.*, *In re* Grand Jury Proceedings, 43 F.3d 966, 968 (5th Cir. 1994) (considering as privileged e-mails along with other documents); United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) ("The fact that an unauthorized "hacker" might intercept an e-mail message does not diminish the legitimate expectation of privacy in any way."); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413, (1999) ("A lawyer 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 (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint.").

37. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010); *see also* United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011) ("We recognize individuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider.").

38. *See, e.g.*, Premiere Digital Access, Inc. v. Cent. Tel. Co., 360 F. Supp. 2d 1168, 1174 (D. Nev. 2005) (e-mails are protected by privilege); Parnes v. Parnes, 80 A.D.3d 948, 951

a large number of people can waive the privilege.[39]

As discussed in Part III, when an attorney and a client communicate over e-mail and there is a good chance that the client's employer will review the e-mail, the court's analysis of whether the client/employee waived the privilege will turn on whether the client voluntarily exposed the e-mail to her employer and therefore waived the attorney-client privilege. Whether the client exposed the e-mail will depend on whether a court determines that she had a reasonable expectation of privacy in her e-mail, or whether that expectation was unreasonable in light of the fact that she used her employer's computer.

II. EMPLOYEES' EXPECTATION OF PRIVACY IN ELECTRONIC DATA

Before examining cases about the waiver of the attorney-client privilege due to using e-mail in Part III, Part II examines when an employee has a reasonable expectation of privacy in her electronic communications at work. The cases that discuss this issue are public-employer cases, because it is in these cases that courts discuss when an employer can search an employee's belongings.

A. The Fourth Amendment Framework

The Fourth Amendment governs public employers' searches of employees' private property.[40] A public-employer search is unreasonable under the Fourth Amendment if it infringes "an expectation of privacy that society is prepared to consider reasonable."[41] While the Fourth Amendment only applies to government employers,[42] cases involving

(N.Y.S.2d 2011) (husband in divorce proceeding did not waive attorney-client privilege by using e-mail where he opened a new account to use with his attorney but his wife found a note containing his password and accessed the account without his permission); *In re* JDN Real Estate-McKinney L.P., 211 S.W.3d 907, 927 (Tex. App. 2006) (e-mails protected by privilege).

39. *See, e.g.*, Wildearth Guardians v. U.S. Forest Serv., 713 F. Supp. 2d 1243, 1266 (D. Colo. 2010) (where an e-mail was "shotgunned" to eleven recipients, and "indiscriminately sought input from *any* of the eleven recipients," the court stated it was "skeptical" that any attorney-client privilege attached to the e-mails but declined to compel production).

40. O'Connor v. Ortega, 480 U.S. 709, 715 (1987) ("Searches and seizures by government employers or supervisors of the private property of their employees . . . are subject to the restraints of the Fourth Amendment.").

41. *Id.* (citing United States v. Jacobsen, 466 U.S. 109, 113 (1984)).

42. Suburban Sew 'N Sweep, Inc. v. Swiss-Bernia, Inc., 91 F.R.D. 254, 256 (N.D. Ill. 1981) ("[I]t is elementary that the Fourth Amendment and its accompanying exclusionary rule

government workplace searches are still instructive when talking about private-employer searches, because courts consider the employee's reasonable expectation of privacy in the thing searched even when the Fourth Amendment does not govern.[43] This paper therefore first examines public-employer search cases before turning to cases where a private employer conducted a search of an employee's computer.

The Supreme Court first examined whether a public employee had a privacy right in his workplace in *O'Connor v. Ortega*.[44] A state hospital conducted a "thorough" search of a doctor's office because it was concerned about the doctor taking advantage of residents in the hospital program.[45] The Court held that the doctor had a reasonable expectation of privacy in at least his desk and file cabinets, noting that the hospital had no policy against employees keeping personal papers in their desks and files.[46] However, the employee's expectation of privacy must be weighed against the "realities of the workplace" and the employer's need to have access to offices in the event that the employer needed to investigate employee misconduct.[47] A workplace search is therefore reasonable when the search is necessary either when the employer suspects employee misconduct or for "non-investigatory, work-related purposes" such as retrieving a needed file and employers do not need a warrant in order to conduct such a search.[48]

O'Connor still provides the framework for when a public-employer search is legal under the Fourth Amendment.[49] Courts start by determining if the public employee had a reasonable expectation of privacy in the thing searched. The Ninth Circuit concluded that a police officer had a reasonable expectation of privacy in his text messages, sent using a city-owned pager that he used to send both personal and work-related text messages.[50] The city had an informal policy that it would not

only apply to conduct of or attributable to the government, and normally do not apply in civil cases.").

43. McCafferty's Inc. v. Bank of Glen Burnie, 179 F.R.D. 163, 168 (D. Md. 1998) (although Fourth Amendment cases do not control, "their usefulness lies in helping the Court to determine whether or not the discarding of privileged communications evidences an intent by the holder of the privilege to abandon the confidentiality which is necessary to sustain the privilege . . . .").

44. 480 U.S. at 711–12.

45. *Id.* at 713.

46. *Id.* at 719.

47. *Id.* at 721.

48. *Id.* at 725. Justice Scalia's approach differed from that of the rest of the justices in the majority in that he would hold that employees' offices are always protected by the Fourth Amendment, but he also would hold that searches related to employee misconduct or for a work-related purpose were reasonable. *Id.* at 732 (Scalia, J., concurring).

49. *See* City of Ontario v. Quon, 560 U.S. 746, 757, (2010).

50. Quon v. Arch Wireless Operating Co., 529 F.3d 892, 906 (9th Cir. 2008), *rev'd on other grounds sub nom.* City of Ontario v. Quon, 560 U.S. 746 (2010).

read employees' messages so long as they paid for any overages.[51] The city did have a formal policy that use of city-owned computers and pagers for personal benefit was prohibited and employees should not expect privacy when using city equipment.[52] However, the officer had gone over the city's plan several times without his supervisor reading his messages, and the supervisor had in fact told the officer he would not read his text messages to determine which ones were personal.[53] The court determined that officer therefore had a reasonable expectation of privacy in his messages.[54]

If the employee had a reasonable expectation of privacy in the thing searched, courts next determine whether the search was reasonable in scope. The Ninth Circuit held that the search of the officer's text messages was not reasonable because there were other ways the city could have achieved its goal of determining which officers were exceeding monthly character limits.[55] For example, the city could have looked only at the phone numbers on the pagers or talked to the officers about the content of their texts.[56] The Supreme Court, however, overturned this portion of the Ninth Circuit's opinion, holding that even assuming the officer had a reasonable expectation of privacy in his texts, the scope of the search was reasonable.[57] The Supreme Court said that city's review of the content of the officer's text messages was not overly intrusive and was "an efficient and expedient way to determine whether [the officer]'s overages were the result of work-related messaging or personal use."[58]

While *Quon* is a case on text messaging, courts similarly apply the *O'Connor* framework to cases involving searches of employees' e-mail.

B. Cases Involving Searches of E-mail

Whether a court finds that a government employee had a reasonable expectation of privacy in his e-mail will probably depend on the reason for the government search and whether the employee knew that his e-mail would likely be searched. A Navy service member had a reasonable

51. *Id.*
52. *Id.*
53. *Id.* at 907.
54. *Id.*
55. *Quon*, 529 F.3d at 908.
56. *Id*. at 909; *see also* Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that people do not have a reasonable expectation of privacy in the phone numbers they dial).
57. City of Ontario v. Quon, 560 U.S. 746, 761 (2010).
58. *Id.*

expectation of privacy in her military e-mail account, and her supervisor's search of her e-mail account was not reasonable, despite the fact that she saw a banner warning her that her computer "was provided only for authorized U.S. Government use" and that "[a]ll information, including personal information, placed on or sent over this system may be monitored."[59] The Navy, searching for evidence of her misconduct with a fellow service member, found e-mails on the service member's computer regarding her drug use and her concerns about passing an upcoming drug test.[60] They charged her with unlawful drug use and court-martialed her; she appealed, claiming that the search of her computer was unlawful and the e-mails should have been suppressed.[61] The U.S. Court of Appeals for the Armed Forces, following the analysis from *O'Connor*, held that the service member did have a reasonable expectation of privacy in her work e-mail despite the warning banner and despite the fact that the e-mails were stored on a government server and written on a government computer.[62] The service member's supervisor did not have her password and testified that he accessed her account to specifically look for misconduct with another Navy officer, not to conduct the monitoring described in the banner.[63] His search "went beyond work-related monitoring" and therefore was illegal under the Fourth Amendment.[64]

The court in *Long* distinguished two public-employee e-mail cases that held the employee did not have a reasonable expectation of privacy in his e-mail: *United States v. Simons* and *United States v. Monroe*.[65] The defendant in *Simons*, who worked for the Central Intelligence Agency's Foreign Bureau of Information Services ("FBIS"), was convicted of possessing child pornography based on images that his employer found on his work computer.[66] The FBIS had a policy allowing computer use for official government business only and prohibiting use of one's work computer to access anything unlawful.[67] In order to enforce this policy, the FBIS would conduct regular audits to look for unauthorized use.[68] During one of these audits, an auditor found an unusual number of searches coming from the defendant's computer containing the word

59. United States v. Long, 64 M.J. 57, 60 (C.A.A.F. 2006).
60. *Id.* at 59.
61. *Id.*
62. *Id.* at 64.
63. *Id.* at 64–65.
64. *Id.* at 65.
65. *Id.* at 64–65 (distinguishing United States v. Simons, 206 F.3d 392 (4th Cir. 2000) and United States v. Monroe, 52 M.J. 326 (2000)).
66. *Simons*, 206 F.3d at 395.
67. *Id.*
68. *Id.*

"sex."[69] Based on this audit, the defendant's supervisor authorized a search of the defendant's computer, which turned up more than 1,000 photos that were later determined to be child pornography.[70] The court held that none of these searches was unlawful because the FBIS policy placed users on notice that their computer use at work was not be private.[71] The audit was within the bounds of the FBIS policy and the search was conducted as part of a normal workplace investigation, so it was a reasonable search under *O'Connor*.[72]

In *United States v. Monroe*, the court held that a member of the Air Force, appealing his conviction for possession of child pornography, had no reasonable expectation of privacy in his Air Force-owned e-mail.[73] The defendant lived on an Air Force base and had access to an e-mail account on the Air Force server.[74] The e-mail system pushed messages from a queue to users' accounts every fifteen minutes, and the system slowed down considerably when large messages became stuck in the queue.[75] While investigating the cause of one of these slowdowns, the system administrator found fifty-nine messages stuck in the queue that were all addressed to the defendant, some of which contained large graphic files that were later discovered to be sexually explicit photographs.[76] The court held that the system administrator's search of the messages was not unlawful because the system had a notice that all users logging onto the system consented to monitoring by the Air Force and the defendant therefore should have been aware that he was using a system that would be accessed by the Air Force.[77]

The court in *Long* distinguished these two cases because while the Air Force discovered the photographs in *Monroe* during routine monitoring, and the FBIS in *Simons* had a specific policy about e-mail audits and the use of e-mail accounts for government business only, the Navy did allow personal use of its e-mail and its log-on warning described a "less intrusive" monitoring policy.[78] In addition, the Navy specifically went looking for evidence of misconduct and did not discover the service member's e-mails about drug use during a routine

69. *Id.* at 396.

70. *Id.* The FBIS then got a warrant in order to seize the defendant's hard drive and several zip drives, but the court reviewed the constitutionality of all of the searches because the record was unclear about where the photos used at trial had come from. *Id.* at 396–97.

71. United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).

72. *Id.*

73. United States v. Monroe, 52 M.J. 326 (C.A.A.F. 2000).

74. *Id.* at 328.

75. *Id.*

76. *Id.*

77. *Id.* at 330.

78. United States v. Long, 64 M.J. 57, 65 (C.A.A.F. 2006)

audit, as the employers in *Monroe* and *Simons* did.[79]

The contrary results in *Long*, *Simons,* and *Monroe* are somewhat perplexing, as all three public employers had policies warning of regular monitoring and all three e-mail accounts were government accounts on government servers. The *Long* court put weight on the Navy's reason for searching the service member's computer and on the service member's expectation that the Navy might search her computer. Other public-employer cases also weigh the employee's expectation that his computer might be searched.

For example, where the public employer's policy prohibited only theft of the government computer, which the policy broadly defined as "improper use of State equipment" including "conducting personal business on State time," the employee did have a reasonable expectation of privacy in his work computer.[80] The policy did not prohibit storing personal files on the computer, so the employee could not have expected that his computer would be searched.[81] Similarly, where a city did not have a policy addressing personal use and was not in the practice of monitoring and accessing employee computers, a fire marshal who was charged with possession of child pornography had a reasonable expectation of privacy in his computer and e-mail.[82]

In contrast, where a school district had a clear policy that "authorized users must not have and shall have no expectation of privacy in their use of the Computer System," and required users to acknowledge that all computers might be monitored every time they logged on to their computers, a teacher's expectation of privacy in his work e-mail was not reasonable.[83] The teacher's e-mails to his wife therefore were not protected by the marital communications privilege, because he was "aware that his employer had access to the contents of his computer and took no steps to safeguard the electronic messages between him and his wife."[84] Another court denied a Department of Justice employee's motion to suppress e-mails despite his statement that he expected that the

79. *Id.*

80. Leventhal v. Knapek, 266 F.3d 64, 67, 74 (2d Cir. 2001).

81. *Id.* at 74. The court held that even though the employee had a reasonable expectation of privacy, the employer's search was reasonable and did not violate his Fourth Amendment rights. *Id.* at 75.

82. United States v. Slanina, 283 F.3d 670, 677 (5th Cir.), *vacated*, 537 U.S. 802 (2002) ("[G]iven the absence of a city policy placing Slanina on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that Slanina's expectation of privacy was reasonable."). The Supreme Court vacated the judgment and remanded the case for a determination of whether it mattered to the charges that the images might not have been real children in light of the Court's decision in Ashcroft v. Free Speech Coal., 535 U.S. 234 (2002).

83. United States v. Hamilton, 778 F. Supp. 2d 651, 653 (E.D. Va. 2011).

84. *Id.* at 655.

e-mails he sent through the department's computer system were private because he used his Blackberry, on which he also kept private photos.[85] The department's e-mail policy specifically stated that an employee consented to monitoring by his use of department-owned computers and e-mail.[86] Courts are more likely to find a reasonable expectation of privacy where the employer's policy is unclear or allows personal use of a work computer and where the employee is not warned that his employer will be monitoring his work computer use, a pattern we see with the attorney-client privilege cases in Part III.

III. WHEN AN EMPLOYEE WAIVES PRIVILEGE THROUGH E-MAIL

While *O'Connor v. Ortega* and the Fourth Amendment govern public-employer searches of e-mail, the Fourth Amendment does not apply to private employers.[87] However, courts still take into account whether the employee had a reasonable expectation of privacy in his e-mail account when considering whether the employee waived attorney-client privilege by communicating with his attorney on a work computer.[88] A court's determination that the employee should have expected that his e-mail account would be monitored will most likely go toward a finding that he waived attorney-client privilege, while a determination that the employee did have a reasonable expectation of privacy in his e-mail and took precautions to keep his communications private will most likely result in the court finding that the employee did not waive attorney-client privilege.

Private employers routinely monitor workplace e-mail accounts, and as many as 40 percent of employers routinely monitor their employees' e-mail.[89] The employers might look for a variety of reasons—to check on worker productivity, to look for sexual harassment or offensive language

85. United States v. Linder, 12 CR 22–1, 2012 WL 3264924, at *8 (N.D. Ill. Aug. 9, 2012).

86. *Id.* at *5.

87. *See* McCafferty's, Inc. v. Bank of Glen Burnie, 179 F.R.D. 163, 168 (D. Md. 1998); Suburban Sew 'N Sweep, Inc. v. Swiss Bernina, Inc., 91 F.R.D. 254, 256 ("[I]t is elementary that the Fourth Amendment and its accompanying exclusionary rule only apply to conduct of or attributable to the government, and normally do not apply in civil cases").

88. *See, e.g.*, Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 896 (Ct. App. 2011) (employee's expectation of privacy in her e-mail was not reasonable); Curto v. Med. World Comm'ns, Inc., 03CV6327 DRH MLO, 2006 WL 1318387, at *5 (E.D.N.Y. May 15, 2006) (employee's expectation of privacy in her e-mail was reasonable).

89. Corey A. Ciocchetti, *The Eavesdropping Employer: A Twenty-First Century Framework for Employee Monitoring*, 48 AM. BUS. L.J. 285, 307–8 (2011).

and pornography, or to monitor for the transmission of confidential information.[90] Employers are capable of tracking employees' web-based e-mail accounts, such as Gmail or Hotmail, even though employees probably assume that their personal e-mail accounts are safe from employer prying.[91] So Jessica, who uses her web-based e-mail account thinking that her employer will not be able to read the e-mails she sends to her attorney, could be taken by surprise when her employer does gain access to the e-mail and intends to use her e-mails as evidence.

A. Employers' Policies on Work E-mail Use Can Affect the Outcome

Courts generally begin their analysis by considering whether an employee had a reasonable expectation of privacy in her e-mail messages. "The use of a company's computer to transmit and receive e-mails does not alone destroy the confidentiality necessary to preserve a claim of attorney-client privilege."[92] An employer's e-mail policy can play a pivotal role in whether a court finds that an employee had a reasonable expectation of privacy.[93]

Some courts, when considering employer policies, follow a four-part test outlined in *In re Asia Global Crossing, Ltd.*:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[94]

90. *Id.* at 308.

91. *See id.*; *see also Fact Sheet 7: Workplace Privacy and Employer Monitoring,* PRIVACY RIGHTS CLEARINGHOUSE (Jan. 2014), https://www.privacyrights.org/fs/fs7-work.htm#4a ("Messages sent within the company as well as those that are sent from your terminal to another company or from another company to you can be subject to monitoring by your employer. This includes web-based email accounts such as Yahoo and Hotmail as well as instant messages.").

92. *In re* Royce Homes, LP, 449 B.R. 709, 734 (Bankr. S.D. Tex. 2011).

93. *Compare* Kaufman v. SunGard Inv. Sys., CIV.A.05-CV-1236(JLL), 2006 WL 1307882, at *4 (D.N.J. May 10, 2006) ("[A]ny privilege attached to the [e-mails] was waived" because the employee used the e-mail knowing that his employer "could search and monitor email communications at any time."), *with* Convertino v. U.S. Dept. of Justice, 674 F. Supp. 2d 97, 110 (D.D.C. 2009) (employer's policy did not ban personal use, and the employee was not aware of that policy).

94. 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005).

Where employers have a clear policy that e-mail is not to be used for personal reasons and the employer can monitor e-mail at any time, courts often find that employees waived their attorney-client privileges by using work e-mail. One court likened using an employer's e-mail, knowing that the company could access and monitor that e-mail at any time, to "the employer looking over your shoulder each time you send an e-mail."[95] That court explicitly said the employee's use of his work e-mail notwithstanding the employer's e-mail policy, which forbade personal use and stated that employees did not have any privacy in their work e-mail, waived the privilege.[96]

Similarly, where an employer's e-mail policy "provided that all communications transmitted via company property should *not* be considered private, that the company could access and monitor an employee's personal communications at any time, and that employees were prohibited from disseminating confidential information over the company's computer system," the court, applying the *Asia Global* factors, concluded that an employee waived his attorney-client privilege by using his employer's e-mail.[97] The policy was "unquestionably" in force,[98] the employer had explicit guidelines that it could monitor its employees' e-mail at any time,[99] and third parties had access to the employee's e-mail account.[100] Although the employer did not show that the employee had actual notice of its e-mail policy, the court, citing *Asia Global*, said that direct notification to an employee is unnecessary when the policy is memorialized, and that knowledge of the policy could be imputed to a key employee.[101]

While the preceding cases are fairly straightforward — the employer had a clear policy prohibiting personal use of company e-mail and warning that the employer would monitor messages, the employee used the e-mail knowing this policy, and the court held that the employee therefore waived attorney-client privilege — courts have held that the employee waived privilege even when the e-mail policy was less clear. The court in *Smyth v. Pillsbury Co.* held that even when employer had no policy forbidding personal use and in fact repeatedly told its employees that their e-mail would be kept "confidential and privileged," an employee still had no reasonable expectation of privacy in his e-mail.[102]

95. Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 440 (N.Y. 2007).

96. *Id.*

97. *Royce Homes*, 449 B.R. at 733 (emphasis added).

98. *Id.* at 738.

99. *Id.* at 739.

100. *Id.* at 740.

101. *Id.* at 741 (citing *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 259 (Bankr. S.D.N.Y. 2005).

102. 914 F. Supp. 97, 98, 101 (E.D. Pa. 1996).

The employee, using his work e-mail on his home computer, made "unprofessional" comments to his supervisor for which he was later fired.[103] The employee voluntarily used an e-mail system to which the entire company had access, and the court did not find a reasonable expectation of privacy "notwithstanding any assurances that such communications would not be intercepted by management."[104] And when an employee stored e-mail messages in personal folders and under a private password with his employer's consent, the court held that he still had no reasonable expectation of privacy in those e-mails.[105] The employee's e-mail was transmitted over the employer's network and the employee did not protect the e-mails merely by moving them to a folder.[106]

An employer's altering a policy to allow more personal use does not always provide shelter for employees sending personal communications. A clothing store chain changed its policy over the years, from one that strictly prohibited personal e-mail use to one that allowed "limited exceptions" for personal use.[107] An executive of the chain moved to suppress e-mails, arguing that his employer's change in policy over the years amounted to an agreement that the employer would not search e-mails.[108] The court denied his motion, pointing out that the company had "a clear and long-consistent policy" of monitoring employee e-mails that was unaltered by the changes allowing some personal use.[109] The court also rejected the employee's argument that he did not ask his attorney to e-mail him at his work account.[110] It noted that the employee had sent e-mails to his attorney from that account about appointments, so he could have expected his attorney to e-mail him at that account about more substantive matters and should have taken the reasonable precaution of using a different account.[111]

Therefore an employer's monitoring policies can (although not necessarily) play a pivotal role in whether a court finds that an employee had a reasonable expectation of privacy. Different policies can lead to

103. *Id.* at 98.

104. *Id.* at 101.

105. McLaren v. Microsoft Corp., 05-97-00824-CV, 1999 WL 339015, at *4 (Tex. App. May 28, 1999).

106. *Id.*

107. United States v. Finazzo, 10-CR-457 (RRM)(RML), 2013 WL 619572, at *5 (E.D.N.Y. Feb. 19, 2013). Among other matters, the court denied a clothing store chain executive's motion to suppress e-mails in an insider trading case; the executive claimed attorney-client privilege in those e-mails. *Id.*

108. *Id.* at *8.

109. *Id.* at *11.

110. *Id.*

111. *Id.*

different outcomes in cases with otherwise similar facts.

B. What's Different When an Employee Uses a Personal E-mail Account

Two cases with similar facts showcase how courts' analysis changes when an employee uses a personal e-mail account, not a work account, to communicate with her attorney. In the case on which the Emily fact pattern is based, the court held that an employee waived attorney-client privilege when she used her work e-mail to communicate with her attorney.[112] The employer had explicitly warned employees that their work e-mail was not private, that it should not be used for personal business, and that the employer would routinely monitor e-mails and other use of work computers in order to ensure that employees were complying with the policy.[113] The employee used a private password to access her work e-mail, and she deleted the e-mails after they were sent.[114] In spite of these precautions, the court said "her belief was unreasonable because she was warned that the company would monitor e-mail to ensure employees were complying with office policy not to use company computers for personal matters, and she was told that she had no expectation of privacy in any messages she sent via the company computer."[115]

In contrast, where an employer's policy prohibited personal use of company e-mail accounts and warned that the employer could access the company e-mail at any time, but was silent on employees' use of their *personal* e-mail accounts while at work—the case on which the Jessica fact pattern is based—the court held that an employee did not waive the attorney-client privilege by using her work laptop and her personal, web-based e-mail account to communicate with her attorney.[116] The employer argued that the determinative factor was the ownership of the computer and that because the employee used a work laptop, knowing the employer's stated policy on using employer computer resources, she knew her e-mails were subject to employer scrutiny and waived any attorney-client privilege.[117] The court rejected this argument because it was "not clear from that language whether the use of personal, password-

112. Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 896 (Ct. App. 2011).
113. *Id.* at 896.
114. *Id.*
115. *Id.*
116. Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010).
117. *Id.* at 658.

protected, web-based e-mail accounts via company equipment is covered" and the employee did not have notice that her e-mail would still be subject to company monitoring if she used her personal e-mail account on a work computer.[118]

The *Holmes* and *Stengart* employees both used work equipment to send e-mails to their attorneys, and both employers had policies prohibiting the use of work systems to send e-mails. However, the courts came to opposite conclusions about whether the employees waived attorney-client privilege. The only distinguishable difference in the two cases is that the *Stengart* employee—"Jessica"—used her personal e-mail account, while the *Holmes* employee—"Emily"—used her work e-mail.

Courts confronted with Jessica's situation—where an employee has used her personal, web-based e-mail account on an employer's computer and the employer wants to introduce the e-mails into evidence—are more likely to hold that attorney-client privilege protects the e-mails than are courts in Emily's situation—where an employee has used her work e-mail account.

In addition to *Stengart*, several cases hold that the employee did not waive attorney-client privilege. For example, in *Curto v. Medical World Communications*, an employee who used her work-provided laptop and her web-based, personal e-mail account to communicate with her attorney did not waive the attorney-client privilege even though her employer had a policy that stated: "Employees should not have an expectation of privacy in anything they create, store, send, or receive on the computer system."[119] The employee exclusively used her America Online e-mail account to communicate with her attorney and deleted all the materials that she had saved on the work laptop before returning the laptop.[120] The court upheld a magistrate judge's order that the employee did not waive attorney-client privilege by using her work laptop because she took precautions including deleting documents and not using her work e-mail account, and because the employer had a history of not enforcing its e-mail and computer policy.[121] The lax enforcement left employees with a "false sense of security" that "lulled" them into thinking that the policy would not be enforced.[122] The court treated the lack of enforcement as part of the reasonableness of the precautions the

118. *Id.* at 659.

119. 03CV6327 DRH MLO, 2006 WL 1318387, at *1 (E.D.N.Y. May 15, 2006).

120. *Id.*

121. *Id.* at *3 (citing Minute Entry For Proceedings Held Before Michael L. Orenstein at 34; Curto v. Med. World Comm'ns, Inc., 03CV6327 DRH MLO, 2006 WL 1318387 (E.D.N.Y. May 15, 2006)).

122. *Id.*

employee took—she had reason to believe that the employer would not use forensic software to check her work laptop because it had not done so previously, and she was careful to use her AOL account only.[123]

Similarly, an employee who left the passwords to his Hotmail and Gmail accounts pre-populated on his work computer did not waive the privilege attached to e-mails to his attorney.[124] The employer had a policy prohibiting the use of personal e-mail accounts on the company system: "e-mail users have no right of personal privacy in any matter stored in, created on, received from, or sent through or over *the system.* This includes the use of personal e-mail accounts *on Company equipment.*"[125] However, there was no evidence that the employee had opened the particular e-mails at issue on his work computer.[126] The employee had a reasonable belief that his communications, sent from his personal e-mail account and his home computer, would remain private even though he left his password populated on his work computer.[127] The *Pure Power* employee, like the *Curto* employee, did not waive the privilege even though he used his work computer and his employer had a clear policy that work computers were not private.

An employee similarly did not waive the attorney-client privilege by using his own Yahoo! e-mail account on his work laptop.[128] His employer had a policy governing use of work e-mail that permitted personal use but warned that the employer could read work e-mail at any time.[129] However, the policy was silent about the use of personal e-mail on work computers and did not warn that it would be possible for an employer to retrieve messages composed on a work computer.[130] The court was concerned about the practicality of holding that attorney-client privilege was waived in this case:

> 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. If they used the company laptop to send or receive any e-mails, the e-mails would not be privileged because the "screen shot" temporary file could be accessed by the company. If they used the hotel computer to avoid this risk, the communication would still not be privileged because the

123. *Id*.

124. Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 565 (S.D.N.Y. 2008).

125. *Id*. at 552–53.

126. *Id*. at 556.

127. *Id*. at 565.

128. Nat'l Econ. Research Assocs. v. Evans, CIV.A. 04-2618-BLS2, 2006 WL 2440008, at *5 (Mass. Aug. 3, 2006).

129. *Id.* at *3.

130. *Id.*

> hotel could access the temporary file on its computer. 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.[131]

Another court shared the *Evans* court's concerns about public policy, holding that communications sent from a personal e-mail account on a work computer should be protected "to preserve the sanctity of communications made in confidence."[132] The plaintiff in *Sims v. Lakeside School*, a teacher, used both his school e-mail and his personal, web-based e-mail on his school laptop to communicate with his attorney and with his wife.[133] The school district had a clear policy stating that school e-mail accounts were the property of the district and that district officials had the right to inspect school laptops at any time.[134] Because the plaintiff was aware of this policy, he had no privacy expectation in his laptop or in his school e-mail.[135] However, the court held that he did have an expectation of privacy in his personal e-mail, even if he used it on his school laptop, and that "any material he created to communicate with his attorney and his spouse" was protected by the attorney-client privilege and the marital communications privilege, respectively.[136] Notably, the court held that the privilege covered anything the plaintiff created for his attorney, even if he stored the material on his school laptop, in which the court concluded the plaintiff had no expectation of privacy.[137]

The employees in *Evans, Curto, Pure Power*, and *Sims* all used work machines and web-based e-mail accounts, and courts held that all of them maintained the attorney-client privilege. These decisions and others like them would seem to indicate that an employee like Jessica who uses a personal e-mail account on a work system does not waive the attorney-client privilege by doing so.

131. *Id*. at *5.

132. Sims v. Lakeside Sch., C06-1412RSM, 2007 WL 2745367, at *2 (W.D. Wash. Sept. 20, 2007).

133. *Id*. at *1.

134. *Id*.

135. *Id*.

136. *Id*.

137. *Id*. at *2 ("[T]o the extent that the laptop contains web-based e-mails sent and received by plaintiff . . . and *any other material* prepared by plaintiff . . . to communicate with his counsel, the Court agrees with plaintiff that such information is protected under the attorney-client privilege and the marital communications privilege." (emphasis added)).

V. WHY PERSONAL E-MAIL IS DIFFERENT

So why should the courts treat Emily different from Jessica, and hold that Emily has waived the attorney-client privilege by using her employer's e-mail system? Three things point to justifying this distinction. First, electronic privacy laws draw a distinction between communications systems open to the public and those that are private. Second, the public policy concerns that bothered the courts in *Evans* and *Sims* only apply to employees' personal e-mail accounts. Third, while an employee might reasonably expect that her boss can read her work e-mail, she does not reasonably expect that her boss will be able to piece together her personal e-mail from her work computer's hard drive.

A. Public and Nonpublic Providers

The Stored Communications Act ("SCA") treats "public" and "nonpublic" e-mail providers differently.[138] Nonpublic e-mail suppliers, which would include company e-mail systems only open to employees, may disclose the contents of e-mail.[139] However, the SCA restricts public e-mail providers, which include any provider of e-mail that is open to the world at large, including web-based e-mail services like Gmail and Hotmail.[140] A public electronic communications service many only voluntarily disclose the contents of the communication to a subscriber or the intended recipient unless an exception applies.[141]

The SCA might provide more protection to public providers than nonpublic because "nonpublic accounts may exist more for the benefit of providers than for the benefit of users" while "an individual who contracts with a commercial ISP available to the public usually does so solely for his own benefit."[142] A user may therefore view his public e-mail account—the one he has through a webmail service—as his own, private account, while he views his work e-mail account as the account

138. 18 U.S.C. §§ 2701–2712 (2013).

139. 18 U.S.C. § 2702(a) (2013).

140. *Id.*; *see also* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998).

141. 18 U.S.C. § 2702(a). The exceptions all refer to requests or search warrants from governmental entities. *See* 18 U.S.C. §§ 2702–03. Section 2702 regulates when a service provider may voluntarily disclose information, while Section 2703 regulates when a service provider is compelled to disclose the information)

142. 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, 1226–27 (2004).

for work matters.[143] Indeed, one court, in granting a motion to compel production of an employee's work e-mails, noted that he had told his attorney to switch to his personal e-mail account so he would not "leave any more tracks."[144] The court noted that the statement showed the employee recognized that he should treat his work e-mail account differently than his personal account, even though there was no evidence the employer monitored employees' e-mail.[145] The law recognizes this difference by treating public and nonpublic providers differently.[146]

Under the SCA, an employer is not even allowed to directly access an employee's personal account without violating the statute. The court in *Pure Power Boot Camp v. Warrior Fitness Boot Camp*, which also held that an employee did not waive attorney-client privilege by using his Hotmail account on his employer's computer, noted that the employer's action in accessing the employee's personal Hotmail account was an SCA violation.[147] The employee had a subjective belief that his personal e-mail was private, and his belief was objectively reasonable despite the fact that he left his passwords pre-populated on his work computer.[148] The employee did not authorize his employer's access just by leaving the passwords in his browser.[149] The court specifically said that if the e-mails came from the employee's *work* account, the case would have a different outcome.[150]

The *Pure Power* court also distinguished between the e-mails that the employer directly accessed and those that it retrieved from the employee's work computer.[151] In most of the attorney-client privilege cases, the employer gets the e-mails from cached data on the work computer that the employee used and the SCA will not apply to the employer's retrieval of the e-mails.[152] However, the SCA is still instructive in that it does treat public e-mail providers differently than non-public e-mail providers.

143. "In practice, the public/nonpublic line often acts as a proxy for the distinction between a user's private account and one assigned to him by his employer." *Id.* at 1227.

144. *In re* Info. Mgmt. Servs., Inc. Derivative Litig., 81 A.3d 278, 285 (Del. Ch. 2013).

145. *Id.*

146. Kerr, *supra* note 142, at 1227.

147. Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 559–60 (S.D.N.Y. 2008).

148. *Id.* at 561.

149. *Id.*

150. *Id.* at 559.

151. *Id.* at 561.

152. *See, e.g.*, Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010); Sims v. Lakeside Sch., C06-1412RSM, 2007 WL 2745367, at *2 (W.D. Wash. Sept. 20, 2007); Curto v. Med. World Comm'ns, Inc., 03CV6327 DRH MLO, 2006 WL 1318387, at *1 (E.D.N.Y. May 15, 2006).

B. Courts' Policy Concerns Only Apply to Personal E-mail

Practically, it does not make sense to require that employees have their own, personal computers in order to have an e-mail account that is not subject to their employers' review. The court in *Evans* had particular concern about the practical ramifications of holding that the attorney-client privilege was waived whenever an employee accessed his e-mail using a work computer.[153] The same concern does not hold true when an employee accesses her work e-mail. In most cases, the employee will only be able to access work e-mail on a work computer. Even when the employer provides some kind of web-based access, the employee still will be sending e-mail through the employer's system no matter which computer he uses. The *Evans* court was much less concerned about the policy ramifications of waiving the attorney-client privilege when the employer used his work e-mail account, saying that the employee "could not reasonably expect to communicate in confidence with his private attorney" if he had used his work account to send the e-mails.[154]

The *Sims* court was equally concerned, writing that "public policy dictates that such communications shall be protected to preserve the sanctity of communications made in confidence."[155] But *Sims* did not extend that sanctity to the employee's work e-mail, holding that he had no reasonable expectation of privacy in his *work* e-mail account.[156]

An employee without a computer at home might only check even a personal e-mail account while at work. And an employee, like Jessica, who exclusively uses a work-provided laptop, would not be able to compose most e-mails comfortably without having to use a work computer.[157] As the *Evans* court articulated, waiving the attorney-client privilege for using a personal account on a work computer would leave some employees without a means to communicate electronically with their attorneys at all.

These employees would probably turn to public computers or even friends' computers, as did a woman who used her fiancé's computer and e-mail account rather than her work-provided computer to communicate with her attorney.[158] Although the court held that the woman did not

153. Nat'l Econ. Research Assocs. v. Evans, CIV.A. 04-2618-BLS2, 2006 WL 2440008, at *3 (Mass. Aug. 3, 2006).

154. *Id.* at *8.

155. *Sims*, 2007 WL 2745367, at *2.

156. *Id.*

157. While an increasing number of people access their e-mail through smartphones, phones are not ideal for composing long messages.

158. Geer v. Gilman Corp., 306 CV 889 JBA, 2007 WL 1423752, at *1 (D. Conn. Feb. 12, 2007).

waive the attorney-client privilege by using her fiancé's account, the case could easily have gone the other way.[159] The woman risked waiving the attorney-client privilege by having a third party see her messages, and it was only the closeness of the relationship between the two that preserved the privilege. Holding that employees who use their own e-mail accounts on employers' machines have waived their privilege would force other employees into similar positions, and would open them up to waiving the privilege because they used another's computer.

C. Reasonable Expectations of Privacy

Most courts hold that an employee does have a reasonable expectation of privacy in the contents of her personal e-mail.[160] Courts' determinations about whether an employee has a reasonable expectation of privacy in her unmonitored work e-mail vary, although most courts hold that an employee does not have a reasonable expectation of privacy where the employer had a clear policy that e-mail would be monitored.[161]

An employee like Jessica reasonably expects that her personal account is private—indeed, that's why she would choose to send e-mails to her attorney from that account and not her work account. "When an e-mail exchange using a work account turns to private matters, it is common for a user to move the discussion to a commercial account. 'I don't want my boss to read this,' a user might note, 'I'll e-mail you from my personal account later.'"[162]

The *Stengart* employee did not waive attorney-client privilege precisely because of the precautions she took in using her personal e-mail account.[163] So did the *Curto* employee, who believed she had deleted all the documents she saved before returning her work laptop.[164] Even the *Pure Power* employee, who left his passwords populated on his work browser, still had what the court termed a reasonably objective expectation of privacy in his personal e-mail accounts because they did

159. *Id.* at *4.

160. *See* Stengart v. Loving Care Agency, Inc., 990 A.2d 650, 655 (N.J. 2010); Curto v. Med. World Comm'ns, Inc., 03CV6327 DRH MLO, 2006 WL 1318387, at *3 (E.D.N.Y. May 15, 2006).

161. *See In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005); Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 898 (Ct. App. 2011); Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 440 (N.Y. 2007).

162. Kerr, *supra* note 142, at 127; *see also In re* Info. Mgmt. Servs., Inc., Derivative Litig., 81 A.3d 278, 285 (Del. 2013) (employee telling attorney he was switching to his personal e-mail account for further communications).

163. *Stengart*, 990 A.2d at 663.

164. *Curto*, 2006 WL 1318387 at *1.

not fall under his employer's e-mail use policy.[165] Conversely, the employee in *Holmes,* using her work account, waived the attorney-client privilege even though she used a private password and deleted the e-mails after she sent them.[166]

So while Jessica and Emily may both have subjective expectations of privacy in the e-mails they exchanged with their attorneys, a court would likely deem Jessica's expectation objectively reasonable, but not Emily's. Even though it's possible to reconstruct e-mails sent from web-based e-mail accounts, employees' likely common understanding of how e-mail works is that web-based accounts are not downloaded onto computers. An employee like Jessica would not be likely to know that her employer could in fact retrieve her e-mail.

CONCLUSION

While the safest course of action for an employee to preserve the attorney-client privilege is for that employee to use only her own computer and e-mail account to communicate with her attorney, doing so is not practical for many employees. It does not make sense to treat an employee like Jessica who uses her personal, web-based e-mail the same as one like Emily who uses her work e-mail account. Although decisions on work e-mail vary across jurisdictions, nearly every court that has decided the issue has held that an employee who uses a personal account on a work computer does not waive the attorney-client privilege even though the employer was able to retrieve the e-mails. This difference does make sense in light of the different expectations employees generally have of their work e-mail accounts as opposed to their personal e-mail accounts and the different way the law treats these services.

165. Pure Power Boot Camp v. Warrior Fitness Boot Camp, 587 F. Supp. 2d 548, 565 (S.D.N.Y. 2008).

166. 119 Cal. Rptr. 3d at 896.