CLICKING AWAY CONFIDENTIALITY:
WORKPLACE WAIVER OF ATTORNEY-CLIENT PRIVILEGE

Adam C. Losey

I. INTRODUCTION: BARBARA HALL AND HER DAUGHTERS

Barbara Hall, an administrative assistant, often arrives an hour and a half early to work solely to check her personal emails[1] on her employer's computer.[2] Afterwards, "[i]n the grand tradition of Chekhov, or perhaps 'Days of Our Lives,' Barbara 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."[3] When she gets home from work, Barbara continues to use her workplace email account to send personal emails.[4]

Barbara Hall and her daughters are not alone. The average employee is estimated to

---

[1] "The abbreviated version of 'electronic mail' has been written as 'email,''e-mail,''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), *available at* http://www.stc.org/confproceed/2001/PDFs/STC48-000133.pdf. Recently, the Court has used both "email" and "e-mail" within the same opinion. *Compare* Federal Election Com'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. The most commonly used and accepted form is "email" and it will be used throughout this note, but the usage of other forms in quotations will not be treated as mistakes. *See* Press Release, Infocrossing, Email or e-mail—to hyphenate or not? (Jun. 26, 2005) ("With the hyphen you get almost 68 million [search] results [on Google]. But if you drop the hyphen, you get nearly ten times as many—650 million!"), *available at* http://www.intellireach.com/Company/press_releases/PR_Jan_26_2005.asp.

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

[3] Hafner, *supra* note 1, at G1.

[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.'" Hafner, *supra* note 1, at G1.

spend nearly an hour a day on personal internet use.[5] While this behavior at work may be economically detrimental,[6] "[v]ery few companies today have a rule against all personal use of electronic communication [and] [e]mployers are becoming more realistic about people's need to send an occasional personal message from work."[7] Few companies will fire an employee solely for sending a personal email from work,[8] and the modern corporate attitude towards personal email in the workplace is one of begrudged tolerance coupled with surveillance.[9]

In 1996, 35% of businesses monitored employee internet use.[10] In 2006, the number grew to over 80%.[11] "[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."[12] While an estimated 90% of companies that monitor employee

---

[5] *Is That Work Related?*, 24 No. 5 Legal Mgmt. 8, at *8 (Sept./Oct. 2005).

[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) (citation omitted).

[7] Larry Keller, *Monitoring employees: Eyes in the workplace*, CNN.COM, Jan. 2, 2001, http://archives.cnn.com/2001/CAREER/trends/01/02/surveillence/; *see also* Nathan Watson, *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.").

[8] However, many companies are firing employees for email misuse. "Increasingly, employers are fighting back by firing workers who violate computer privileges. Fully 26% of employers have terminated employees for e-mail misuse." Nancy Flynn, *2006 Workplace E-Mail, Instant Messaging & BLOG Survery*, American Management Association and the ePolicy Institute (2006). *See also* Kim Zetter, *Employers Crack Down on Personal Internet Use*, PC WORLD MAGAZINE, August, 2006, 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." Larry Keller, *Monitoring employees: Eyes in the workplace*, CNN.COM, Jan. 2, 2001, http://archives.cnn.com/2001/CAREER/trends/01/02/surveillence/.

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

[11] *Id.*

[12] Nancy Flynn, *2005 Electronic Monitoring & Surveillance Survey*, American Management Association and the ePolicy Institute (2005).

communications notify their employees about the possibility of monitoring,[13] many employees are oblivious to the fact that a permanent record may exist of their internet and email use at work.[14]

This ignorance has resulted in serious consequences for employee litigants. American[15] courts have held that employers are generally free to monitor[16] employee computer use.[17] Even government employers and supervisors can monitor employee computer usage without probable cause.[18] However, this Note discusses workplace monitoring of a specific type of communication that has been extended special legal protections throughout history.[19]

Employees who email an attorney from the workplace, or from a workplace email

---

[13] Kyle Schurman, *E-mail & Your Legal Rights*, SMART COMPUTING, July, 2001, at 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*?, 24 No. 5 Legal Mgmt. 8, at *8 (September/October 2005).

[15] This is not the case in most European countries. *See generally* Kesan, *supra* note 6, at 307-11 (discussing the interplay of privacy laws and employer surveillence of employees in the United Kingdom, France, Germany, and Italy).

[16] 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. *E.g.*, Doe v. XYC Corp. 887 A.2d 1156, 1162 (N.J. Super. Ct. App. Div. 2005) ("The duty to monitor employee's internet activities does not exist.").

[17] For an a critical discussion of employer-employee privacy law in the United States, *see generally* Rafael Gelly, *Distilling the Essence of Contract Terms: An Anti-Antiformalist Approach to Contract and Employment Law*, 53 FLA. L. REV. 669, 671 (2001) (discussing and criticizing "[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.").

[18] *See* United States v. LeBlanc, 490 F.3d 361, 365 (5th Cir. 2007).

[19] *See* Ken M. Zeidner, *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."); Max Radin, *The Privilege of Confidential Communication Between Lawyer and Client*, 16 CAL. L. REV. 487, 488 (1927-28) ("Advocates from very ancient times could not be called as witnesses against their clients while a case was in progress. Cicero in prosecuting the Roman governor of Sicily regrets that he cannot summon the latter's patronus, Hortensius.").

account,[20] may lose the evidentiary protections of attorney-client privilege.[21] This loss of privilege subsequently allows an employer to forensically recover[22] a current or former employee's otherwise privileged emails to use against the employee in litigation.[23] This is particularly devastating to the employee, as these types of emails are often damning.[24] The employee's lawyer may well even be vulnerable to a malpractice lawsuit for failing advise the employee on how to take precautions to avoid waiver.[25]

The typical workplace waiver factual background involves an employee, using an employer-owned computer, communicating with an attorney regarding an action detrimental to the employer.[26] The employer always has some sort of written policy providing notice to

---

[20] Courts have acknowledged that "sending a message over [a company's] e-mail system [is] like placing a copy of that message in the company files[,]" and is thus synonymous to using an employer-owned computer. *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 common law. *E.g.*, FED. R. EVID. 501. When a claim or defense is governed by state law (e.g., in a diversity action), however, 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." CHRIS 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 email, 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 looks at or composes an email, a forensic expert may be able to later recover the email regardless of whether the email was intentionally saved on the computer.

[23] *See* FED. R. EVID. 801(d)(2)(A).

[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 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. Medical World Communications, Inc., 2006 WL 1318387 at *8 (E.D.N.Y. 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, 180 n.160 (1995).

[26] *See e.g.*, Kaufman v. SunGard Inv. System, 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

employees that their computer usage is subject to monitoring.[27]

In these workplace waiver cases,[28] a schism is quietly developing. Some courts are

---

SunGard's acquisition of OSI's assets and hiring of Kaufman as a senior executive . . . [e-mails related to this litigation] were sent from and received on SunGard's e-mail system during Kaufman's employment with SunGard."); Long v. Marubeni America Corp., 2006 WL 2998671, at *1 (S.D.N.Y. Oct. 19, 2006) (employee's Kevin Long and Ludvic Presto used their employers 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 v. Med. World Commc'ns, Inc., 2006 WL 1318387 at *1-2 (E.D.N.Y. May 15, 2006) (employee Curto used an assigned company-owned laptop to frequently email her attorney concerning an EEOC complaint against her employer); Nat'l Econ. Research Assocs., Inc. v. Evans, 2006 WL 2440008 at *1 (Mass. Super. Ct. Aug. 03, 2006) (Employee Evans used his employer's computer to email 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, 695-96 (Va. 2007) (employee Cook used his employer's computer to prepare, print, and delete a privileged document to send to his attorney regarding legal action detrimental to his employer).

[27] *See e.g.*, *Kaufman*, 2006 WL 1307882 at *4 ("SunGard policy also 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 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 a provisions in the employer's policies and procedures manual stating the employee emails "are subject to monitoring"); *Curto*, 2006 WL 1318387 at *1 (employee handbook stated that "[t]he computers and computer accounts given to employees are to assist them in the performance of their jobs. 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."); *Long*, 2006 WL 2998671 at *1 (employee handbook stated that personal use of company computers was prohibited, and that an 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]."); *Banks* 650 S.E.2d at 698 ("employee handbook provided that there was no expectation of privacy regarding [company computers].").

[28] The phrase "workplace waiver cases" is used throughout this Note to refer to cases that (1) have a factual background similar to that described *supra* in notes 26-27 and accompanying text, and (2) address the legal question of whether an employee's otherwise

discretely (and perhaps inadvertently) abandoning the traditionally accepted narrow interpretation of attorney-client privilege in favor of a broad protective approach, on public policy grounds.[29] Others continue to adhere to traditional doctrine.[30] A clash between these two schools of thought is inevitable.[31]

Barbara Hall's email conversations with her daughters "range from the mundane business of trading recipes to the more textured landscape of family illness and romantic relationships[,]"[32] and would not likely be protected by attorney-client privilege.[33] Yet, if Barbara were to email an attorney to ask if she might be fired for sending personal emails on company time,[34] her otherwise privileged email could likely be used against her by her employer in any future litigation.[35] She would then find herself out of work, and finally forced to use a personal email account for personal email.

Part II of this note discusses attorney-client privilege, and points out the growing and unspoken abandonment of traditional approaches in these non-traditional cases. Part III of this note 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 suggests methods for determining when attorney-client privilege should protect data stored on an employer-issued computer or email system[36] from discovery. Finally, Part VI discusses the future of workplace waiver jurisprudence.

II. ATTORNEY-CLIENT PRIVILEGE

A. *The Traditional Approach*

Attorney-client privilege protects from discovery confidential communications made

---

privileged communication has lost its protected status and is thus presumably admissible against the employee by his or her employer.

29 *See* discussion *infra* Parts II.B, V.C.

30 *See* discussion *infra* Parts II.A, V.C.

31 *See* discussion *infra* Part V.C.

32 Hafner, *supra* note 1, at G1.

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

34 To which the attorney should respond "yes." *See supra* note 8.

35 *See* FED. R. EVID. 801(d)(2)(A).

36 *See supra* note 20.

between an attorney and client made for the purpose of obtaining legal assistance.[37] 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. The privilege recognizes that sound legal advice or advocacy serves public ends and that such advice or advocacy depends upon the lawyer's being fully informed by the client.[38]

Yet, as discovery is intended to be broad and inclusive,[39] the Court noted in 1947 that "privilege limitation must be restricted to its narrowest bounds[.]"[40] In 1961, Professor Wigmore stated that,

> Its benefits are all indirect and speculative; its obstruction plain and concrete . . . It is worth preserving for the sake of a general policy, but it is nonetheless an obstacle to the investigation of truth. It ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle.[41]

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[,]"[42] with the court's thumb on the scale favoring waiver. In workplace waiver cases,[43] application of the traditional approach would involve 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. This traditional approach may now be obsolete.

B. *The Modern Approach*

When Wigmore and the Court originally advocated the narrow construction of attorney-

---

[37] *See* Bryan S. Gowdy, Note, *Should the Federal Government have an Attorney-Client Privilege?*, 51 FLA. L. REV. 695, 697 (1999).

[38] Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

[39] The Court often references "the broad discovery authorized by the Federal Rules of Civil Procedure. . . ." Codd v. Velger, 429 U.S. 624, 638 (1977).

[40] Hickman v. Taylor, 329 U.S. 495, 506 (1947).

[41] 8 Wigmore, Evidence § 2291 at 554 (McNaughton ed.1961).

[42] Suburban Sew 'N Sweep, Inc. v. Swiss-Bernina, Inc., 91 F.R.D. 254, 257 (N.D. Ill. 1981).

[43] *See supra* note 28.

client privilege, personal computers and email did not exist.[44] Technology has since revolutionized interpersonal communications,[45] and attorney-client communication now regularly occurs in a manner and form that would be completely alien to Wigmore. Email is *sui generis*; it combines the accountability of a pen-and-ink letter with the convenience of a phone call.[46] It can be instantly accessed from a personal computer anywhere in the world, and it has blurred the line between formal correspondence and casual communication.[47]

Antiquated legal rubrics may not be applicable to modern legal questions involving email. In an attempt to honor the policies behind attorney-client privilege,[48] some courts have deemed it necessary to break with tradition and interpret the privilege broadly.[49] This broad interpretation has created, when applied, a judicially-created bulwark protecting employees against what some judges view as an unfair practice by employers.[50] If this broad interpretation

---

[44] While email has arguably been around since the late 1960's, email did not exist in its modern form until October 1971, when an engineer named Ray Tomlinson chose the '@' symbol for email addresses and wrote software to send the first network email. Barry M. Leiner Et. Al., *A Brief History of the Internet*, http://arxiv.org/abs/cs/9901011.

[45] *See e.g.*, Stephen J. Snyder & Abigail E. Crouse, *Applying Rule 1 in the Information Age*, 4 SEDONA CONF. J. 165, 167 (2003) ("email has revolutionized the way people communicate.").

[46] As a phone call can be made from any phone hooked up to a telephone service provider, email 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*, COMPUTERWORLD UK, June 12, 2007, http://www.techworld.com/news/index.cfm?NewsID=9119 140-41. As in correspondence by letter, a permanent record exists of the communication. Some argue that the existence of these two qualities in a single medium of communication is dangerous, 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. It is clear, however, that email is here to stay.

[47] For better or worse. *See infra* note 60 and *supra* note 46.

[48] *See infra* section II A.

[49] *See e.g.*, Sims v. Lakeside School, 2007 WL 2745367 at *2 (W.D. Wash. Sept. 20, 2007) ("public policy dictates that [privileged] communications shall be protected to preserve the sanctity of communications made in confidence.") (citation omitted).

[50] *See infra* Part IV.A-B.

is adopted in workplace waiver cases,[51] employers would still be permitted to monitor employee communications, but they would be prevented them from using these communications against an employee in litigation. Although no court has explicitly articulated this broadened approach, at least one court has undoubtably adopted it.[52] Another court attempted to finesse around the traditional approach by explaining that "[i]n stating that we construe the privilege strictly, we do not mean that it is disfavored[,]"[53] while the court's reasoning suggested the application of the broad approach.

This broadened approach is not unprecedented. "Historically, the attorney-client privilege subordinates the need for information to determine truth to the need for a sphere of autonomy[.]"[54] Courts have been slowly backing away from the traditional approach in certain situations; "because the privilege carries through policy purposes-encouraging attorney-client communication to enhance compliance with the law and facilitating the administration of justice, the Supreme Court has not applied it mechanically."[55]

C. *The Chilling Effects*

It is unclear if any chilling effects would result from adhering to a traditional interpretation of attorney-client privilege in workplace waiver[56] situations . Nothing prevents an employee in the workplace or at home from communicating with an attorney on a personally

---

51 *See supra* note 28.

52 *See supra* note 49.

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

54 *See* 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).

55 *In re Teleglobe*, 493 F.3d at 360.

56 *See supra* note 28.

owned computer,[57] or via another medium of communication.[58] The argument that "personal communications with [the employee's] attorneys were exchanged at the office out of necessity arising from the long business hours at [the employee's workplace]"[59] has been used to tie the exclusion of evidence to the purpose of the privilege in workplace waiver cases. While this argument was ignored for procedural reasons by one court,[60] essentially the same reasoning was used by another as justification for its decision to protect privileged emails.[61]

I is clear that an overworked employee could bring a personal computer into work and email his attorney from his personal email account,[62] or could pick up the telephone to speak with his attorney in lieu of sending an email. It is not unusual for an employee to routinely bring a personal computer to work,[63] and some undoubtably already use the telephone to communicate

---

[57] This is based on the assumption that the employee owns a personal computer, and has internet access. Approximately 90% of American families with an annual household income over $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 6 (2005), http://www.census.gov/population/www/socdemo/computer.html. This number has likely risen since 2003, and will continue to rise. *See supra* note 46. As an employee consulting an attorney to obtain legal advice is likely to have an annual household income of over $50,000, the underlying assumption is reasonable.

[58] Phone calls, letters, and face-to-face conversations are not yet antiquated to the point of obsolescence. Ample alternatives to email remain for an employee to privately communicate with their attorney.

[59] *Kaufman*, 2006 WL 1307882 at *4

[60] *Id.*

[61] *See* Nat'l Econ. Research Assocs., Inc. v. Evans, 2006 WL 2440008 at *5 (Mass. Super. Ct. Aug. 03, 2006) ("[i]f [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. . . . [p]ragmatically, 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."

[62] However, bringing in a personal computer might not be enough to avoid employer surveillence, as the employee would likely be forced to use the employer's internet connection or network to send email. *See supra* note 20.

[63] *See, e.g.*, 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."); United States v. Barrows, 481 F.3d 1246, 1247 (10th Cir. 2007) ("Mr. Barrows brought his personal computer to work."); United States v. Murray, 2007 WL 1704288 at *1 (N-M. Ct. Crim. App. 2007) ("the appellant sometimes brought his personal laptop computer to work so that he could

with counsel at work. Still, denying privilege in these cases could chill attorney-client communication in a significant way.

Email is particularly useful for legal communications,[64] 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.[65] 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.[66] If an employee's privileged communications with an attorney can be intercepted without his knowledge and used against him, the employee has a strong incentive to avoid seeking legal advice. This is the very chilling effect that the privilege is designed to prevent..

D. *The Crime-Fraud Exception*

A major exception to the attorney-client privilege is the crime-fraud exception; a communication will not be privileged if it was made in furtherance of a crime or fraud.[67] The purpose of the crime-fraud exception is to assure that the "seal of secrecy" between lawyer and client does not extend to communications made for the purpose of obtaining advice for the commission of a fraud or crime.[68]

Following this reasoning, courts have been unsympathetic to employees who use employer-issued computers to commit crimes, and subsequently seek the protections of the

---

listen to music while working."); Gernady v. Pactiv Corp., 2005 WL 241472 at *8 (N.D. Ill. 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.").

64 This is as email uniquely combines the convenience of a phone call with the accountability of a pen-and-ink letter. *See supra* note 46. However, there are some critics of email. "'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 Can't Build: A Sentence*, N.Y. TIMES, Dec. 17 2004, at 24 (quoting R. Craig Hogan).

65 *See supra* note 62.

66 "[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 (Bob Hepple ed., 2002).

67 *See* United States v. Zolin, 491 U.S. 554, 563 (1989).

68 *Id.*

attorney-client privilege.[69] One New York court declined to extend attorney-client privilege to a personal computer that was linked to a crime,[70] stating that attorney-client privilege does not extend to physical property where "reasonable grounds" exist to believe such property was used in a crime.[71] This doctrine could be used outside of a criminal context to defeat employee privilege claims. If an employee used a workplace computer or email account to commit a crime against the employer, the employee's commission of a crime might also defeat their claim of privilege in a civil lawsuit.

Taking this reasoning a step further, the Supreme Court of Kentucky has placed the "'breach of fiduciary relationship on an equal par with fraud and deceit' for the purpose of the crime-fraud exception to the attorney-client privilege."[72] Thus, if an employee were to be found to owe a fiduciary duty of loyalty to an employer,[73] and to have breached that duty, a claim of privilege could fail on crime-fraud grounds.[74] In workplace waiver[75] cases, the employee is often communicating with an attorney regarding an action detrimental to the employer,[76] a clearly disloyal act.[77]

---

[69] *See* Kelcey Nichols, *Hiding Evidence From the Boss: Attorney-Client Privilege and Company Computers*, 3 SHIDLER J. L. COM & TECH. 6, 6 (2006) ("Courts may be less likely to grant attorney-client privilege when the computer in question contains information relevant to a crime.").

[70] *In re* Grand Jury Subpoena, 770 N.Y.S.2d 568, 574 (N.Y. Sup. Ct. 2003).

[71] *Id.*

[72] Invesco Institutional, Inc. v. Paas, 244 F.R.D. 374, 378-79 (W.D. Ky. 2007) (citation omitted).

[73] "Employees owe a fiduciary duty to their employers[.]" Susan R. Klein, *Lies, Omissions, and Concealment: The Golden Rule in Law Enforcement and the Federal Criminal Code*, 39 TEX. TECH L. REV. 1321, 1342. An employee is prohibited from acting in any manner inconsistent with his agency and is bound to exercise good faith in the performance of his duties. Western Elec. Co. v. Brenner, 41 N.Y.2d 291, 294 (N.Y. 1977).

[74] *Id*.

[75] *See supra* note 28.

[76] *See supra* note 26.

[77] To illustrate, assume employee Abe works for employer Widget, Inc. Abe emails attorney Ralph from work to ask about any legal ramifications that would arise if he quit his job with Widget, Inc. and formed his own competing business, called Digit, Inc. If his email is intercepted or recovered by Widget, Inc., they could claim that Abe has breached his duty of loyalty to Widget, Inc. and thus any claim of privilege Abe makes regarding his email to Ralph must fail under the crime-fraud exception.

E. *The Work Product Doctrine*

The work-product doctrine[78] is a federal doctrine derived from *Hickman v. Taylor*,[79] and is now codified in the Federal Rules of Civil Procedure.[80] It is distinct from and more expansive than attorney-client privilege.[81] "In [a] civil context, work-product protection is not absolute, but is a 'qualified privilege or immunity'"[82] 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.[83]

"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."[84] 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."[85]

As some courts treat waiver questions differently for attorney-client privilege and work product doctrine,[86] an employee's claim of work product protection might be stronger than the employee's attorney-client privilege claim in a workplace waiver[87] situation.[88] In many cases

---

78 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).

79 29 U.S. 495 (1947).

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

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

82 United States v. Armstrong, 517 U.S. 456, 474 (1996).

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

84 *See Hickman*, 329 U.S. at 512-13.

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

86 *Id*.

87 *See supra* note 28

88 This approach hasn't 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 America Corp., 2006 WL 2998671, at *4 (S.D.N.Y. Oct. 19, 2006) (employee waived attorney-client privilege and work product protections; Curto v. Med. World Commc'ns, Inc., 2006 WL 1318387 at *5-9 (E.D.N.Y. May 15, 2006) (employee entitled to either or both attorney-client privilege or work product doctrine protections for the same reasons) .

involving employee waiver of attorney-client privilege, the employee has also claimed that the communications at issue were also protected by the work product doctrine.[89]

The work product doctrine has already been successfully used as an alternative position in a high-profile case involving electronic communications wherein attorney-client privilege was found to be waived. Martha Stewart's forwarding of a privileged email to her daughter was found to constitute waiver of attorney-client privilege, yet was still considered protected under the work product doctrine as Stewart did not "substantially increase the risk that the Government would gain access to materials prepared in anticipation of litigation."[90] However, in *Lynch v. Hamrick*,[91] Juanita Lynch's privileged telephone conversations held in the presence of her daughter received no such protection through application of the work product doctrine.[92] The contrast between these cases illustrates how courts are particularly friendly to litigants who have made a technological blunder.[93]

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."[94] This rationale could be extended to workplace waiver[95] situations, especially when an employee attempts to remove traces of the privileged materials from the employer's computer system.[96] However, it seems clear that the work product doctrine has taken a backseat to attorney-client privilege. To date, all courts addressing workplace waiver[97] have simply lumped the two concepts together or given work product claims token consideration.[98]

III. CHAOS IN THE COURTS

Courts have struggled in determining whether an employee waived attorney-client

---

89 *See e.g.*, *Long* 2006 WL 2998671 at *3-5; *Curto* 2006 WL at *2.

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

91 2007 WL 1098574 (Ala. 2007).

92 *Lynch*, 2007 WL 1098574 at *4.

93 *See* discussion *infra* Parts II.A, IV.A, V.C.

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

95 *See supra* note 28

96 *See* discussion *infra* Part III.B.

97 *See supra* note 28

98 *See supra* note 80.

privilege by checking an otherwise privileged email on a company computer, and holdings have varied considerably.[99] The decisions center around whether the employee-client had an objectively reasonable expectation of privacy when communicating with an attorney.[100] Courts have taken fact-specific approaches to determine the objective reasonableness of the employee's belief, and the different variables that courts have given consideration will be discussed in the following subsections.

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

Every court addressing workplace waiver[101] has first looked to the employer's policies[102]

---

[99] *Compare e.g.*, Kaufman v. SunGard Inv. Sys., 2006 WL 1307882 at *1-3 (D.N.J. May 10, 2006) (although employee deleted privileged emails on company laptop which were later recovered by a computer technician, employee had waived privilege) *and* Long v. Marubeni Am. Corp., 2006 WL 2998671 at *1-3 (S.D.N.Y. 2006) (employee waived privilege by checking emails on company computer) *and* Banks v. Mario Indus. of Va., Inc., 650 S.E.2d 687, 695-96 (Va. 2007) (employee waived privilege by preparing an otherwise privileged communication on a company computer) *with* Curto v. Med. World Commc'ns, Inc., 2006 WL 1318387 at *4-5 (E.D.N.Y. May 15, 2006) (employee had not waived privilege by leaving traces of privileged emails on a company computer, although company policy stated all emails viewed on company computer were subject to monitoring) *and* Nat'l Econ. Research Assocs., Inc. v. Evans, 2006 WL 2440008 at *3-5 (Mass. Super. Ct. Aug. 03, 2006) (employee did not waive privilege by checking email on company computer) *and* Sims v. Lakeside School, 2007 WL 2745367 at *2 (W.D. Wash. Sept. 20, 2007) (holding that public policy demanded that employee's privileged communications be protected).

[100] "The attorney-client privilege protects from disclosure those 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 (American Bar Association 2005). *See also e.g.*, 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 circumstances that it was reasonably expected and understood to be confidential.").

[101] *See supra* note 28.

[102] Most employers have some sort of written policy allowing the employer to monitor employee computer use. *See supra*, note 27. In the event that an employer had no such policy language, the lack of a policy would likely be determinative. *See* Transocean Capital, Inc.

regarding employee computer use.[103] Employer policies have been universally considered first, and this is a testament to the importance of policy language. 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 the "necessary and sufficient" approach can be seen in *Banks v. Mario Industries Of Virginia, Inc.*,[104] in which an employee used an employer-owned computer to prepare a memorandum for his attorney regarding his planned resignation.[105] The employee printed the letter and sent it via non-electronic mail, and then singly deleted[106] the electronic copy of the letter.[107] The employer later forensically recovered[108] the memorandum, and sought to use it as evidence against the employee.[109] The court held that since "[The employer]'s employee handbook provided that there was no expectation of privacy regarding [the employer]'s computers[,]"[110] and "[the employee] created the pre-resignation memorandum on a work computer located at Mario's office[,]"[111] *ipso facto* attorney-client privilege did not protect the deleted memorandum from discovery.[112]

---

v. Fortin, 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.").

103 *See supra* note 27 for sample policy language.

104 650 S.E.2d 687 (Va. 2007).

105 *Id*. at 695.

106 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 computers reference mark to the document. Thus, the term "single 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 192-93 (American Bar Association 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 698.

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

108 *See supra* note 22.

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

110 *Id*.

111 *Id*.

112 *Id*.

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.*[113] In *Scott*, a physician wrote several emails to his attorney regarding a suit against his employer for wrongful termination, and he used his employer's email system to do so.[114] While the court eventually found that the employee-physician had waived privilege,[115] it treated the presence of appropriate policy language[116] as an important first step in determining waiver.[117] The court indicated that its decision was based primarily on the policy language by stating that "the effect of an employer e-mail policy, such as that of [the employer], is to have the employer looking over your shoulder each time you send an e-mail. In other words, the otherwise privileged communication[s] would not have been made in confidence because of [the policy]."[118]

The weight given to this variable hinges on the court's interpretation of the strength and sufficiency of the policy language. What a court determines is sufficiently strong language depends largely on the surrounding factual 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.[119] Yet, in another factual situation, an employer may need to specifically describe the method used to monitor employees in order for the language to be seen by a court as sufficient to establish waiver.[120]

B. *Employee Use of a Password-Protected Email Account*

In workplace waiver[121] cases, an employee will often use a personal password-protected email account to email counsel.[122] In *Curto v. Medical World Communications, Inc.*,[123] the

---

113 2007 WL 3053351 (N.Y. Sup. Oct. 17, 2007).

114 *Id*. at *1.

115 *Id*. at *5.

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

117 *Id*. at *5.

118 *Id*. at *3.

119 *See Banks*, 650 S.E.2d at 695.

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

121 *See supra* note 28.

122 *See e.g.*, Nat'l Econ. Research Assocs., Inc. v. Evans, 2006 WL 2440008 at *1 (Mass. Super. Ct. Aug. 03, 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."); Curto v.

Eastern District of New York considered this to be an appropriate factor in considering if attorney-client privilege should protect employee data stored on an employer-owned computer.[124] In *National Economic Research Associates, Inc. v. Evans,*[125] the Superior Court of Massachusetts found this to be a determinative factor.[126] The Sixth District Court of Appeals in California, in *People v. Jiang,*[127] 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."[128]

While these holdings seem to indicate that password protection equates to privacy, this is not necessarily true, as "[an employee] does not have an absolute expectation of privacy in records kept or accessed on his workplace computer, even if password protected."[129] In *Long v. Marubeni America Corp.,*[130] the Southern District of New York considered the use of a personal

---

Med. World Commc'ns, Inc., 2006 WL 1318387 at *3 (E.D.N.Y. May 15, 2006) at *3 ("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."); Long v. Marubeni Am. Corp., 2006 WL 2998671 at *2 (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.") *but see* Kaufman v. SunGard Inv. Sys., 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.").

123 2006 WL 1318387 (E.D.N.Y. May. 15, 2006).

124 *Id*. at *5, 8.

125 2006 WL 2440008 (Mass. Super. Ct. Aug. 3, 2006).

126 "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.* * 4

127 33 Cal.Rptr.3d 227 (Cal. Ct. App. 2005), *withdrawn* 33 Cal.Rptr.3d 184 (Cal. Ct. App. 2005).

128 *Id*. at 202.

129 Campbell v. Woodard Photographic, Inc., 433 F.Supp.2d 857, 861 n.4 (N.D. Ohio 2006).

130 2006 WL 2998671 (S.D.N.Y. Oct. 19, 2006).

password-protected email account to be irrelevant.[131] The court, referring to language in the employer's policy handbook,[132] held that the employee's erroneous subjective belief that using a personal password-protected email account equated to privacy was inconsequential.[133]

Where an employer has provided in their policies that the employee has no expectation of privacy when using an employer-owned computer,[134] giving weight an employee's erroneous subjective belief that use of a personal password-protected email account shields his communications from employer surveillance allows the employee to circumvent the employer's policies.[135] However, password protection may be relevant in analyzing work product claims.[136]

C. *Common Usage of Personal Email on Company Computers*

In *Curto*, the court determined that widespread use of personal email by various employees used personal email accounts at work had bearing on the objective reasonableness of an individual employee's expectation of privacy in using personal email.[137] The court made a specific reference to the fact that "several other MWC employees, including its president, had personal [email] accounts on their work computers."[138]

The fact personal email accounts are widely used in the workplace does not necessarily mean that those employees expected their communications to be private.[139] This inference of

---

131 "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 *8.

132 *Id*.

133 *Id*.

134 As in all the cases cited in this sub-section. *See* Curto v. Med. World Commc'ns, Inc., 2006 WL 1318387 at *3 (E.D.N.Y. May 15, 2006) at *1; Nat'l Econ. Research Assocs., Inc. v. Evans, 2006 WL 2440008 at *3 (Mass. Super. Ct. Aug. 03, 2006) ; Long v. Marubeni Am. Corp., 2006 WL 2998671 at *8 (S.D.N.Y. Oct. 19, 2006); People v. Jiang 33 Cal.Rptr.3d 227 (Cal. Ct. App. 2005), *withdrawn* 33 Cal.Rptr.3d 184, 197-98 (Cal. Ct. App. 2005).

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

136 *See* discussion *supra* Part II.E.

137 *Curto*, 2006 WL 1318387 at *3 n.2.

138 *Id*.

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

privacy from common use may be rational in exceptional circumstances,[140] but it is questionable whether such an inference is objectively reasonable.[141]

D. Employee Attempts to Delete Privileged Material

The *Curto* court reasoned that an employee attempt to singly delete[142] privileged files was a reasonable precaution to prevent inadvertent disclosure.[143] The *Evans* court reached a similar conclusion regarding an employee's attempt to double delete[144] privileged files.[145] In both cases, the files were discovered by the employer.[146]

These attempts to delete information undoubtably created a subjective belief in the mind of the employee that the communication was made inaccessible to the employer.[147] Yet, in light of commonly used technology,[148] that belief was objectively unreasonable. That the employer was able to recover the documents, even when a document was purportedly double deleted,[149]

---

[140] The argument is stronger when control-group executives are in the habit of using personal email at work, as in *Curto*. *See supra* note 138 and accompanying text. It would be further strengthened if the employee was instructed by a supervisory employee to use a personal email account for emails, such as to send them a work-related file.

[141] 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 email at work was shielded from surveillance, an inference of privacy would be illogical..

[142] *See supra* note 106.

[143] *Curto*, 2006 WL 1318387 at *3, 8. Yet, it seems clear that the *Curto* court was referring to single deletion, which is arguably not a "reasonable precaution taken . . . to prevent the disclosure of [a privileged document]", as the *Curto* court stated. *Id*. at *1.

[144] *See supra* note 106.

[145] Nat'l Econ. Research Assocs., Inc. v. Evans, 2006 WL 2440008 at *1 (Mass. Super. Ct. Aug. 03, 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*. at *1.

[146] *See Evans*, 2006 WL 2440008 at *1; *Curto*, 2006 WL 1318387 at *1.

[147] For otherwise, why would the employee bother to delete the file?

[148] Recovery of deleted data from computers through the use of forensic software has been commonplace since the early 1990's. *See* David W. Hendron, *The Continuing Evolution of Computer Forensics*, 34 L. ENFORCEMENT Q. 19, 19-20 (Winter 2005-2006).

[149] "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.

illustrates this.

Further, the employers in both *Curto* and *Evans* made clear that employees had no expectation of privacy while using a work computer.[150] 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.[151] The employee's attempted deletion might be more relevant in a work produce analysis.[152]

E. *Employer Enforcement of any Existing Computer Usage Policy*

In determining if privilege had been waived, the *Curto* court considered the frequency of the employer's enforcement of its computer usage policy.[153] The court acknowledged that no other court had previously found this to be relevant,[154] 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."[155]

The court further stated that prior cases on employee expectations of privacy were not controlling as (1) they did "not address the confidentiality of employee's e-mails and personal computer files with regard to the attorney-client privilege or attorney work product immunity[,]"[156] and (2) that "none of these cases involves an employee working from a home

---

When you ski down a snowy 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." CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME 240 (2d ed. 2004).

150 *See Evans*, 2006 WL 2440008 at *2-3; *Curto*, 2006 WL 1318387 at *1.

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

152 *See* discussion *supra* Part II.E.

153 *Curto*, 2006 WL 1318387 at *4-5.

154 *Id*.

155 *Id*. at *5.

156 *Id*.

office."[157]

The former rationale is a weak basis to differentiate *Curto* from prior case law. The objective reasonableness of an employee's privacy belief has little relation to the person the employee is communicating with, but rather is tied to the medium the employee uses to communicate.[158] However, the latter rationale is much stronger and goes to the essence of *Curto*.[159] *Curto* suggests that consideration of the employer's habitual enforcement would not be appropriate in all situations, and the court's explicit limitation of their holding states this.[160] Moreover, the *Curto* court downplayed the importance of employer enforcement, stating that the factor was "in no way . . . dispositive" and characterized it "as a 'sub-factor' to be examined, along with [other factors]."[161] *Curto*'s token defense justifying consideration of the frequency of the employer's enforcement of its computer usage policy illustrates its relative unimportance.

F. The Location of the Computer

The actual physical location of the computer has logical and legal significance in workplace waiver[162] 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.[163] However, technologically sophisticated surveillance intruding into an individual's home has been frowned upon by the Court in other contexts.[164] Allowing an employee to take a computer into their home, then later using

---

157 *Id*.

158 An employee sending his wife a personal email from work is engaging in the same activity as an employee sending an email to an attorney. The only difference between the two is the content of the email and the recipient; these factors have nothing to do with the objective reasonableness of the employee's belief that the email is private.

159 The essence being that an employee working from a home office should be treated differently than an employee working outside of the home. *See* discussion *infra* Part III.F.

160 *See infra* note 166 and accompanying text.

161 *Id*.

162 *See supra* note 28.

163 The converse is true regarding an employee's personal computer taken to work. *See supra* notes 62-63 and accompanying text..

164 "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

information stored on that computer against the employee, smacks of a Trojan Horse.[165]

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."[166] By so limiting their holding, the *Curto* court indicated that a computer's location can be determinative.[167] Another recent case has cited *Curto* to "highlight the perils" of an employee using an employer issued computer in the home.[168]

A more interesting question would be posed by an employee accessing a workplace email account[169] from home.[170] It is doubtful that this 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 email account and thus it would not present the same image of an employer-set snare..

G. *The Forensic Method Used to View an Employee's Emails*

The *Evans* court took issue with the method used by the employer to monitor its employee's email usage.[171] The employer in *Evans* utilized software that routinely took "screen

---

technologically to cross the "'firm line [of privacy] at the entrance to the house.'" *Id*. at 40 (citation omitted). Although *Kyllo* case involved the Fourth Amendment and criminal law, the language used by the Court and the Court's articulation of its desire to protect the home against what the Court clearly viewed as invasive technological surveillence implies that the Court would have similar protectionist leanings in workplace waiver cases.

[165] The Court has previously frowned upon "a Trojan Horse dressed up in legal form." NLRB. v. City Disposal Systems Inc., 465 U.S. 822, 844 (1984).

[166] *Curto*, 2006 WL 1318387 at *8.

[167] *Id.*

[168] Geer v. Gilman Corp., 2007 WL 1423752 at *4 (D. Conn. Feb. 12, 2007).

[169] *See supra* note 20.

[170] Barbara Hall is one of many employees who access their workplace email account from home. *See* note 4 and accompanying text.

[171] Nat'l Econ. Research Assocs., Inc. v. Evans, 2006 WL 2440008 at *4 (Mass. Super. Ct. Aug. 03, 2006).

shots"[172] of what the employee was viewing on the employer's computer.[173] The court was shocked that this was possible.[174] Yet, the employer stated in it's policy manual that "Network administrators can read your [electronic] mail!"[175] While shocking to the court,[176] the particular forensic method it was unaware of is relatively commonplace.[177]

While stopping short of declaring the method of surveillance *prima facie* 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
>
> 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.[178]

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!"[179] Moreover, forcing an employer to lay out the specific technical procedure used to monitor an employee might aid employees in circumventing the monitoring systems.

---

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

173 *Evans*, 2006 WL 2440008 at *4.

174 "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*.

175 *Id*. at *3.

176 *Id*.

177 *See* note 12 and accompanying text.

178 *Evans*, 2006 WL 2440008 at *5.

179 *Id.* at *3.

However, the *Evans* court's reaction to the employer's method of surveillance seemed ultimately grounded in a concern for fairness.[180] The court's holding stemmed from its obvious feeling that the utilized was overly-invasive and draconian in application.[181] Thus, if a court considers a method of surveillence to be inherently unfair,[182] it may require a company to take extraordinary steps to ensure notice.[183]

H. *Fairness and Public Policy*

The *Curto* court specifically considered the "overarching issue of fairness" as a variable.[184] From the context that the *Curto* court used the word "fairness," it is clear that the court was concerned with the public policy implications of its decision. All courts, whether implicitly or explicitly, have considered issues of fairness and public policy. It may be that all workplace waiver[185] decisions are reverse engineered to match whatever the court feels is the correct result from a fairness standpoint, as the sparsity of existing case law coupled with rich factual situations have resulted in extremely malleable cases. The danger in this reliance on a court's interpretation of what is fair or in the interest of public policy is that what different people[186] considers to be "fair" wildly differs.

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*,[187] in

---

180 *Id*.

181 *Id*.

182 Begging the question, what exactly is an "unfair" method of surveillance? Employers utilize a myriad of method to keep an eye on employees, running the gamut from peeping over the employee's shoulders to keystroke monitoring and email duplication and review. *See* 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.

183 That is, in order to use recovered information against an employee in litigation. 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.

184 Curto, 2006 WL 1318387 at *3, 5.

185 *See supra* note 28.

186 And thus what judges consider to be fair differs as well, since to date all American judges have been flesh-and-blood human beings.

187 2007 WL 2745367 (W.D. Wash. Sept. 20, 2007).

which an employee used his employer's laptop to communicate with his attorney and the employer later forensically recovered the emails.[188] 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[,]"[189] 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."[190] The only legal support cited by the *Sims* court for deciding the case on public policy grounds was a 92 year old case that does not once mention attorney-client privilege,[191] 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 information gained from spying on employees in litigation, their unilateral imposition of this policy viewpoint with no legitimate legal support illustrates the danger of judicial imposition of public policy judgments. As the Court has repeatedly stated, "[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."[192] 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 and objectively consider the factual circumstances and principles of existing law,[193] rather than applying subjective interpretations of fairness. Failing to do so would result in chaos, as it would be impossible to establish any semblance of uniformity in workplace waiver cases.

IV. MAKING SENSE OF IT ALL

---

188 *Id*. at *1.

189 *Id*.

190 *Id*. at *2.

191 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*.

192 Lowe v. SEC, 472 U.S. 181, 213 (1985).

193 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")

A. *The Knowledge Gap*

Much of the difficulty in these cases stems from the employee-employer knowledge gap.[194] Most employees have an erroneous belief that email communications made on a company computer are private,[195] yet that belief is unreasonable from a moderately technologically sophisticated standpoint. Whether an objectively reasonable person is moderately technologically sophisticated is an open question.[196]

This puts the judge in the unenviable position of trying to determine who should bear the consequences of this knowledge gap.[197] The court is thus forced to decide whether a commonly held incorrect belief is an objectively reasonable belief. This position is made all the worse by the fact that few courts are technologically savvy,[198] and some appear to personally identify and sympathize with technologically unsophisticated employees.[199]

Interestingly, when faced with ambiguity, courts that frequently address cases dealing with technological issues have a marked tendency to rule differently in technology cases than

---

[194] "[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.

[195] *See supra* notes 13-14 and accompanying text.

[196] This is certainly debatable, yet very little reliable and current statistical information exists on the subject. *See* Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science, and Behavioral Economics*, 82 NOTRE DAME L. REV. 583, 611-12 (2002) (proposing that a lack of technological sophistication in the general population can be inferred from the inability of people to avoid pop-up ads). Yet, as time marches on, the average level of technological sophistication will inevitably rise. *See* discussion *infra* V.C. Thus, the objectively reasonable person will become technologically sophisticated if he isn't already.

[197] "Hard cases, it is said, make bad law." *Ex Parte Long*, 3 W.R. 19 (Q.B. 1854, Lord Campbell, Ch. J.).

[198] According to Judge Posner, "[e]veryone knows that younger people are on average more comfortable with computers than older people . . . [,]" and it is also common knowledge that most judges fall into the latter age category. Sheehan v. Daily Racing Form, Inc., 104 F.3d 940, 942 (7th Cir. 1997).

[199] *See supra* note 174.

courts that do not.[200] This suggests that the level of technological sophistication of the judge is linked to the court's interpretation of what is an objectively reasonable level of technological sophistication.[201]

B. *Modern vs. Traditional Approaches to Attorney-Client Privilege*

Some courts have adopted a non-traditional approach to attorney-client privilege in workplace waiver[202] cases. These courts have broadly interpreted the privilege in an attempt to deal with situations where they feel the privilege should be upheld. They may do so either for public policy reasons,[203] or where they feel that the tradition approach is antiquated and unable to cope with issues involving technology. Other courts have adhered to Wigmore's traditional approach.[204] While it is possible that courts adopting a broadened approach have done so unwittingly, the unspoken difference of breadth has naturally led to inconsistent holdings and will continue to do so until some uniformity of reasoning is established.

V. WHAT TO DO?

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 stored on an employer-issued computer."[205] Without a bright line approach, courts will continue to consider a legion of factual variables,[206] leading to possible inconsistency. Yet, in the face of differing factual situations, some variability may be desirable. An attempt to eschew obfuscation[207] through the imposition of a forced bright-line test would have an effect similar to the use of the term "eschew obfuscation" itself.[208]

---

200 *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).

201 *Id*.

202 *See supra* note 28.

203 *See* discussion *supra* Parts II.B, III.F.

204 *See* discussion *supra* Part II.A.

205 Kelcey Nichols, *Hiding Evidence From the Boss: Attorney-Client Privilege and Company Computers*, 3 SHIDLER J. L. COM & TECH. 6, 6 (2006).

206 *See supra* Part III.

207 Literally, the meaning is "avoid ambiguity, adopt clarity."

208 That is, to unnecessarily confuse in an attempt to clarify.

B. *Distillation of Logically Pertinent Variables*

It is generally accepted that in workplace waiver[209] cases a court should first look to the language of the employer's policies.[210] If the policies make clear that the employee has no expectation of privacy while using a work computer, then it seems 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,[211] or (2) the actions of the employer[212] rendered this policy language ineffective. Depending on the circumstances, a court might also consider analyzing the issue (1) under the work product doctrine,[213] (2) as a breach of fiduciary duty and thus a fraud exception to attorney-client privilege,[214] and (3) in the event that the computer was used in relation to a crime, as a crime exception to attorney-client privilege.[215]

However, problems may emerge when considering such factual variables as (1) usage of a personal password-protected email account,[216] (2) other employees' use of personal email at work,[217] (3) employee attempts to delete or hide files from the employer,[218] (4) the forensic method used by the employer to recover information,[219] or (5) any other technologically related factual situation 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.[220] Under a modern, broadened, approach to attorney-client privilege, they might be pertinent.[221] Either way, courts may well need specialized outside help in these cases.

---

209 *See supra* note 28.
210 *See* discussion *supra* Part III.A.
211 *See* discussion *supra* Part III.F.
212 *See* discussion *supra* Part III.C.
213 *See* discussion *supra* Part II.E.
214 *See* discussion *supra* Part II.D.
215 *See* discussion *supra* Part III.A.
216 *See* discussion *supra* Part III.B.
217 *See* discussion *supra* Part III.C.
218 *See* discussion *supra* Part III.D.
219 *See* discussion *supra* Part III.A.
220 *See* discussion *supra* Part II.A.
221 *See* discussion *supra* Part III.B.

Court appointed experts,[222] special masters,[223] or even adversarial testimony by the parties' competing experts[224] could go a long way in assisting in the determination of the objective reasonableness of an employee's belief.

VI.. CONCLUSION: ADOPTION OF A MODERN APPROACH OR RE-AFFIRMATION OF TRADITION?

Courts can and should use presumptions and distill existing case law to determine the logically pertinent factual variables in workplace waiver cases, but a clash is 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 deciding factor in whether the broad or narrow approach will win out may be timing.

It seems clear that judges adopting the modern approach truly feel uncomfortable, from a personal standpoint, with the technological-peeping engaged in by employers. A large part of why many of these judges probably feel uncomfortable is their unfamiliarity with technology in general. Correspondingly, it is likely that judges rejecting the modern approach and sticking to traditional interpretations of attorney-client privileges are those who are more familiar and comfortable with technology.

As time progresses, the judiciary as a whole will become more technologically savvy,[225] and thus less likely to have a problem with technologically sophisticated methods of employer surveillence. Thus, the farther in the future these two schools of thought come to loggerheads, the more likely it is the traditional approach will be re-affirmed. Ironically, in workplace waiver cases, the traditional approach may become more popular over time, while the modern approach will slowly fade away. While it is unclear what direction the law will take, it is clear that employees should take care in the workplace, lest they click away their confidentiality.

---

222 *See* FED. R. EVID. 706.

223 *See* FED. R. CIV. P. 53.

224 *See* FED. R. EVID. 702.

225 *See supra* note 198.