St. John's Law Review

Volume 90
Number 2 *Volume 90, Summer 2016, Number 2*

Article 6

November 2016

Confidentiality and Attorney Client Privilege in the Internet Age: How to Handle Employer Monitoring of Employee Email

Anthony Biondo

CONFIDENTIALITY AND ATTORNEY-CLIENT PRIVILEGE IN THE INTERNET AGE: HOW TO HANDLE EMPLOYER MONITORING OF EMPLOYEE EMAIL

ANTHONY BIONDO[†]

INTRODUCTION

Attorney-client privilege, one of the oldest privileges for confidential communications,[1] needs to adapt to the modern world. The privilege plays an important role in the legal system by preventing attorneys from being compelled to divulge confidential communications between themselves and their clients. This assurance of confidentiality encourages clients to be fully open, which is essential to a well-functioning attorney-client relationship.[2] However, clients may find that communication is unprivileged because they communicated with their attorney through a system operated and monitored by their employer. Many employers now provide employees with technology systems—such as computers and email systems—and many employers monitor the communications made through these systems.[3] Since privilege will not attach to a communication that is revealed to a third party,[4] some courts have held that when an employee uses a monitored email system to communicate with

[†] Senior Staff, *St. John's Law Review*; J.D., 2016, St. John's University School of Law; B.S., 2013, Computer Science, Stony Brook University.

[1] 4 JOHN HENRY WIGMORE, A TREATISE ON THE SYSTEM OF EVIDENCE IN TRIALS AT COMMON LAW § 2290, at 3193–94 (1904).

[2] 4 WIGMORE, *supra* note 1, § 2291, at 3196.

[3] In a 2007 survey of employers, it was found that 43% of companies surveyed monitored employee email, and of those, 40% assigned an individual to manually read and review email while 73% used technology tools to automatically monitor email. *2007 Electronic Monitoring & Surveillance Survey*, AMERICAN MANAGEMENT ASSOCIATION AND THE EPOLICY INSTITUTE, http://www.plattgroupllc.com/jun08/2007ElectronicMonitoringSurveillance Survey.pdf [hereinafter *ePolicy Survey*].

[4] 4 WIGMORE, *supra* note 1, § 2285, at 3185.

his attorney, the communication is unprivileged.[5] This Note focuses on email, as it is a common method of electronic communication that is often facilitated by employer-controlled systems.[6]

New technology and new methods of communication have created issues in the application of attorney-client privilege.[7] In particular, the fact that email systems are often facilitated and monitored by a third party,[8] often an employer,[9] creates uncertainty in the application of the confidentiality element of attorney-client privilege.[10] Further compounding the issue are employer policies that prohibit personal use or allow for broad monitoring of employer systems, which are often buried away deep in an employee handbook, and employees may not realize that such a policy exists or fully understand the ramifications of the policy on the confidentiality of their communications.[11] This false sense of security can lead to an inadvertent loss of privilege by a client.[12]

In considering whether an employer has the ability to access an electronic communication, courts are attempting to look beyond the transaction as experienced by the users, and probe

---

[5] *See, e.g.*, Long v. Marubeni Am. Corp., No. 05Civ.639(GEL)(KNF), 2006 WL 2998671, at *3 (S.D.N.Y. Oct. 19, 2006) (holding that employer's policy of prohibiting any personal use of company-issued computers removed any possible expectation of privacy and that communication was unprivileged since employee used a private email account to communicate with attorney on a company-issued computer).

[6] *See ePolicy Survey*, *supra* note 3.

[7] JEROME G. SNIDER & HOWARD A. ELLINS, CORPORATE PRIVILEGES AND CONFIDENTIAL INFORMATION § 2.08 (1999) ("[M]any important issues currently at the center of the privilege discussion concern new technology.").

[8] *See infra* Section III.B.

[9] *See ePolicy Survey*, *supra* note 3.

[10] SNIDER & ELLINS, *supra* note 7, § 2.08 ("Using new technology can raise concerns about whether purportedly privileged communications were actually made in confidence, or whether the use of certain technologies effectuates a waiver of the attorney-client privilege.").

[11] *See ePolicy Survey*, *supra* note 3 ("Unfortunately, the methods employers use to alert employees to e-mail and Internet monitoring are not necessarily the most effective: 70% of organizations in 2007 relied on an employee handbook to inform users about computer monitoring."). Additionally, employees may be mistaken in thinking that the employer's policy does not cover their actions. *See, e.g.*, Long v. Marubeni Am. Corp., No. 05Civ.639(GEL)(KNF), 2006 WL 2998671, at *4 (S.D.N.Y. Oct. 19, 2006) (holding that employees lost privilege by using a company-issued computer to access a password protected private email account).

[12] *See, e.g.*, Aventa Learning, Inc. v. K12, Inc., 830 F. Supp. 2d 1083, 1107 (W.D. Wash. 2011) (holding that an employee lost privilege despite claim that he never received or read the employee handbook).

into the path of the message as it flows through the Internet.[13] However, employers are only one of a number of parties that facilitate electronic communications with the technical ability and limited legal right to intercept and monitor them.[14] Though an employer may have a comparatively broad right to monitor the emails flowing through its systems, they are not the only party with a qualified right to do so.[15] This Note argues that courts should focus on the communication as experienced by the user/client. The policy of encouraging free and open discourse and candor favors protecting the client's reasonable expectations. Since electronic communication on the Internet is often facilitated by numerous third parties, it is unreasonable to expect a client to consider the monitoring ability of each third party when communicating with his attorney electronically.

In confronting the issue of whether an employer-monitored electronic communication is privileged, courts will divide the confidentiality problem into a two-step inquiry: (1) Was there a subjective expectation of privacy on the part of the client/employee, and (2) Was that subjective expectation of privacy objectively reasonable?[16] As to the first question, clients who did not subjectively believe that their communications would be confidential are not entitled to the protection of attorney-client privilege, because there was no need of an assurance of confidentiality to encourage them to make the communication.[17]

---

[13] *See* discussion *infra* Part II (discussing different approaches taken by courts in approaching the issue); Section III.B (discussing the issue of perspectives in the legal analysis of internet activities).

[14] *See* discussion *infra* Section III.A (discussing the rights of Internet Service Providers and Internet Mailbox Providers to access communications facilitated through their systems).

[15] *See* discussion *infra* Section III.A. New York, for example, has a statute preventing an electronic communication from losing its privileged character because a third-party facilitator may have access to it. N.Y. C.P.L.R. § 4548 (McKinney 2016). However, at least one court has held this statute inapplicable to employer monitoring. Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 440 (N.Y. Sup. Ct. 2007) (discussed *infra*).

[16] United States v. Schwimmer, 892 F.2d 237, 244 (2d Cir. 1989) ("[A]ll claims of privilege arising out of the attorney-client relationship . . . require[] a showing that the communication in question was given in confidence and that the client reasonably understood it to be so given.").

[17] 4 WIGMORE, *supra* note 1, § 2311, at 3234 ("One of the circumstances, by which it is commonly apparent that the communication is not confidential, is the *presence of a third person* . . . . [E]ven if we might predicate a desire for confidence by the client, the policy of the privilege would still not protect him, because it goes no further than is necessary to secure the client's subjective freedom of

As to the second question, however, courts diverge and conflict arises.[18] Some courts formalistically conclude that if the employer has the right to monitor the use of its systems, the expectation of privacy is so eroded as to be objectively unreasonable, and refuse to apply privilege.[19] Though the bright-line nature of this rule seemingly provides certainty, the rule may actually inject more uncertainty into the analysis by forcing clients to consider the rights of numerous third parties facilitating an electronic communication.[20] Other courts have adopted one of several factor tests, such as the "oft-quoted"[21] four-factor test from the case *In re Asia Global Crossing, Ltd*.[22] These tests provide a case-by-case analysis in order to prevent communications from inequitably being unprivileged,[23] but the factors are not sufficiently tied to the reality of communication on the Internet or to a user's reasonable perspective of Internet email communication.[24]

This Note argues for the use of an objective element that focuses on the experience from the perspective of the user. The subjective element of the analysis remains unchanged, but a court will be asked to consider whether the client's subjective belief was objectively reasonable from their perspective as a user

---

consultation . . . ."); *see also* United States v. Rigas, 281 F. Supp. 2d 733, 737 (S.D.N.Y. 2003) ("As a general rule, the voluntary production of a privileged document waives any claim of privilege with respect to that document.").

[18] Indeed, when analyzing the particular, many courts take for granted that the employee subjectively believed that his communication would be private. *See, e.g.*, *In re* Asia Glob. Crossing, Ltd., 322 B.R. 247, 258 (Bankr. S.D.N.Y. 2005) ("[T]he Court assumes that the Insider E-mails are otherwise privileged, and further, that the Insiders subjectively intended that they be confidential.").

[19] *See, e.g.*, Long v. Marubeni Am. Corp., No. 05Civ.639(GEL)(KNF), 2006 WL 2998671, at *3 (S.D.N.Y. Oct. 19, 2006) (holding that employees had no reasonable expectation of privacy when employer policy stated that employees "have no right of personal privacy" when using employer systems); *Scott*, 847 N.Y.S.2d at 443 (finding no expectation of privacy where employer acknowledged that it did not monitor employee email but retained the right to do so).

[20] *See infra* Section III.B.

[21] Goldstein v. Colborne Acquisition Co., LLC, 873 F. Supp. 2d 932, 935 (N.D. Ill. 2012).

[22] 322 B.R. at 257.

[23] *See* Upjohn Co. v. United States, 449 U.S. 383, 396 (1981) ("[T]he recognition of a privilege based on a confidential relationship . . . should be determined on a case-by-case basis." (quoting S. REP. NO. 93-1277 (1974), *as reprinted in* 1974 U.S.C.C.A.N. 7051, 7059)).

[24] *See id.* at 393 ("An uncertain privilege, or one which purports to be certain but results in widely varying applications by the courts, is little better than no privilege at all.").

of the Internet. This test avoids the issue of requiring clients to consider the path their electronic communication takes through the Internet by focusing on their perspective as a user of the Internet. Given the seemingly private nature of email, this analysis starts with a strong presumption that an email message is privileged. Next, for each party that has a right to access the email message as it flows through the Internet, the court considers the relationship as between the client and the party with access from the client's perspective as an Internet user. The court asks what the nature of this relationship is, how foreseeable it is that the communication may be of interest to this party, and whether the party regularly exercises its right to monitor the email such that the client should expect that the message would be monitored. This approach has the effect of limiting the analysis to the perspective of the user, who is entirely unaware of some parties—like operators of routers on the Internet—and well aware of others—like an employer or email provider—for transparent parties, monitoring is entirely unforeseeable and thus privilege is not affected.

This Note proceeds in four parts. Part I provides an overview of the attorney-client privilege with a focus on the history and policy behind the confidentiality requirement. Part II explores the differing approaches, and their respective applications, currently used by courts to determine when privilege attaches to an attorney-client communication transmitted through or using an employer's systems. Part III provides a background of the relevant technology and discuss the different viewpoints courts can take when analyzing an electronic communication. Part IV proposes a new objective analysis of the reasonableness of a client's subjective belief of privacy that focuses on the communication from the perspective of the user, rather than the perspective of an outsider viewing the Internet as a series of physical connections.

I. ATTORNEY-CLIENT PRIVILEGE

Professor John Henry Wigmore explained the concept of attorney-client privilege in his well-known treatise *Evidence in Trials at Common Law*:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relevant to that purpose, (4) made in

> confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the client waives the protection.[25]

This Part examines the privilege by dividing these elements into three components. The first component defines the subject matter covered by the privilege, legal advice sought from a professional legal advisor. The second component defines the type of material covered, communications between a client and an attorney for the purpose of seeking legal advice. The third component covers how an act, inconsistent with the intent for a communication to be or remain confidential, affects privilege.

A. Component One: Legal Advice Is Sought from a Professional Legal Advisor in His or Her Capacity as Such

The first component is that legal advice is sought from a professional legal advisor in his or her capacity as such. This component defines the scope of the subject matter to which privilege may be applied.[26] It is the intent of the client that controls.[27] The client must intend to obtain legal advice or assistance in order for privilege to attach.[28] The privilege, however, is quite broad; notably, there is no limitation that either litigation or a specific dispute be contemplated or underway at the time of the consultation.[29]

---

[25] 4 WIGMORE, *supra* note 1, § 2292, at 3204. This formulation has received substantial deference in the courts. *See, e.g.*, United States v. Tedder, 801 F.2d 1437, 1441 (4th Cir. 1986) (considering the Wigmore formulation); *see also, e.g.*, RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 68 (AM. LAW INST. 2000) (providing only four elements); Paul R. Rice, *Attorney-Client Privilege: The Eroding Concept of Confidentiality Should Be Abolished*, 47 DUKE L.J. 853, 853–55 n.1 (1998) (collecting statutes).

[26] 4 WIGMORE, *supra* note 1, §§ 2294–2304, at 3206–23.

[27] 1 PAUL R. RICE ET AL., ATTORNEY-CLIENT PRIVILEGE IN THE U.S. § 7:1 (2015) [hereinafter PRIVILEGE].

[28] *Id.*; *see, e.g.*, United States v. Dennis, 843 F.2d 652, 657 (2d Cir. 1988) ("The key . . . is the intent of the client and whether he reasonably understood the conference to be confidential."); United States v. Huberts, 637 F.2d 630, 640 (9th Cir. 1980) (holding that attorney hired by a counterfeiter to purchase printing equipment for him "was acting as a business agent rather than a legal adviser" such that privilege could not attach).

[29] PRIVILEGE, *supra* note 27, § 7:1; *see, e.g.*, *In re* Bieter Co., 16 F.3d 929, 938 n.8 (8th Cir. 1994) (holding that the "prepared in anticipation of litigation" standard applicable to attorney work product protection was not necessary in order for attorney-client privilege to attach).

This demonstrates the primary modern justification for the attorney-client privilege, which is to free the client from apprehension and encourage full and frank disclosure when the client seeks legal advice from his attorney.[30] It stems from a recognition that in order for lawyers to give sound legal advice and provide strong advocacy, the lawyer must be fully informed by the client.[31] However, any privilege enforced by the court is an exception to the general rule that every person can be called upon to give testimony upon all facts.[32] This component helps to balance the competing policy interest in the efficient administration of justice against the policy of promoting client candor.[33] It helps to narrowly tailor the privilege to only protect those disclosures that are "necessary to obtain informed legal advice which might not have been made absent the privilege."[34]

B. Component Two: A Communication Has Been Made by the Client Relating to the Purpose of Seeking Legal Advice

The second component is that the privilege covers a communication made by the client relating to the purpose of seeking legal advice. This component defines what type of material is covered. It is only a communication between the attorney and the client that is protected by the privilege.[35] The facts communicated are not covered by the privilege, only the contents of the communication itself.[36] Facts and information do

---

[30] *See* 4 WIGMORE, *supra* note 1, § 2291, at 3196–97; Upjohn Co. v. United States., 449 U.S. 383, 389 (1981) ("Its purpose 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.").

[31] *Upjohn Co.*, 449 U.S. at 389 ("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.").

[32] *See* 4 WIGMORE, *supra* note 1, § 2285, at 3185 ("[T]he principle of Privilege, as an exception to the general liability of every person to give testimony to all facts inquired of in a court of justice . . . .").

[33] *Id.* § 2295, at 3211 (discussing the policy of the requirement).

[34] Fisher v. United States, 425 U.S. 391, 403 (1976).

[35] *See Upjohn Co.*, 449 U.S. at 395 ("The privilege only protects disclosure of communications; it does not protect disclosure of the underlying facts by those who communicated with the attorney."); PRIVILEGE, *supra* note 27, at § 5:1 ("An important but commonly misunderstood limitation of the privilege is that it does *not* protect the *information* contained within communications to the attorney.").

[36] *See, e.g.*, *In re* Six Grand Jury Witnesses, 979 F.2d 939, 943–44 (2d Cir. 1992) (stating that the court was still able to compel employees to reveal their analyses of certain costs as these were the underlying facts in the case, it did not matter that

not become privileged simply because they have been communicated by a client to his or her attorney.[37] For example, if a client has communicated with his attorney facts about a particular event, he cannot be compelled to answer questions of the form "what did you tell your attorney about the event," but could still be compelled to answer factual questions about the event itself.[38] Like the first component, this component also helps to narrowly tailor the privilege. It protects the rights of the adversary and the fact finder by allowing them to learn the facts of the case, while promoting client candor by preventing disclosure of communications made while seeking legal advice.[39]

C. Component Three: The Communication Was Made in Confidence and the Confidence of the Communication Has Been Maintained

The third component is that the communication has been made in confidence and that the confidence be maintained. This component defines the effect of an action inconsistent with the intent of a communication to be privileged. In order for privilege to attach, the client must have reasonably intended for the communication to be made in confidence.[40] This is a two-part analysis. First, the client must subjectively intend that the communication with his attorney be confidential.[41] Second, this subjective intent must be objectively reasonable under the

---

they had performed an analysis of costs at the request of counsel and communicated this analysis to counsel).

[37] *See id.* at 944 ("[M]erely by asking witnesses to conduct an analysis defense counsel may not thereby silence all the key witnesses on the cost aspects of the [subject] contracts under [a] claim of privilege.").

[38] *See* PRIVILEGE, *supra* note 27, at § 5:1.

[39] *See, e.g.*, *Fisher*, 425 U.S. at 403 ("However, since the privilege has the effect of withholding relevant information from the fact-finder, it applies only where necessary to achieve its purpose.").

[40] *See, e.g.*, United States v. Schwimmer, 892 F.2d 237, 244 (2d Cir. 1989) ("[A]ll claims of privilege arising out of the attorney-client relationship . . . require[] a showing that the communication in question was given in confidence and that the client reasonably understood it to be so given.").

[41] PRIVILEGE, *supra* note 27, at § 6:1 ("The client must *intend* his communications with his attorney to be confidential.").

circumstances.[42] Finally, this confidence must then be maintained in order for the communication to remain privileged; otherwise, privilege is waived.[43]

The argument for the confidentiality requirement is based in policy. In seeking to protect only those disclosures that are "necessary to obtain informed legal advice which might not have been made absent the privilege,"[44] if the client is willing to make a disclosure in the presence of a third party, then the client does not need the encouragement of privilege protection in order to make the disclosure.[45] Professor John Henry Wigmore views confidentiality as an essential component of the relationship between the two parties—it makes the communication worth protecting because a legal assurance of nondisclosure cannot aid a relationship where confidentiality is neither present nor expected.[46] If confidentiality is not essential to the relationship, he argues, then any assurances of confidentiality through the application of privilege do not sufficiently aid the relationship—and, conversely, the lack of a privilege does not harm it—and the costs of providing such protection outweigh the benefits.[47]

This logic is not without criticism.[48] Professor Paul R. Rice argues that this argument "equates secrecy with safety."[49] Rice defines "safety" as the risk that a communication will be used against the client, whereas secrecy is the risk that it will simply be disclosed to a third party.[50] Rice argues that the exclusionary effect of the privilege is what is fundamental to the candor and to the preservation of the relationship, and not any assurance of

---

[42] *Id.* ("The client's subjective intention of confidentiality must be *reasonable* under the circumstances.").

[43] *Id.* ("[T]he confidentiality must have been subsequently *maintained.*").

[44] *Fisher*, 425 U.S. at 403.

[45] *See, e.g.*, 4 WIGMORE, *supra* note 1, § 2311, at 3233 (citation omitted) ("The reason for prohibiting disclosure ceases when the client does not appear to have been desirous of secrecy.").

[46] *Id.* § 2285, at 3185 ("This element of *confidentiality must be essential* to the full and satisfactory maintenance of the relation between the parties.").

[47] *Id.* ("The *injury* that would inure to the relation by the disclosure of the communications must be *greater than the benefit* thereby gained for the correct disposal of litigation.").

[48] *See* Rice, *supra* note 25, at 859 (arguing that the confidentiality requirement should be abolished in its entirety).

[49] *Id.* at 859–60 ("[I]t assumes that a client who is not concerned with public embarrassment is also unconcerned about being legally compromised by the use of these communications.").

[50] *Id.*

absolute secrecy of the communications.[51] Secrecy is within the control of the client, since the attorney has a professional responsibility to maintain secrecy and it is within the client's power to insist upon secrecy.[52] Rice argues that requiring secrecy, which the client can already insist upon if it is indeed essential to the relationship, does not further the relationship, and that the costs of maintaining the confidentiality requirement outweigh the speculative benefits of narrowly tailoring the privilege.[53]

Since rigid adherence to the requirement of confidentiality may result in inequities, for example, when the parties are unaware of a third party monitoring their communication, some courts have begun to look at the issue through waiver doctrine.[54] This analysis is focused on the voluntary acts of the client that are inconsistent with the existence of a privilege.[55] It views the waiver—or failure of privilege to attach—as the product of a "voluntary relinquishment of the attorney-client privilege."[56] This view of the confidentiality requirement has the effect of introducing exceptions to the rule, such as the inadvertent disclosure exception.[57] The inadvertent disclosure exception, formally recognized in the Federal Rules of Evidence,[58] protects clients from inadvertent waiver when they have involuntarily or

---

[51] *Id.* at 860.

[52] *Id.* ("While secrecy often may be desired by the client, it is ensured, in part, through the attorney by the Code of Professional Responsibility, and otherwise within the factual control of the client."); MODEL RULES OF PROF'L CONDUCT r. 1.6(a) (AM. BAR ASS'N 2014) ("A lawyer shall not reveal information relating to the representation of a client . . . .").

[53] Rice, *supra* note 25, at 860–61.

[54] *Id.* at 881 ("Some courts began applying the standard for waiver . . . ."); United States v. Mejia, 655 F.3d 126, 134 (2d Cir. 2011) ("[T]he person invoking the privilege must have taken steps to ensure that it was not waived . . . .").

[55] SNIDER & ELLINS, *supra* note 7, at § 2.06 ("Courts have categorized the various acts and events that will create a waiver as voluntary or express and as unintentional or implied. . . . [Thus, courts] consider waiver in terms of the act that led to the disclosure.").

[56] Rice, *supra* note 25, at 881 n.76 (quoting State v. Beaupre, 459 A.2d 233, 236 (N.H. 1983)); *see, e.g.*, Eisenberg v. Gagnon, 766 F.2d 770, 788 (3d Cir. 1985) (requiring waiver of attorney-client privilege to be knowing).

[57] Rice, *supra* note 25, at 881 ("As courts moved away from requiring confidentiality as an absolute prerequisite for the existence of the privilege . . . a number of new waiver concepts emerged.").

[58] FED. R. EVID. 502(b)(1).

mistakenly revealed the communication.[59] With new electronic communications that are often facilitated and transparently monitored by third parties, inadvertent disclosure of a communication is more likely than ever. Given complex nature of the Internet as a system of ferrying messages via multiple third-party computer systems, true confidentiality is rarely, if ever, assured.[60] If uncertainty in the true confidentiality of an email is allowed to translate into uncertainty in the application of a privilege, the privilege will be ineffective in encouraging the candor required to protect the attorney-client relationship. Principles of waiver, a concern for safety over absolute privacy, and taking the perspective of a user rather than of an external viewer will help inject a much-needed element of certainty into the privilege as applied in complicated environments such as the Internet.

II. CURRENT APPROACHES TAKEN BY COURTS

Currently, courts take two different approaches when confronted with an issue involving an employee communicating with his attorney through an employer system.[61] Once the other elements of attorney-client privilege have been met, and it has been shown that there was a subjective belief on the part of the client that the communication was private, the narrow question becomes the objective reasonableness of the client's subjective belief.[62] This is where the two approaches diverge. Section II.A addresses the use of factor tests, particularly the oft-quoted four-factor test from *In re Asia Global Crossing, Ltd*.[63] Section II.B

---

[59] Rule 502(b) provides for protection from waiver when: "(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 . . . ." FED. R. EVID. 502(b). However, courts have treated "mistakenly, albeit voluntarily, made" disclosures inconsistently. PRIVILEGE, *supra* note 27, at § 9:72.

[60] *See infra* Sections III.A, III.B.

[61] *Compare In re* Asia Glob. Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005) (providing a four-factor test), *with* Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 440 (N.Y. Sup. Ct. 2007) (focusing on confidentiality).

[62] *See, e.g.*, *In Re Asia Glob. Crossing, Ltd.*, 322 B.R. at 255 (emphasis omitted) ("Confidentiality has both a subjective and objective component; the communication must be given in confidence, and the client must reasonably understand it to be so given." (citing United States v. Schwimmer, 892 F.2d 237, 244 (2d Cir. 1989))).

[63] 322 B.R. at 257.

addresses the use of a more formalistic approach in which courts still consider various factors but place a strong emphasis on actual confidentiality.

A. Four-Factor Test

Courts considering the issue commonly cite the four-factor test from *In re Asia Global Crossing, Ltd*.[64] In that case, the United States Bankruptcy Court for the Southern District of New York addressed the issue when a debtor vacated its offices and left allegedly privileged emails behind on the debtor's servers.[65] The Trustee began an investigation involving the officers of the debtor who had sent the emails, and served a subpoena *duces tecum* on the officers seeking the production of the emails.[66] The debtor asserted privilege, which the debtors opposed because the messages were not communicated confidentially due to the use of a corporate email system.[67] Based on right-to-privacy in the workplace cases under the Fourth Amendment, the court identified four factors that should be considered in determining whether a belief in privacy was objectively reasonable:

> (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?[68]

The court then noted that the employer "clearly had access to its own servers" where the emails were stored, that it had a policy of banning personal use of the email system, and that it notified employees of this policy.[69] However, the court was equivocal as to whether or not the employer had a policy of actually monitoring email and refused to conclude that privilege had been waived as a matter of law.[70]

---

[64] *Id.*
[65] *Id.* at 252.
[66] *Id.* at 252–53.
[67] *Id.*
[68] *Id.* at 257 (footnote omitted).
[69] *Id.* at 259.
[70] *Id.* at 260–61.

Many courts have since looked to these factors for "advisory"[71] guidance on how to determine the objective reasonableness of a client's expectation of confidentiality.[72] In *United States v. Hatfield*, the United States District Court for the Eastern District of New York considered the factors when a criminal defendant asserted privilege for several documents that were otherwise privileged but had been stored on the hard drive of an employer-provided computer.[73]

As to the first factor—the existence of a computer use policy—the court noted that the employer's policy did not explicitly prohibit personal usage, though it did explicitly prohibit some behavior, such as sexual harassment, installing pirated software, and sending junk mail.[74] The court thus reasoned that this silence favored privilege.[75] As to the second factor—a monitoring policy—the court noted that the employer's policy allowed for the right to monitor, but that it did not explicitly say that the company would monitor employee system use; this, too, tipped in favor of applying privilege.[76] As to the third factor—a right of access—the court once again noted that the employer had reserved a right of access and that this factor tipped in favor of nonprivilege.[77] As to the fourth factor—proper notice of the monitoring policy—the court noted that the defendant had notice of the policy and that this factor tipped in favor of privilege.[78]

As a tiebreaker,[79] the court added a fifth factor: how the employer interpreted its own computer usage policy.[80] The court pointed to evidence that "unambiguously shows that [the employer] believed that employees did not forfeit applicable

---

[71] *See, e.g.*, United States v. Finazzo, No. 10-CR-457 (RRM)(RML), 2013 WL 619572, at *7 (E.D.N.Y. Feb. 19, 2013) ("[T]he test is only advisory."); United States v. Hatfield, No. 06-CR-0550 (JS), 2009 WL 3806300, at *8 n.13 (E.D.N.Y. Nov. 13, 2009) ("[T]he [c]ourt construes [the test] as being strictly advisory.").

[72] *See, e.g.*, *Finazzo*, 2013 WL 619572, at *7; Hanson v. First Nat'l Bank, Civil Action No. 5:10-0906, 2011 WL 5201430, at *5–6 (S.D. W. Va. Oct. 31, 2011); *Hatfield*, 2009 WL 3806300, at *8 n.13; Scott v. Beth Israel Med. Ctr. Inc., 847 N.Y.S.2d 436, 441–42 (N.Y. Sup. Ct. 2007).

[73] *Hatfield*, 2009 WL 3806300, at *1.

[74] *Id.* at *9.

[75] *Id.*

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.* at *10 (noting that this fifth factor was "ultimately [the] deciding factor").

[80] *Id.*

privileges by maintaining personal legal documents on their company computers."[81] Indeed, the employer's own counsel testified that he believed individual privilege was protected under the policy.[82] Accordingly, the court reasoned that the government, in arguing in favor of nonprivilege, was trying to impose an interpretation of the usage policy that was never imagined by the employer itself.[83] The court finally held that the communication was privileged.[84]

Courts do not, in every case where they apply the four-factor test, hold that privilege may be applied. In *In re Royce Homes, LP*,[85] the United States Bankruptcy Court for the Southern District of Texas reached the opposite conclusion after applying the four-factor test.[86] There, an employee used a computer owned by the debtor to draft and send email messages, and the Trustee appointed to administer the debtor's estate sought production of the messages to determine if the debtor made any transfers.[87] Adopting the four-factor test,[88] the court compelled disclosure of the messages.[89] The court noted that the employer had a policy allowing for access and monitoring of employer systems and prohibiting certain uses of employer systems, and that all information on the systems belonged to the company and would not be considered private.[90] Finally, the court concluded that the employee knew or should have known of this policy, and that he offered no evidence to rebut the assumption that he did, ultimately compelling disclosure of the documents.[91]

This test, however, appears to place an undue emphasis on the draftsman's art, as courts applying the test tend to focus on the wording of the employer's policy reserving the right to inspect employee communications. All four of the *Asia Global* factors focus on the employer's policies,[92] while only the fifth "tiebreaker element" from *Hatfield* introduces an element far more likely to

---

[81] *Id.*
[82] *Id.*
[83] *Id.*
[84] *Id.*
[85] 449 B.R. 709 (Bankr. S.D. Tex. 2011).
[86] *Id.* at 737–38.
[87] *Id.* at 732–33.
[88] *Id.* at 737–38.
[89] *Id.* at 732.
[90] *Id.* at 738.
[91] *Id.* at 732.
[92] *See In re* Asia Glob. Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005).

be on an employee's mind when considering the confidentiality of a communication: how the policy is actually enforced by the employer.[93] In focusing on a policy that may or may not be enforced, this test leads to inconsistent applications of the privilege, harming the attorney-client relationship.

B. Formalistic Approach: Focusing on Confidentiality-in-Fact

Some courts take a more formalistic approach to the issue. These courts place an emphasis on confidentiality-in-fact, reasoning that if the communication was available at the time of communication to a third party—the employer—privilege cannot attach.[94] In *Hatfield*, the court noted that most courts, after applying the four-factor test, have held that employees may still assert privilege on a communication made using an employer system.[95] Some cases, such as *Long v. Marubeni America Corp.*[96] and *Scott v. Beth Israel Medical Center Inc.*,[97] purport to be applying the four-factor test, but in reality seem to be taking a more formalistic approach to the issue.[98] These cases actually place a substantial emphasis on actual confidentiality, or the lack thereof, and thus may properly be categorized as applying a formalistic test. These two cases will be considered in this subpart.

In *Long v. Marubeni America Corp.*,[99] the plaintiff asserted privilege for several email messages sent through private password protected third party mailbox accounts using computers provided by his employer, the defendant.[100] The employer had obtained these messages through monitoring

---

[93] *See* United States v. Hatfield, No 06-CR-0550 (JS), 2009 WL 3806300, at *10 (E.D.N.Y. Nov. 13, 2009).

[94] *See, e.g.*, Scott v. Beth Israel Med. Ctr., Inc., 847 N.Y.S.2d 436, 440 (N.Y. Sup. Ct. 2007).

[95] *Hatfield*, 2009 WL 3806300, at *8 ("[M]ost-but not all-courts have held that employees do not waive privilege simply by maintaining documents on a company computer system.").

[96] No. 05Civ.639(GEL)(KNF), 2006 WL 2998671 (S.D.N.Y. 2006).

[97] 847 N.Y.S.2d 436.

[98] *Compare Hatfield*, 2009 WL 3806300, at *8 (noting that these both apply a factor test), *with* Alex DeLisi, Note, *Employer Monitoring of Employee Email: Attorney-Client Privilege Should Attach to Communications That the Client Believed Were Confidential*, 81 FORDHAM L. REV. 3521, 3551 (2013) (categorizing both *Long* and *Scott* as applying a formalistic test).

[99] 2006 WL 2998671.

[100] *Id.* at *2.

software installed on the computer.[101] The court did not reference the four-factor test explicitly, but did consider all four factors, noting that use of the system for personal matters was prohibited, that the employer's policy said that employees have no right of privacy on employer systems, that the employer had the right to monitor the systems, and that the plaintiff knew or should have known of the policy.[102] The court, however, focused on the principle of waiver: that the plaintiff knew of the policy and continued anyway, and that the confidentiality of the documents was in fact compromised as a result, and held that the emails were not privileged.[103]

In *Scott v. Beth Israel Medical Center Inc.*,[104] a New York trial court held that privilege did not attach when an employee communicated with his attorney through his employer's email system.[105] First, the court rejected the proposition that waiver was prevented by New York C.P.L.R. 4548, which preserves privilege when parties necessary for the facilitation of an electronic communication have access to the communication.[106] The court then turned to the four-factor test, and considered the effect of the employee handbook on privilege.[107] Rather than holding that the expectation of privacy was unreasonable, the court simply held that "the effect of [the policy] is to have the employer looking over your shoulder each time you send an email," concluding that the communication was not made in confidence and that the communications was not privileged.[108]

In focusing on actual confidentiality, these courts, while they purport to be applying a factor test, are actually taking a far more formalistic approach to this issue. The courts in these cases are formalistically concluding that a lack of confidentiality precludes the application of privilege. While this does inject an element of certainty into the equation, it is easy to see how this

---

[101] *Id.* at *1.

[102] *Id.* at *3.

[103] *Id.* ("The plaintiffs disregarded the admonishment voluntarily and, as a consequence, have stripped from the e-mail messages referenced above the confidential cloak with which they claim those communications were covered.").

[104] 847 N.Y.S.2d 436 (N.Y. Sup. Ct. 2007).

[105] *Id.* at 447.

[106] *Id.* at 440.

[107] *Id.* at 441.

[108] *Id.* at 440.

would result in some communications being unexpectedly unprivileged, as it weighs heavily in favor of the communication not being privileged.

III. CONFIDENTIALITY, TECHNOLOGY, AND PERSPECTIVES

Section III.A provides a background of the legal protections provided to protect email from interception and monitoring through the Electronic Communications Privacy Act ("ECPA").[109] Section III.B provides an overview of the different viewpoints one could take when analyzing an electronic communication, along with a background of the relevant technology.

A. Legal Protections of Electronic Communications

The legal protections afforded to email are similar to those afforded to other forms of communication. Both email providers and Internet Service Providers ("ISPs") are restricted in what they can monitor by the ECPA.[110] The ECPA consists of two parts: The Wiretap Act,[111] which governs the interception of electronic communications, and the Stored Communications Act,[112] which governs unauthorized access to stored electronic information.[113] The actual scope of the ECPA in protecting email is the subject of much debate beyond the scope of this Note.[114] This subsection considers briefly the implications of the ECPA and its exceptions on the following three parties: ISPs, Internet mailbox providers, and employers providing mailboxes and equipment.

---

[109] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848.

[110] *Id.*

[111] 18 U.S.C. §§ 2510–2522 (2012).

[112] *Id.* §§ 2701–2712.

[113] *See* Ariana R. Levinson, *Toward a Cohesive Interpretation of the Electronic Communications Privacy Act for the Electronic Monitoring of Employees*, 114 W. VA. L. REV. 461, 485 (2012).

[114] *See id.* (discussing the debate about the scope of the ECPA and how it impacts employer monitoring of employee communications); Miguel Helft & Claire Cain Miller, *1986 Privacy Law Is Outrun by the Web*, N.Y. TIMES (Jan. 10, 2011), http://nyti.ms/1HH6nw6; Rainey Reitman, *Deep Dive: Updating the Electronic Communications Privacy Act*, ELECTRONIC FRONTIER FOUNDATION (Dec. 6, 2012), https://www.eff.org/deeplinks/2012/12/deep-dive-updating-electronic-communications-privacy-act (arguing for a modification of the law to account for modern technology).

The United States Court of Appeals for the Tenth Circuit recently addressed the rights of ISPs in *Kirch v. Embarq Management Co.*[115] In that case, customers filed an action alleging interception under the ECPA when the defendant, their ISP, authorized an online advertising company to conduct a test for directing and targeting advertisements to users that involved directing traffic through the advertising company's servers.[116] Since the definition of "interception" in the ECPA does not include the contents of communication "acquired in the ordinary course of business," the court held that the ISP had not actually intercepted any communications and therefore did not violate the ECPA.[117] Advertising, the court reasoned, was a legitimate business purpose for collecting and analyzing the information.[118]

Next, we consider the rights of Internet mailbox providers. Google's privacy policy has been the subject of recent litigation, including two conflicting decisions. In *In re Google, Inc. Privacy Policy Litigation*,[119] Magistrate Judge Grewal for the United States District Court for the Northern District of California[120] held that the definition of "interception" in the Wiretap Act similarly did not include Google acting as a service provider when it obtained and used the information "in the ordinary course of its business."[121] The court broadly interpreted the phrase "ordinary course of business" to include Google's "core targeted advertising" business.[122] As to the Stored Communications Act, the court said that the claim "borders on frivolous," and explained that the Act exempts conduct authorized "by the person or entity providing a wire or electronic communications service," which Google clearly authorized its own conduct.[123] Additionally, in *In re Google Inc. Gmail*

---

[115] 702 F.3d 1245 (10th Cir. 2012).

[116] *Id.* at 1245–46.

[117] *Id.* at 1251 ("Earthlink acquired the contents of electronic communications but did so in the ordinary course of business." (quoting Hall v. Earthlink Network, Inc., 396 F.3d 500, 504 (2d Cir. 2005))).

[118] *Id.*

[119] No. C-12-01382-PSG, 2013 WL 6248499 (N.D. Cal. Dec. 3, 2013).

[120] This is Google's home district. *See Google Locations*, GOOGLE, http://www.google.com/about/company/facts/locations (last visited Aug. 26, 2016) (listing Mountain View, CA as company headquarters).

[121] 2013 WL 6248499, at *10 (quoting 18 U.S.C § 2510(5)(a) (2012)).

[122] *Id.* at *10–11 (citing *Kirch*, 702 F.3d at 1250).

[123] *Id.* at *12 (quoting 18 U.S.C § 2701(c)(1) (2012)).

Litigation,[124] the court narrowly interpreted the same phrase in the Wiretap Act—the "ordinary course of business"—to only include interception that was an "instrumental component of Google's operation of a functioning email system."[125] The court did not address the Stored Communications Act.[126]

Finally, we consider the rights of employers in monitoring employer-operated systems. In ECPA cases involving employers monitoring employee email, courts have applied the same exceptions as to other providers and have tended to permit broad monitoring. In *Freedom Calls Foundation v. Bukstel*,[127] the plaintiff employer monitored and used the email account of the ex-employee defendant—[defendant]@freedomcalls.org—who had left the company, founded an identically named organization and created himself a similar email address—[defendant]@freedomcalls.us.[128] In the ensuing trademark dispute, the defendant counterclaimed based on the ECPA that his former employer had no right to access the emails still stored in his old mailbox or to continue monitoring it for new emails mistakenly sent to the incorrect address.[129] The United States District Court for the Eastern District of New York held that the provider exceptions in both the Wiretap Act and the Stored Communications Act applied to protect the plaintiff from these claims.[130] Since the plaintiff provided the defendant with the communication service, the court reasoned, they had the right to search those stored emails as the need arose.[131] As to the Wiretap Act, the court reasoned that the plaintiff was not intercepting the emails as it received them in the normal course of business and was using them to handle client matters in a timely fashion.[132]

---

[124] No. 13-MD-02430-LHK, 2013 WL 5423918 (N.D. Cal. Sept. 26, 2013).

[125] *Id.* at *8.

[126] *Id.*

[127] No. 05CV5460(SJ)(VVP), 2006 WL 845509 (E.D.N.Y. Mar. 3, 2006).

[128] *Id.* at *2.

[129] *Id.* at *27.

[130] *Id.*

[131] *Id.* (citing Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 114 (3d Cir. 2003)).

[132] *Id.*

Similarly, in *Fraser v. Nationwide Mutual Insurance Co.*,[133] the plaintiff sued his ex-employer for damages under the ECPA after the defendant employer searched his mailbox on its central server for emails indicating his disloyalty, found such emails, and terminated Plaintiff's employment.[134] As to the Wiretap Act, the United States Court of Appeals for the Third Circuit held that the employer did not "intercept" his communications because it obtained the emails at an earlier time and accessed them once they were already stored.[135] An intercept, the court reasoned, had to be contemporaneous with transmission.[136] As to the Stored Communications Act, just like in *Freedom Calls Foundation*, the court reasoned that the act of accessing email authorized by the service provider was excepted from the act, and that the employer as a service provider could do as it wished.[137]

Clearly, the ECPA provides protection that is uncertain at best to employees, email users, and Internet users generally. It can be said that these service providers all have a sort of qualified permission to monitor Internet traffic and emails for business purposes. An employer-employee relationship is a special case, but an employer's rights to inspect email are still limited in much the same way as that of any other service provider.

B. Perspectives and Technical Background

When analyzing a legal problem on the Internet, the outcome often depends on whether the problem is analyzed from the "internal" perspective of a user on the Internet or from the "external" perspective of the Internet as a set of physical links between various systems spread throughout the globe.[138] To the internal observer, an email is "the equivalent of old-fashioned postal mail," a user simply drops the message in the mailbox of

---

[133] 352 F.3d 107.

[134] *Id.* at 110–11.

[135] *Id.* at 113–14.

[136] *Id.* (citing United States v. Steiger, 318 F.3d 1039, 1048–49 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002); Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 458 (5th Cir. 1994)).

[137] *Id.* at 114–15.

[138] *See* Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 357 (2003) ("The Internet's facts depend on whether we look to physical reality or virtual reality for guidance.").

the recipient.[139] To the external observer, this is a far more complicated process involving the transmission of a message between several third parties to get it to its destination.[140] One can look at the situation in more and more abstract ways, ranging from "0s and 1s" to the simple postal mail analogy.[141] Depending on how abstract a viewpoint one adopts, the question of whether a communication is confidential may be answered differently.

For example, a phone conversation, as an objective matter, cannot be guaranteed to be private because it is routed through wires operated by the phone company—a third party.[142] Courts are willing to extend privilege to phone conversations, however, because of the legal protections afforded to them.[143] This is taking a more internal perspective—the view of a party on the phone as having a private conversation with another, albeit facilitated by a third party. The legal protections afforded to modern Internet communications are not as strong.[144] In deciding problems of privilege based on what parties have access to a communication, courts are choosing a perspective whether or not they actually recognize that they are doing so.[145] If a court holds that employer monitoring of a system destroys any possibility of privilege, it is implicitly taking an external perspective to the issue. A problem arises when a court takes an external perspective as to some aspects, such as employer monitoring, but ignores other aspects, such as the facilitation of the communications through other third parties such as ISPs.

---

[139] *Id.* at 365.

[140] *Id.* at 365–66.

[141] *Id.* at 361–62 ("This does not necessarily mean that the Internet must be viewed only as 0s and 1s . . . . [W]e look for analogies between realspace and the behind-the-scenes action that computers connected to the Internet process and complete.").

[142] *See* David Hricik, *Confidentiality & Privilege in High-Tech Communications*, 60 TEX. B.J. 104, 107 (1997) ("[A]s an objective matter, there is no guarantee that land-based phone conversations cannot be overheard, misdirected, or intercepted, whether lawfully or not.").

[143] *See* 18 U.S.C. § 2515 (2012) (prohibiting the use of unlawfully intercepted communications as evidence in most situations, including in state and federal court); 18 U.S.C. § 2520(a) (2012) (creating a civil damage remedy for unlawfully intercepted communications); SNIDER & ELLINS, *supra* note 7, at § 2.08 ("Traditional landline telephone conversations are generally treated as confidential.").

[144] *See supra* Section III.A.

[145] Kerr, *supra* note 138, at 381 ("Courts *already* choose perspectives when they apply law to the Internet. They just [do not] realize it.").

An explanation of the technical background illustrates the issue. Information transmitted through the Internet is broken up into small "packets" of information,[146] each of which is independently routed[147] through a number of routers[148] and then reconstructed[149] at the other end—multiple copies of parts of a message may exist in different places at the same time.[150] Since each packet of data is considered independently, the packets that make up an email are not even guaranteed to take the same path through the Internet to their destination.[151] The routing of Internet traffic is even subject to—likely illegal—manipulation from elsewhere in the world.[152] Indeed, the actual transmission of the packet between routers may be protected under wiretap statutes, but the routers in between, which copy and relay the data to the next router, operated by ISPs create a privacy hazard.[153] ISPs can and do intercept, monitor, and even modify traffic for a variety of reasons, such as injecting

---

[146] JAMES F. KUROSE & KEITH W. ROSS, COMPUTER NETWORKING: A TOP-DOWN APPROACH 56 (5th ed. 2010) ("In modern computer networks, the source breaks long messages into smaller chunks of data known as packets."); *see also* INFO. SCIS. INST., INTERNET PROTOCOL 1 (Jon Postel ed., 1981), http://tools.ietf.org/pdf/rfc791.pdf [hereinafter RFC 791].

[147] *See* RFC 791, *supra* note 146, at 2 ("The internet protocol treats each internet datagram as an independent entity unrelated to any other internet datagram.").

[148] KUROSE & ROSS, *supra* note 146, at 59 ("When a packet arrives at a router in the network, the router examines a portion of the packet's destination address and forwards the packet to an adjacent router."); *see* RFC 791, *supra* note 146, at 7 ("This is done by passing the datagrams from one internet module to another until the destination is reached.").

[149] KUROSE & ROSS, *supra* note 146, at 56; *see generally* INFO. SCIS. INST., TRANSMISSION CONTROL PROTOCOL (Jon Postel ed., 1981), http://tools.ietf.org/pdf/rfc793.pdf [hereinafter RFC 793].

[150] Hricik, *supra* note 142, at 113 ("[M]ultiple copies can exist at any given time . . . .").

[151] RFC 791, *supra* note 146, at 2.

[152] Such a situation has recently occurred. In what may best be described as a heist, a hacker at a Canadian ISP recently managed to redirect "an entire chunk of raw internet traffic from more than a dozen internet service providers" through its servers, sifting through the data to intercept bitcoins, an electronic currency. *See* Andy Greenberg, *Hacker Redirects Traffic from 19 Internet Providers To Steal Bitcoins*, WIRED (Aug. 7, 2014, 1:00 PM), http://www.wired.com/2014/08/isp-bitcoin-theft.

[153] *See, e.g.*, *Test Your ISP*, ELEC. FRONTIER FOUND., https://www.eff.org/testyourisp (last visited Aug. 26, 2016).

advertisements,[154] detecting and inhibiting the use of peer-to-peer file sharing software,[155] or sifting through the content of communications to detect copyrighted material.[156]

This process applies to every communication on the Internet, and email is built atop this system. An email message is not sent directly from one computer to another, but is ferried as packets from the sender's computer to their mail provider, which transmits it to the recipient's mail provider, where it is stored in a mailbox awaiting retrieval by the recipient.[157] Copies of the message likely remain in mailboxes stored on servers controlled by both the sender and the recipient's mail provider.[158] The copies of these messages are often further monitored and analyzed by one's email provider, be it a commercial provider like Google, Microsoft, or the user's employer.[159]

For example, Google, one of the world's most popular email providers,[160] has "automated systems [that] analyze [the user's] content (including emails) to provide [the user] personally relevant product features, such as . . . tailored advertising."[161] Google also will share personal information with outside entities

---

[154] *See, e.g.*, Nate Anderson, *How a Banner Ad for H&R Block Appeared on apple.com—Without Apple's OK*, ARS TECHNICA (Apr. 7, 2013, 8:30 PM), http://arstechnica.com/tech-policy/2013/04/how-a-banner-ad-for-hs-ok (describing ISP injection of advertisements).

[155] Milton L. Mueller & Hadi Asghari, *Deep Packet Inspection and Bandwidth Management: Battles over BitTorrent in Canada and the United States*, 36 TELECOMMS. POL'Y 462, 462 (2012) (discussing the throttling of data used by BitTorrent, a peer-to-peer file sharing program).

[156] David Kravets, *ISPs Now Monitoring for Copyright Infringement*, WIRED (Feb. 25, 2013, 2:04 PM), http://www.wired.com/2013/02/copyright-scofflaws-beware.

[157] *See* Marshall Brain & Tim Crosby, *How E-mail Works*, HOWSTUFFWORKS.COM, http://computer.howstuffworks.com/e-mail-messaging/email3.htm (last visited Aug. 26, 2016); s*ee also* JONATHAN B. POSTEL, SIMPLE MAIL TRANSFER PROTOCOL 1–2 (1982), http://tools.ietf.org/pdf/rfc821.pdf.

[158] *See* Brain & Crosby, *supra* note 157. The messages are stored in "remote message folders." *See* M. CRISPIN, INTERNET MESSAGE ACCESS PROTOCOL VERSION – 4REV1 (2003), http://tools.ietf.org/pdf/rfc3501.pdf ("[This protocol] permits manipulation of mailboxes (remote message folders) . . . .").

[159] *See, e.g.*, *Privacy Policy*, GOOGLE, http://www.google.com/intl/en/policies/privacy (last updated June 28, 2016).

[160] As of May 2015, Google reported that Gmail had 900 million users. Kelly Sheridan, *Google I/O: Gmail Hits 900M Users, Android Reaches a Billion*, INFORMATIONWEEK (May 28, 2015, 4:05 PM), http://www.informationweek.com/software/enterprise-applications/google-i-o-gmail-hits-900m-users-android-reaches-a-billion/d/d-id/1320612.

[161] *Terms of Service*, GOOGLE, http://www.google.com/intl/en/policies/terms (last updated April 14, 2014).

for a number of reasons, such as to "enforce applicable Terms of Service, including investigation of potential violations[;] [to] detect, prevent, or otherwise address fraud, security or technical issues[;] [and to] protect against harm to the rights, property or safety of Google, [its] users or the public as required or permitted by law."[162] In a recent incident, Microsoft, apparently acting under the terms of its own privacy policy,[163] accessed the mailbox of a Hotmail subscriber as part of an internal investigation of the theft of the source code of one of its products.[164] Microsoft was one of "a number of companies [with] broad terms of service" that allow for this action, though it is admittedly "rare that any [company] actually follow[s] through and sift[s] through a customer's personal email."[165]

This illustrates the problem with taking an external perspective to determine whether email messages are confidential—they simply are not. And yet, it can hardly be said that this monitoring actually affects the attorney-client relationship. From an external perspective, most electronic communications are not truly private, but the user's acceptance of this type of monitoring would not seem to be inconsistent with the user's expectation of confidentiality and privilege. Consider Professor Rice's idea of safety over privacy: An internet user can feel safe despite electronic monitoring because the user expects that the monitoring has nothing to do with the subject of the communication.[166] Employer monitoring is, of course, more invasive than the use of an automated system by Google to pick which ads to display—it is the nature of the relationship between the client and his employer that makes employer monitoring a cause for concern. Rather than attempting to take an external

---

[162] *Privacy Policy*, *supra* note 159.

[163] Microsoft later updated its policy to state that it would hand private content over to law enforcement when it suspected a crime has occurred rather than investigate the matter itself. *See Microsoft Privacy Statement*, MICROSOFT, https://privacy.microsoft.com/en-us/privacystatement (last updated Aug. 2016) ("[W]e will not inspect a customer's private content ourselves, but we may refer the matter to law enforcement."); *see also* Nick Wingfield, *Microsoft Makes Pledge Not To Snoop on Emails*, N.Y. TIMES, Mar. 29, 2014, at B4.

[164] Nick Wingfield & Nick Bilton, *Microsoft Software Leak Inquiry Raises Privacy Issues*, N.Y. TIMES (Mar. 20, 2014), http://www.nytimes.com/2014/03/21/technology/microsofts-software-leak-case-raises-privacy-issues.html. Hotmail is an email service provided by Microsoft. *Id.*

[165] *Id.*

[166] Rice, *supra* note 25, at 860.

perspective of the issue, courts should focus on privacy from the perspective of the user because the user's perspective is tied to his relationship between himself and the party monitoring his communications.

IV. TWO-FACTOR APPROACH

This Part proposes a new approach to handling the issue of whether privilege can be applied when a client has used an employer-monitored system to communicate with his attorney.

Current tests, such as the four-factor test, vary significantly in their application by focusing too much on actual confidentiality when true privacy is extremely hard to come by on the Internet, and by focusing too much on employee manuals, which are often left unread by employees. Variety in application injects undue uncertainty into the privileged status of electronic communications, which harms the attorney-client relationship. In applying the current tests, courts are implicitly taking an external perspective on the transaction, while ignoring the nature of the parties that have access to the communication. The difference between an employer as an email provider and other parties that have access to a typical electronic communication lies in the relationship between the user and the provider. Taking an internal perspective, a user is aware of and chooses the provider it wants to facilitate electronic communication—this relationship between the user and the provider makes a right of access relevant.

This Note proposes an approach that takes an internal perspective of the communication, through the eyes of the user, to determine whether the user's subjective belief of confidentiality was reasonable. This approach analyzes the relationship between the user and the parties with qualified access to monitor the communication. The analysis starts with a presumption in favor of privilege—an internal perspective of an email user's experience suggests that an email, whether facilitated by an employer or not, is a private communication, like dropping a sealed letter in a mailbox. However, the nature of the relationship between the email user and a party facilitating the communication may overcome this presumption of privilege. This analysis is undertaken in two parts. First, the

court considers the relationship between the parties. Second, the Court considers the nature of the right of access and how it is actually enforced by the party with access.

At step one, the court considers the relationship between the user and the facilitating party with qualified access. This analysis should focus on the foreseeability of a message being accessed for a purpose related to the subject matter of the message. For example, an employee who uses employer-monitored email to communicate with his or her lawyer about a lawsuit involving his or her employer would not have a strong claim to privilege on that communication. This is because the employee can expect his or her employer to have an interest in monitoring employee communications related to itself. Conversely, an employee using such a system to communicate about a matter unrelated to the employer cannot foresee his or her employer having any interest in monitoring that message beyond monitoring in the ordinary course of business. This logic applies to monitoring by any party. For example, Google's automated monitoring of email for advertising purposes is hardly inconsistent with a client's expectation that a communication will remain confidential, or at least will not be revealed to a party that may have a legal stake in the matter. Finally, a party, such as the operator of an Internet router, is not at all relevant because the party has little to no relationship with the user and the user has no way of foreseeing this party's presence. This shift in focus from true confidentiality or right of access to "safety," motive to access, and foreseeability is necessary to protect privacy interests because some party almost always has a right of access to monitor Internet communications for some purpose. However, most parties that monitor Internet communications do not do so with a purpose relating to the subject matter of the underlying communication being monitored. Therefore, clients do not, and should not, expect the monitoring to impact such communications.

At step two, the court considers the nature of the right of qualified access with a focus on how it is actually enforced. An Internet Service Provider or Internet Mailbox Provider has a relatively limited qualified right of access, circumscribed both by privacy laws and by narrow terms of service agreements. An employer has a more substantial right of access, circumscribed by its employee monitoring policy. The exact wording of the

employer's policy deserves little attention, however, and the analysis should be limited to whether it is broad enough to allow for interception and inspection of the communication at issue. However, the employee's knowledge of the policy and the employer's application of that policy is far more important. If an employer openly monitors communications on a regular basis, and regularly informs its employees, this fact would weigh against the application of privilege. Conversely, if an employer reserves a right included in its employee handbook but never exercises that right, it would be unfair to say that this alone can prevent the application of privilege.

CONCLUSION

In the modern world, electronic communications are essential, but third parties often facilitate them. These third parties may have a qualified right of access to the communications, such as permission to access them for business purposes. Employers have among the broadest qualified rights to access information stored on systems they provide to their employees. Since courts will not apply privilege to prevent the disclosure of nonconfidential communications, a framework for handling cases in which a third party has a qualified right of access for an electronic communication is needed—particularly in the case of an employer which monitors its employees. In order to inject certainty into privilege and to avoid reliance on the art of drafting an employee handbook, courts should follow a two-stepped approach. First, the court should consider the relation of the parties; how foreseeable is it that the party with qualified access—the employer—will become an adversary or will have some interest in the matter discussed. Second, the court should consider the nature of the qualified privilege; how broad is the party's—employer's—right to monitor the communications, how do they actually monitor the communications in practice, and how do they interpret their own policy. With this approach, the policy of the attorney-client privilege is upheld, and the situation of a court unexpectedly refusing to apply the privilege can be avoided.