University of Cincinnati Law Review

Volume 81 | Issue 2 Article 7

5-30-2013

# Risky Mail: Concerns in Confidential Attorney-Client Email

Rebecca Bolin
*Yale Law School*, rbolin@gmail.com

# RISKY MAIL: CONCERNS IN CONFIDENTIAL ATTORNEY–CLIENT EMAIL

*Rebecca Bolin*∗

*Early in the days of attorney–client email, David Hricik wrote a soothing law review article,* Lawyers Worry Too Much About Transmitting Client Confidences By Internet E-mail, *arguing that email had risks but could be assumed private for the purpose of professional ethics. The ABA agreed in 1999, issuing a formal opinion that encrypting email was not required by ethical standards, and most jurisdictions followed suit. The 1999 ABA opinion persists today, despite being dangerously technology-specific, focused on almost obsolete technology, and more than ten years later, resting on unsettled legal foundation.*

*Attorneys should be concerned about the risks to confidentiality in attorney–client email for three reasons: legal uncertainty about general privacy expectations for email, broad waivers of email privacy through provider policies, and unrelated disclosure by third parties. Case-specific issues have become critical to determine ethical duties in confidential email: manifold local privacy laws, local ethical standards, and provider policies.*

*Legal, authorized third-party access now poses a serious risk to confidentiality in attorney–client email. At least one type of email, employer-provided email, is no longer considered confidential in this context, a known ethical hazard for attorneys. In the context of Fourth Amendment law, email privacy remains unsettled, even after the landmark Sixth Circuit decision in* United States v. Warshak.

*Attorneys and clients need to understand these risks before informed consent is possible. Technology-based solutions may be part of broader best practices to protect confidentiality. Attorneys and clients must understand the technology at issue, rather than blindly risking clients' confidences and attorneys' ethical duties on obsolete reassurances and technologies they do not understand.*

---

∗ Resident Fellow, Yale Law School Information Society Project. J.D. Yale Law School, B.A. Computational & Applied Mathematics, Rice University. Thanks to the entire Yale Law School Information Society Project and Jack Balkin, Sidney Byrd, Robert Gordon, Margot Kaminski, Christina Mulligan, Wendy Seltzer, and Lee Wilson for helpful comments on earlier drafts.

## I. INTRODUCTION

> Warning—This e-mail, including all attachments is *not* encrypted. Accordingly, it is possible for others to read and use this confidential information. We take no responsibility for using unencrypted e-mail and this e-mail and related attachments may be deemed by the court to be a waiver of attorney–client privilege and the work-product doctrine.[1]

This mocking warning is how a technologist sees lax email practice of attorneys—self-serving boilerplate with no corresponding action.[2] Attorneys have been lulled into false security, risking clients' most precious secrets. In 2009, more than 93% of attorneys used email to communicate privileged or confidential information.[3]

At the dawn of attorney–client email, Professor David Hricik wrote a calm, level-headed law review article, *Lawyers Worry Too Much About Transmitting Client Confidences By Internet E-Mail*, published in 1998.[4]

---

1. Jack Seward, *Failure to Encrypt E-Mail Jeopardizes the Privilege and Work-Product Doctrine: Protect or Perish*, 25 AM. BANKR. INST. J. 44, 44 (2006) ("One thing we can perhaps all agree on is that the following message is not going to be well-received by clients, and in all seriousness professionals are not about to use it, but bankruptcy professionals may indeed need to read it more than once.").

2. *Id*.

3. *Web and Communication Technology*, *in* AMERICAN BAR ASSOCIATION LEGAL TECHNOLOGY SURVEY REPORT 30 (2009).

4. David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-Mail*, 11 GEO. J. LEGAL ETHICS 459 (1998).

Professor Hricik argued that email was not so dangerous, and could be relied on like phone calls or faxes—imperfect but assumed private. The corresponding ABA opinion, issued in 1999, agreed.[5] Encryption was too much worry over email.

In 2005, Professor Hricik brushed up that opinion, again writing that email should be considered private.[6] Since that time, local bar associations have refined and struggled with this position, while technology and law marched on. The ABA modified its position in 2011, requiring attorneys to counsel and warn clients about employer emails and equipment. While an excellent step forward, this discussion is still incomplete. Even today, academics, practitioners, and bar associations rely on dated technology, outdated law, and incomplete assessment of risks. The ABA's 20/20 Committee on Ethics passedlong-awaited reforms in summer 2012, retreating from its now obsolete 1999 position, and offering some guidance in an unresolved ethical problem area.

After disjoint state and national bar opinions, email privacy remains in a state of flux, balancing case-specific policies and security risks, far from the ABA's confident conclusions about broad email privacy back in 1999. This shaky legal foundation is not stable enough for a client's weighty matters and an attorney's ethical duties. Lawyers should consider all of the potential hazards in email to their ethical obligations and their clients' confidences.

I am not concerned by malicious, illegal access in this context, or by careless attorneys sending email to the wrong users or losing devices, though surely both are problematic to an attorney's ethical duties of confidentiality.[7] Careless misdirection and illegal, "hacker" invasion are known hazards.[8] I am primarily concerned about the gray fog surrounding email's particular confidentiality issues involving legal, authorized access by third parties, as well as evolving expectations in email privacy in legal and ethical standards.

---

5. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).

6. *See* David Hricik & Amy Falkingham, *Lawyers Still Worry Too Much About Transmitting E-Mail Over the Internet*, 10 J. TECH. L. & POL'Y 265, 266 (2005).

7. Hricik, *supra* note 4, at 487–88 ("In contrast, inadvertent transmission on an OSP *does* effect [sic] confidentiality, because the recipient most likely does not owe any duty whatsoever to the sender. In this regard, however, the potential for misdirection of e-mail is no different than it is with a fax: reasonable care can virtually eliminate any risk.").

8. *See generally*, Roland L. Trope & Sarah Jane Hughes, *Red Skies in the Morning—Professional Ethics at the Dawn of Cloud Computing*, 38 WM. MITCHELL L. REV. 111 (2011); Bill Piatt & Paula DeWitte, *Loose Lips Sink Attorney–client Ships: Unintended Technological Disclosure of Confidential Communications*, 39 ST. MARY'S L.J. 781 (2008); Ash Mayfield, Comment, *Decrypting the Code of Ethics: The Relationship Between an Attorney's Ethical Duties and Network Security*, 60 OKLA. L. REV. 547 (2007); Andrew Beckerman-Rodau, *Ethical Risks from the Use of Technology*, 31 RUTGERS COMPUTER& TECH. L. J. 1 (2004).

Since 1999, at least one major category of email, workplace employer-provided email, is no longer considered private in this context. Third-party access has now become a known ethical issue for attorneys and clients, showing that expectations in email may now be case-specific inquiry, depending on the provider's privacy policy. Attorneys using third-party systems should no longer rely on the ABA's technology-specific assurance and should instead carefully consider the policies of third-party email services. Attorneys now need to attempt to differentiate individual third-party providers with generally privacy-focused policies, like Yahoo,[9] from services with less robust privacy protection.

In Part I of this Article, I explain the existing legal and technological framework for decisions about email security. This Part describes outdated understandings of technology, as well as the outdated statutes currently covering email.

Part II discusses the major ethical rulings in this area, starting with the ABA's technology-specific 1999 ruling that email should be assumed private. The updated view on email security in the more thoughtful State Bar of California's 2010 opinion shows that the 1999 technology-specific assumptions have become dangerous as technology evolved but ethical standards did not. The ABA's 2011 ethics opinion about employee-provided email concedes that an entire category of email is no longer private, despite the broad conclusion from 1999. Finally, in summer 2012, the ABA released new model rules that retreat from its 1999 position and require attorneys to educate themselves and their clients about the risks of email. Taken as a whole, these opinions and rules show a turning point: case-specific factors about email now determine privacy expectations, not general, technology-specific principles.

Part III explores enduring issues in email confidentiality. The expectation of privacy in email in the context of the Fourth Amendment remains unsettled, more than ten years later. The only federal appellate case on the issue finds a Fourth Amendment expectation of privacy, but not with respect to the Internet Service Provider (ISP) itself, and only after investigating the provider's policies. Privacy policies themselves might contain broad waivers of privacy, which may surprise readers. Finally, confidentiality is at risk when a third party makes an authorized

9. I use Yahoo as an example of a responsible service provider with extensive privacy policies, based in part on its unpopular refusal to give the contents of an email account to the parents of a Marine killed in Iraq. *See* Claudia Buck, *Digital Assets Are Often Forgotten When People Die*, BUFFALO NEWS, Dec. 26. 2011, at C4. However, even in that case, Yahoo lost and was forced to violate its own privacy policies. I also use as examples other generally privacy-focused email providers: "free" providers such as Microsoft (Hotmail), Google (Gmail), or paid providers such as emails associated with Internet accounts for users, such as Comcast.

disclosure, such as responding to information freedom laws or civil discovery.

Part IV considers technology-based solutions for sensitive data, both as technical solutions and as markers of confidentiality. Ethics opinions cannot endure with specific technology requirements. Instead, attorneys need to be aware of technological risks in systems they use and weigh risks with their clients to obtain meaningful consent.

### *A. Background*

Clients tell attorneys their most private, secret information, and attorneys have a solemn duty to protect clients' confidences and keep their secrets.[10] Confidentiality is the bedrock principle of legal ethics, and its duties are nearly absolute.[11] Attorneys have an ethical and practical duty to safeguard their client's information, and failure to do so may waive attorney–client privilege.

Confidentiality is an ethical duty for all attorneys. All states have a codified version of Model Rule of Professional Conduct 1.6, requiring attorneys to safeguard their clients' confidential information.[12] Confidentiality applies to "all information relating to the representation, whatever its source."[13] Attorneys in all states have a duty to protect both privileged and confidential information, even when using email.[14]

Rule 1.6(a) requires a lawyer to refrain from revealing "information relating to the representation of a client unless the client gives informed consent."[15] This requirement is closely related to Rule 1.1 requiring "competent representation to a client," which includes confidentiality.[16] Comments to Rule 1.6 also require attorneys to take reasonable efforts to safeguard the information from their own agents, and from communicating confidential information to unintended recipients.[17]

These rules are not technology-specific, but instead show an attorney must use his professional judgment about the medium of communication and the risks to confidential information. The rules also allow attorneys to rely on both law and contracts, including confidentiality agreements, in this ethical duty. An attorney may not disclose confidential

10. *See generally* Daniel R. Fischel, *Lawyers and Confidentiality*, 65 U. CHI. L. REV. 1, 3–9 (1998) (explaining confidentiality's importance to lawyers and clients).

11. *Id*. at 1.

12. MODEL RULES OF PROF'L CONDUCT R. 1.6 (2009).

13. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 3 (2009).

14. Hricik, *supra* note 4, at 478.

15. MODEL RULES OF PROF'L CONDUCT R. 1.6(a) (2009).

16. MODEL RULES OF PROF'L CONDUCT R. 1.1 (2009).

17. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 16, 17 (2009).

information, subject to very limited exceptions.[18]

Confidentiality is critical to protecting the privileged status of an attorney's communications with clients. Attorney–client privilege is intended to encourage clients' honest and full disclosure without fear.[19] The traditional elements of attorney client privilege are: (1) where legal advice of any kind is sought (2) from a professional legal advisor in his capacity as such, (3) the communications relevant to that purpose, (4) made in confidence (5) by the client, (6) are at this instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except when the client waives the privilege.[20] Because privilege is an obstruction to truth in a system generally designed to seek truth, privilege is often strictly confined.[21] The relevant element here, present in all formulations of the elements, is confidentiality, and the risk of waiver when communications are not confidential.[22]

Privilege protects communications which are "intended to remain confidential," and are made in such circumstances that they are "reasonably expected and understood to be confidential."[23] Privilege can be waived by types of third-party access. For example, a communication might not be confidential if the parties made no effort to prevent the communication from being overheard, or if the information is intended to reach other parties.[24] Attorneys may waive privilege by sending information in a way that allows third parties to access it.[25]

Courts and jurisdictions can vary wildly in determining when privilege is waived by third-party access, broadly using three different strategies: a strict test under which disclosure causes waiver, a lenient test which uses intent, or a middle-ground test, which most courts use.[26] Courts can consider (1) reasonableness of precautions, (2) number of inadvertent disclosures, (3) extent of disclosure, (4) measures to rectify

18. *See* Fischel, *supra* note 10, at 1.

19. Upjohn Co. v. United States, 449 US 383, 389 (1981).

20. JOHN HENRY WIGMORE, EVIDENCE § 2292 (John T. McNaughton ed., 1961).

21. *Id*. § 2291(4).

22. Other formulations of the traditional factors will also include confidentiality. *See, e.g.*, RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 68 (2000) ("(1) a communication (2) made between privileged persons (3) in confidence (4) for the purpose of obtaining or providing legal assistance for the client.").

23. United States v. Melvin, 650 F.2d. 641, 645 (5th Cir. 1981).

24. United States v. Gann, 732 F.2d. 714, 723 (9th Cir. 1984) (no privilege when statement made in presence of several searching police officers); *In re* Grand Jury Proceedings, 727 F.2d 1352, 1358 (4th Cir. 1984) (intended public prospectus).

25. Hricick considers this kind of waiver through sending email to the wrong parties. *See* Hricik & Fallingham, *supra* note 6, at 268.

26. David B. Smallman, *The Purloined Communications Exception to Inadvertent Waiver: Internet Publication and Preservation of Attorney–Client Privilege*, 32 TORT & INS. L.J. 715, 723 (1997).

the disclosure, (5) any delay in taking those measures, and (6) overriding issues of fairness and justice.[27] Courts have varied slightly interpreting the requirements for confidentiality. Some follow a subjective, "intent" requirement, while others refer to circumstances "reasonably apparent."[28] Courts often inquire whether a reasonable person would have expected the communication to reach third parties, not the subjective state of mind of the communicator.

Expectation of privacy is related to, but not identical to, confidentiality in the context of privileged communication; communications may still be considered confidential even when they are not private. A surreptitious eavesdropper, though compromising privacy, may not compromise confidentiality, assuming the attorney and client took reasonable steps to protect the communications.[29] Sometimes, a known third-party's presence will not waive privilege. For example, an attorney speaking to a client through a translator is not private, but would be considered confidential.[30] An attorney speaking to a client with another privileged party, such as a spouse, would also not compromise privilege.[31] Recorded jail communications can also be privileged, despite the eavesdropper.[32]

Privilege law can allow attorneys and clients to use reasonable efforts

27. *Id.* at 723–24.

28. RESTATEMENT (THIRD) OF LAW GOVERNING LAWYERS § 71, reporter's note to cmt. b (2000) (citing Esposito v. United States, 436 F.2d 603, 606 (9th Cir.1970) ("reasonable person"); United States v. Tellier, 255 F.2d 441, 447 (2d Cir. 1958) ("understood")); *cf.* Robert P. Mosteller & Kenneth S. Broun, *The Danger to Confidential Communications in the Mismatch Between the Fourth Amendment's "Reasonable Expectation of Privacy" and the Confidentiality of Evidentiary Privileges*, 32 CAMPBELL L. R. 147, 172–73 (2010).

29. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 71 cmt. c, illus. 1 (2000) ("Client and Lawyer confer in Client's office about a legal matter. Client realizes that occupants of nearby offices can normally hear the sound of voices coming from Client's office but reasonably supposes they cannot intelligibly detect individual words. An occupant of an adjoining office secretly records the conference between Client and Lawyer and is able to make out the contents of their communications. Even if it violates no law in the jurisdiction, the secret recording ordinarily would not be anticipated by persons wishing to confer in confidence. Accordingly, the fact that the eavesdropper overheard the Client–Lawyer communications does not impair their confidential status.").

30. United States v. Kovel, 296 F.2d 918, 921 (2d Cir. 1961) (allowing confidentiality with necessary third parties).

31. RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 71 cmt. b (2000) ("[I]n a jurisdiction that recognizes an absolute husband–wife privilege, the presence of a wife at an otherwise confidential meeting between the husband and the husband's lawyer does not destroy the confidentiality required for the attorney–client privilege.").

32. *See* United States v. Salyer, No. 10-0061, 2012 WL 507118 (D. Cal. 2012) (determining privilege in calls made by a defendant in custody and recorded, based on content seeking legal advice); RESTATEMENT (THIRD) OF LAW GOVERNING LAWYERS, § 71 cmt. c, illus. 3 (2000) ("A jailer requires Client, an incarcerated person, and Lawyer to confer only in a conference area that, as Client and Lawyer know, is sometimes secretly subjected to recorded video surveillance by the jailer. If Client and Lawyer take reasonable precautions to avoid being overheard, the fact that the jailer secretly records their conversation does not deprive it of its confidential character.").

to create confidentiality in places where a reasonable expectation of privacy can never exist. An attorney may, with reasonable measures, speak confidentially to a client at a public restaurant, at a park bench, at a jail, or in a courthouse hallway. All of these circumstances are outside the protection of the Fourth Amendment's reasonable expectation of privacy. [33] The role of the participants, the actions of the participants, and the law of privilege allows the speakers to construct a temporary space for confidentiality, using reasonable means to protect its confidentiality. In such a space, the efforts of the parties are critical to establish confidentiality.[34]

### *B. How Email Works*

The bedrock for the ABA and state decisions about confidentiality in encrypted email is Professor Hricik's 1998 description of "Internet e-mail," then an emerging technology.[35] This conceptual understanding, before clouds and Wi-Fi and mobile broadband, fixes email as a technology far from its modern embodiment. Though useful at the time, these facts are incomplete today.

The Internet is a collection of hosts, such as home computers or servers in a data center, connected to a network of routers, devices that decide how to move information through the network.[36] Routers can be as simple as the home variety that often provide Wi-Fi wireless networking, or as complex as the cabinet-sized core routers in major Internet exchange points. For a host to send information to a particular destination host, it must first split the information into short segments called "packets." The host directly connects to its local router and sends each packet to the local router along with the intended destination.[37]

The router forwards the packet based on the destination to another router it believes is closer to the destination. The process continues until the packet reaches a router that is directly connected to the destination host, which simply forwards it to the host. Any intermediate router will

33. *See* Mosteller & Broun, *supra* note 28, at 172–73.

34. *See* RESTATEMENT (THIRD) OF THE LAW GOVERNING LAWYERS § 71 cmt. c, illus. 2 (2000); *id.* § 71, reporter's note to cmt. c (based on Schwartz v. Wenger, 124 N.W.2d 489 (Minn. 1963) (allowing eavesdropper testimony because client and attorney made no effort to ensure secrecy in courtroom hallway conversation)).

35. Hricik, *supra* note 4, at 461–65 ("E-mail programs send correspondence from one personal account to any Internet machine . . . [s]ignificantly, for the reasons discussed below, when I log onto AOL, my computer is connected directly over a phone line to AOL.").

36. *See* ANDREW S. TANENBAUM & DAVID J. WETHERALL, COMPUTER NETWORKS 54 (5th ed. 2011) [hereinafter COMPUTER NETWORKS].

37. *Id*. at 355–63 (["T]he network layer must know about the topology of the network (i.e. the set of all routers and links) and choose appropriate paths through it, even for large networks.").

be able to read the contents of an unencrypted packet.[38] The packets contain a sequence number and other information that allows the receiving host to reassemble the original, complete message.

This style of decentralized routing is called "packet-switched networking" and allows the Internet to continue to operate even when some of the links in the network fail, because packets will simply take a different path.[39] Neither the sender nor any router controls which full path any packet takes over the network, and each packet may take a completely different path even for the same message. This routing also makes it impossible to predict the route of any particular message or any packet with certainty. The decentralized network of the Internet differs from a circuit-switched network, such as the historical telephone network.[40] In a circuit-switched network, the entire message will follow the same path, and the connection will be dedicated that communication for a finite period of time.[41]

In 1997, users believed that email traveled to a personal computer, like a physical mailbox, where it stopped:[42]

> Thus, if I send an e-mail message from my AOL e-mail address to my Baker & Botts e-mail address, AOL merely sends the message through its host onto the Internet. The e-mail is then routed over the Internet to Baker & Botts' host computer, where it is then routed by that computer to my mailbox. I can then complete the transmission by logging onto my Baker & Botts e-mail mailbox, providing my password for my Baker & Botts mailbox, and downloading the message to the computer in my office.[43]

When Professor Hricik wrote his article, this description was more or less true. AOL, like most service providers, deleted mail off its servers after a few days to save on then-expensive storage. In 1997, Professor wrote of AOL's e-mail deletion policy:

(i) The current default is about two (2) days after it is read. E-mail that is

---

38. *See* Hricik, *supra* note 4, at 466.

39. COMPUTER NETWORKS, *supra* note 36, at 162–64 ("With packet switching there is no fixed path, so different packets can follow different paths, depending on the network conditions at the time they are sent, and they may arrive out of order . . . . With packet switching, packets can be routed around dead switches.").

40. *Id*. at 9–12.

41. *Id.* at 161–2 ("[O]nce a [phone] call has been set up, a dedicated path between both ends exists and will continue to exist until the call is finished. An important property of circuit switching is the need to set up an end-to-end path *before* any data can be sent.").

42. Daniel J. Pope & Helen Whatley Pope, "*Is It Safe . . . .*", 64 DEF. COUNS. J. 138, 141 (1997) ("Unlike web pages, e-mail addresses are accessible only by the mailbox owners and by those responsible for maintaining the computer system in which the mailbox resides. Anyone can send to an e-mail address, but only its owner, or one with the password to the mailbox, can access what has been sent. In this way, e-mailboxes are similar to post office boxes—without the key, you can't get in.").

43. Hricik, *supra* note 4, at 465.

> sent but not read is permanently deleted from the system after about twenty-five to thirty (25–30) days. (Consequently, to keep copies of any communications, you should store them on your personal computer hard drive or in print form.).[44]

Today, AOL's terms of service are silent on the deletion issue, suggesting it could keep a copy of everything coming in or out of an email account forever.

When Professor Hricik accessed his AOL mail in 1998, he used a program running on his computer called a mail client. Well-known, stand-alone mail clients are common today as well, such as Microsoft Outlook. These programs allow the user to store a copy of the mail on the user's own device, and the mail client accesses the mail from the device's storage, transferring incoming and outgoing mail to the server. Today, many companies use these clients with their own internal servers that perform mail exchange in an internal network. Today, there is no one "Baker & Botts' host computer"; there are multiple in an internal network which many attorneys can access from many locations, through internal networks as well as the Internet through secured connections.

Another common method of accessing mail is using an email client within a webpage. This type of access to email through an Internet site is called "webmail." Corporate off-site mail and services like Gmail or Yahoo use this type of access. For these services, data is accessed, stored, and sent to off-site computing and storage facilities, commonly called "the cloud."[45] The operator of the cloud would, technically speaking, be able to view any unencrypted message stored in its servers. The data may also be stored temporarily in storage such as a browser cache when accessed by a user.

Today, cloud computing is common for many Internet users, not just mysterious system administrators. Users routinely store data in clouds, from photos to emails to online gaming profiles.[46] Sophisticated

---

44. *Id*. at 488–89.

45. Paul Lanois, *Privacy in the Age of the Cloud*, 15 J. INTERNET L. 3, 3 (2011); COMPUTER NETWORKS, *supra* note 36, at 672–73 ("Nowadays, much of the excitement around the Web is using it for applications and services. Examples include buying products on e-commerce sites, searching library catalogs, exploring maps, reading and sending email, and collaborating on documents. These uses are like traditional application software (e.g. mail readers and word processors). The twist is that these applications run inside the browser, with user data stored on servers in Internet data centers. They use Web protocols to access information via the Internet, and the browser to display a user interface. The advantage of this approach is that users do not need to install separate application programs, and user data can be accessed from different computers and backed up from the service operator. It is proving so successful it that it is rivaling traditional application software. Of course, the fact that these applications are offered for free by large service providers helps. This model is the prevalent form of cloud computing, in which computing moves off individual desktop computers and into shared clusters of servers in the Internet.") (emphasis omitted).

46. Lanois, *supra* note 45, at 3–4.

corporations store their data using expensive, complex networks with the highest security; 45%of multi-national companies were using some form of cloud computing in 2011.[47] Of course, cloud computing has its own risks and ethics issues, yet to be decided, especially if maintained by a third party.[48] It also has security and privacy only as good as the provider allows. At a minimum, cloud-based solutions risk the problem of inconsistent jurisdictional rules on privacy and inconsistent cross-national standards.[49]

Users can access webmail services for email using many kinds of web-based applications, mail applications, and smartphone applications. For example, a user can access Google's Gmail through any major browser, as well as through specially designed Gmail mobile programs or through iPhone's mail application configured for that account. Often, users access the data using only the cloud, storing nothing on their own computers. Others still use Professor Hricik's model and download data to their computers after deleting the server copy, leaving an archival copy or perhaps no copy at all for the mail provider. It is possible to use a webmail service exactly as Professor Hricik described in 1998, or to access data only through webmail, or to store copies on both a computer and on the cloud.

Professor Hricik believed email could not be searched or even stored by a service provider.[50] Because mail was so quickly deleted at that time, no copy persisted to search.[51] Today, email may be stored long-term in the cloud, which is easy to search and often must be searched. It may even exist without a user's knowledge as an archival or back-up

47. *Id*. at 3.

48. *See generally* Nicole Black, CLOUD COMPUTING FOR LAWYERS 26 (2012) (published by the ABA). The ABA's 20/20 Commission issued a paper for comment in 2010 which included issues about cloud computing, but has not yet addressed those issues in formal recommendations. *See* Letter from ABA Comm'n on Ethics 20/20 Working Grp. on the Implications of New Techs., to ABA Entities, Courts, Bar Ass'n (state, local, specialty and int'l), Law Schs, Individuals, and Entities (Sept. 20, 2010) *available at http://www.americanbar.org/groups/professional_responsibility/aba_commission_on_ethics_20_20/work_product.html*.

49. *See* Lanois, *supra* note 45, at 10. Though not strictly "email," message delivery within a cloud is how many secure environments, such as banks or medical providers, correspond with users. Readers may be familiar with a generic email from a secure provider notifying users to log in to their account to read their message, perhaps for a banking alert or a medical bill. For example, a bank might notify a user of a bill or transaction by email or text message. However, the message will direct the user to the bank's secure web portal to view details. Thus, the provider secures the message by the user's authentication and access methods. Many law firms or corporate clients already have similar mailboxes to store secure messages.

50. Hricik, *supra* note 4, at 472–73 ("As with the [Web], a third-party with access to a law firm's database could, for example, search by client's name, or a specific topic, and locate such documents. The same is true for information on the [Web], but it is not true for Internet e-mail.").

51. *See generally id*. at 473 ("[T]he concerns present when a law firm gives access of its database to a third party are not in any way reasonably analogous to transmitting Internet e-mail.").

copy. Providers regularly search e-mail to monitor spam, to monitor employees' personal use, to provide targeted advertising, or to enforce terms of service. When Professor Hricik sends a message to his Baker & Botts account from AOL today, both providers likely keep multiple copies on multiple servers. They may even store archival snapshots of the servers for back-up purposes, in multiple locations, which may be in neither Baker Botts' Texas headquarters nor AOL's Virginia headquarters. The copies may not even be stored in the United States.

The common persistence of that data, unlikely in the 1990s, may leave a complete record. Justice Brandeis observed in dissent for a case in a wiretapping precedent to *Katz*, "[w]ays may some day be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[52] Today, those secret drawers are servers with years of archived emails. Complete copies of emails may be commonly kept at both the sending and receiving end.

Professor Hricik and the ABA categorized email into four categories: direct e-mail, private system e-mail, "on-line service," and "Internet e-mail."[53] The first category, direct email, is considered an email sent from one modem to another, or "[t]he modem simply converts the content of the e-mail into digital information that is carried on land-based phone lines to the recipient's modem."[54] "This is virtually indistinguishable from . . . sending a fax."[55] In 2005, Professor Hricik suggested this was possible using two dial-up connections and that the direct phone line would protect the communication.[56] Today, such a connection for email is unlikely outside a private network.

The second category, "private system email," persists today as the most secure.[57] In 1998, Professor Hricik described a local network using local proprietary connections called a Local Area Network (LAN), as opposed to the Internet at large. This secure network is how most offices operate today.[58] Professor Hricik also describes offsite access

52. Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting).

53. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 6–7 (1999); Hricik, *supra* note 4, at 485–92 (titling the categories with slight modification).

54. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 6 (1999).

55. *Id*.

56. *See* Hricik & Fallingham, *supra* note 6, at 272.

57. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 6–7 (1999).

58. COMPUTER NETWORKS, *supra* note 36, at 19–23 ("LANs are widely used to connect personal computers and consumer electronics to let them share resources (e.g. printers) and exchange information. When LANs are used by companies, they are called enterprise networks. Wireless LANs are very popular these days, especially in homes, older office buildings, cafeterias, and other places where it is too much trouble to install cables.") (emphasis omitted).

when a "lawyer's network dials that client's network directly over land-based phone lines and transmits the message."[59] Professor Hricik claimed that this communication never used "external phone lines" to access the private network.[60]

In 2005, Professor Hricik presented a more modern version of accessing private networks through Virtual Private Networks (VPN) and Secure Sockets Layer (SSL).[61] Both VPN and SSL require certificates that provide a secure "tunnel" through the Internet using encryption and authentication requirements.[62] Packets that are intercepted by intermediate routers are unintelligible. Both SSL and VPN applications may use "external phone lines" and the Internet at large, but can secure data in the transit network using additional security measures, always including encryption, and typically requiring authentication of one or both end points.

Readers today are likely quite familiar with SSL technology, commonly used by "secure" websites like banks. Readers are likely familiar with a cartoon lock on their browser indicating a connection like SSL, or newer protocols today, such as TLS. Readers may also be familiar with VPN, which requires special software to allow a user to remotely log on to a secure network. Many firms and companies use this kind of software and even more security, such as dynamic passwords on key chains. Today, private networks and remote access are commonly used to communicate and secure email.

The third email category, "on-line service providers," is shorthand for an email address provided by an Internet Service Provider.[63] In the 1990s, this email was furnished as part of a paid service to access the Internet; thus, AOL was both the mail provider and the ISP.[64] This same identity persisted over AOL's other private services, identifying the user based on a screen name.[65] At that time, Professor Hricik would have used a dial-up connection to connect to AOL's proprietary network, or "online" service, and he may have then connected the Internet through AOL. Messages sent directly to AOL could use the dial-up connection to AOL's "online" services, not the Internet.

Professor Hricik relied on AOL policies and the law at the time to suggest that an attorney could rely on this service to send a message to

59. Hricik, *supra* note 4, at 486.

60. *Id.*

61. Hricik & Fallingham, *supra* note 6, at 279–80.

62. COMPUTER NETWORKS, *supra* note 36, at 26, 853–55 (explaining VPN and SSL).

63. Hricik, *supra* note 4, at 487–88.

64. *Id*. at 464–65.

65. *See id*.

an "online" client who used the same service.[66] Note in that case, the attorney's dial-up connection and e-mail would be provided by AOL, as would the client's. Today, a user can still have an e-mail assigned by their service provider, such as Comcast, but distinct mail providers are more common, such as Google or Hotmail, and such communication would generally include the Internet. Today, this situation is unlikely outside a private network.

The fourth type, "Internet E-Mail," is e-mail communicated by an Internet provider but using a separate mail service.[67] Today, we would consider this most mail outside a private network. Today, users commonly use a third-party Internet service provider, such as Comcast, to communicate mail from another mail service, such as Gmail.

In 1998, Professor Hricik relied heavily on "land-based phone lines," where he believed messages moved.[68] Lawyers in the days of dial-up could connect directly through phone lines,[69] as Professor Hricik remembered in 2005.[70] Today, outside of a private network, email goes through multiple servers and routers, and is sent over fiber-optic cabling with mixed purpose, including television, phone, and Internet data.[71]

Professor Hricik always knew the first stop on his email's journey, the initial router that was installed at AOL and dialed into by his home modem, or by Baker & Botts at his office. Today, Professor Hricik could send the same emails using Wi-Fi, or he could use his phone, tablet, or computer on mobile broadband.[72]

Using any of these services, he could access his email from the mail provider's cloud, using a web client to access a cloud instead of a mail client. These messages may or may not use wireless services, and they would then use modern fiber-optic cables and innumerable networking equipment like routers and switches along the way in unknown

66. *Id*. at 492.

67. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 8–9 (1999).

68. *See also id*. at 9 ("[Because] Internet e-mail typically travels through land-based phone lines, the only points of unique vulnerability consist of the third party-owned Internet services providers or 'ISPs.'").

69. Peter R. Jarvis & Bradley F. Tellam, *The Internet: New Dangers of Ethics Traps*, 56 OR. ST. B. BULL. 17 (1995) ("If a lawyer's computer and a client's computer communicate directly over the phone lines and not through a third-party computer, the fact that the lawyer and the client are communicating in bits and bytes rather than by voice should not affect the availability of attorney–client privilege."); David Hricik, *Confidentiality and Privilege in High-Tech Communications*, 60 TEX. B. J. 104, 110 (1997).

70. Hricik & Fallingham, *supra* note 6, at 272 ("E-mail can also be sent directly over land-based phone lines, from one computer to another. When e-mail is sent this way, it is no different than sending a fax.").

71. *Id*. at 277.

72. *See* COMPUTER NETWORKS, *supra* note 36, at 65–69 (Third Generation Mobile Phone Networks), 70–73 (Wireless LANs: 802.11).

jurisdictions.

### *C. Privacy Statutes for Email: ECPA*

To understand email privacy requires discussing the dated federal privacy laws and their exceptions to determine these rights. Two types of laws can apply to email: those targeted at real-time interceptions, such as wiretapping, and those intended for access of communications in storage at a later date.

The Electronic Communications Privacy Act (ECPA) was enacted in 1986 to amend Title III of the Omnibus Crime Control and Safe Streets Act of 1968, which prevented wiretapping.[73] ECPA was intended to protect privacy in new communication mediums and had wide support.[74] ECPA has not been amended since, despite growing criticism, in the context of email and many other applications.[75] The 1986 amendments had two chapters relevant here: the Wiretap Act and the Stored Communications Act (SCA).

The Wiretap Act establishes criminal and civil liability for "any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" as well as for any use, disclosure, or attempted use of such interceptions.[76] This was intended to protect "the privacy of electronic communications by prohibiting their unlawful interception while travelling to the recipient."[77] Like previous wiretap provisions, ECPA states that intercepted messages do not lose their privileged character because of its statutory authority.[78] ECPA in itself has no authority regarding privilege.

The Wiretap Act exempts interceptions "where one of the parties to the communication has given prior consent to such interception" and disclosure by a service provider "with the lawful consent of the originator or any addressee or intended recipient."[79] ECPA also exempts communications services providers if they use intercepts "in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the

73. Yvette Joy Liebesman, *The Potential Effects of* United States v. Councilman *on the Confidentiality of Attorney–client E-Mail Communications*, 18 GEO. J. LEGAL ETHICS 893, 899 (2005).

74. *See id*. at 902–03.

75. *See* Miguel Helft & Claire Cain Miller, *News Analysis: 1986 Privacy Law is Outrun by the Web*, N.Y. TIMES, Jan. 9, 2011, *available at http://www.nytimes.com/2011/01/10/technology/10privacy.html?pagewanted=all*.

76. 18 U.S.C. § 2511(1)(a) (2006).

77. Liebesman, *supra* note 73, at 900.

78. 18 U.S.C. § 2517(4) (2006).

79. 18 U.S.C. § 2511(2)(d); 2511(3)(b)(ii) (2006).

protection of the rights or property of the provider of that service."[80]

The Stored Communications Act covers messages in storage. SCA established liability for a person who "intentionally accesses without authorization a facility through which an electronic communication service is provided" or "intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage."[81]

Service providers have an exemption from the Stored Communications Act to access stored communications.[82] However, it is a crime for ISPs to disclose stored communications, generally speaking,[83] subject to several exceptions similar to the Wiretap Act, including "as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service."[84] Service providers can also disclose communications with consent "of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of the remote computer service."[85] Government entities, such as law enforcement, have abilities to compel disclosure within ECPA, discussed later, which are not enjoyed by private entities, such as service providers.[86]

## II. ETHICS OPINIONS REGARDING EMAIL

In the late 1990s, attorneys became concerned about the then-emerging technology of email, and local bar associations responded. The South Carolina Bar issued the earliest opinion about email encryption in 1995, which prohibited e-mail as insecure and required a client's approval.[87] However, a second 1997 opinion required only expectation of privacy and allowed email if encryption was discussed between the client and lawyer. "A lawyer should discuss with a client such options as encryption in order to safeguard against even inadvertent disclosure of sensitive or privileged information when using e-mail."[88]

Other local bar associations found encryption unnecessary in the late 1990s: Alaska, District of Columbia, Illinois, Kentucky, New York City, New York State, North Dakota, Pennsylvania, South Carolina and

80. 18 U.S.C. § 2511(2)(a)(i) (2006).
81. Liebesman, *supra* note 73, at 901; 18 U.S.C. § 2701(a) (2006).
82. 18 U.S.C. § 2701(c) (2006).
83. 18 U.S.C. § 2702 (2006).
84. 18 U.S.C. § 2702(b)(5) (2006).
85. 18 U.S.C. § 2702(b)(3) (2006).
86. 18 U.S.C. § 2703 (2006).
87. South Carolina Bar Advisory Op. No. 94-27 (1995).
88. South Carolina Bar Advisory Op. No. 97-08 (1997).

Vermont, though often with a requirement to inform clients.[89] Some bar associations required more caution, in the form of specific types of consent or technological protections.[90]

In the 1990s, courts encountered little privileged email, and had made only a handful of isolated rulings in otherwise routine cases that email could be used for privileged material.[91] In 1995, the American Bar Association tackled "rapidly developing technology."[92] In Formal Opinion 95-398, the ABA considered third-party maintenance of networks and "terminal[s]" containing clients' information.[93] The ABA states that when a non-attorney accesses client files in this context, attorneys must supervise the relationship to ensure that the non-attorneys understand their obligations and "make reasonable efforts to ensure that the service provider will not make unauthorized disclosures of client information."[94]

This ruling was consistent with guidance from Model Rule of Professional Conduct 1.6 and with practices concerning third-party access to attorney data. Opinion 95-398 also references Rule 5.3, Responsibilities Regarding Nonlawyer Assistants. This rule requires firms to establish policies to uphold confidentiality requirements, and

89. Alaska Bar Ass'n, Ethics Op. 98-2 (1998) ("While it is not necessary to seek specific client consent to the use of unencrypted e-mail, clients should nonetheless be advised, and cautioned, that the communications are not absolutely secure."); District of Columbia Bar Ass'n, Op. No. 281 (1998); Ill. State Bar Ass'n Advisory, Op. on Prof'l Conduct No. 96-10 (1997); Kentucky Bar Ass'n, Advisory Ethics Op. KBA E-403 (1998) ("[A] lawyer does not violate Rule 1.6 by communicating with a client using electronic mail services, including the Internet, without encryption. Nor is it necessary, as some commentators have suggested, to seek specific client consent to the use of unencrypted e-mail."); Ass'n of the Bar of the City of New York, Formal Op. 1998-2 (1998) ("Different levels of security on the Internet as well as off the Internet would seem to be appropriate for matters of differing sensitivity. But we do not believe that a blanket prohibition on the use of e-mail for client communications is either necessary or appropriate."); New York State Bar Ass'n, Comm. on Prof'l Ethics, Op. 709 (1998); State Bar Ass'n of N. Dakota, Ethics Comm., Op. 97-09 (1997) ("[R]outine matter with clients and/or other lawyer jointly representing clients via unencrypted e-mail carries adequate assurances, and/or a reasonable expection, or confidentiality."); Orange Cnty. Bar Ass'n, Professionalism and Ethics Comm., Formal Op. No. 97-002 (1997) ("The use of encrypted e-mail is encouraged, but not required."); Vermont Bar Ass'n, Advisory Ethics Op. 97-05 (1997) ("The Committee believes that any lawyer may use e-mail and the internet . . . .").

90. State Bar of Arizona, Ethics Op. 97-04 (1997) ("Lawyers may want to have the e-mail encrypted with a password known only to the lawyer and client so that there is no inadvertent disclosure of confidential information."); Iowa Bar Ass'n, Op. 97-01 (1997); Missouri Informal Advisory Ops. 990007, 980029, 970230, and 970161; Pennsylvania Bar Ass'n Comm. On Legal Ethics, Op. 97-130 (1997) (lawyers must obtain consent to use unencrypted email for sensitive communications); North Carolina Ethics Op. RPC 215 (1995).

91. *See, e.g.*, Amylin Pharma., Inc. v. Regents of Univ. of Minn., No. 96cv2061-JM, 1998 WL 849078 (D. Cal. 1998); Int'l Marine Carriers, Inc. v. United States, No. 9510670, 1997 WL 160371, at * 3 (D.N.Y 1997); Nat'l Emp't Serv. Corp. v. Liberty Mut. Ins. Co., No. 93-2528-G, 1994 WL 878920, at * 3 (Mass. 1994).

92. ABA Comm. On Ethics and Prof'l Responsibility, Formal Op. 95-398 (1995).

93. *Id*.

94. *Id*.

attorneys must ensure that nonlawyers behave appropriately. Opinion 95-398 found that "a lawyer might be well-advised to secure from the service provider in writing, along with or apart from any written contract for services that might exist, a written statement of the service provider's assurance of confidentiality."[95] The ABA has applied this rule to many kinds of outsiders hired by attorneys, from accounting, to photocopying, to paper disposal, and to technical vendors with access to confidential databases.[96]

### *A. ABA Formal Opinion 99-413*

In 1999, inspired by Professor Hricik's calming assurances that email should be assumed private, the ABA responded to the states' patchwork ethical opinions with Formal Opinion No. 99-413, declaring that email encryption was generally not necessary to protect client confidence:[97]

> A lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet without violating the Model Rules of Professional Conduct (1998) because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint. The same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail. A lawyer should consult with the client and follow her instructions, however, as to the mode of transmitting highly sensitive information relating to the client's representation.[98]

The ABA cited to Professor Hricik constantly, in thirteen footnotes out of forty.[99] The ABA compared email to many other forms of communication: commercial and U.S. postal mail, telephones, cordless and cellular phones, and facsimile.[100] The ABA found that email was technically insecure, like other means of transmission, but that "interception or dissemination is a violation of the law," as with other technologies.[101]

The ABA addressed third-party access to email, when provided through an OSP—at that time a service like AOL. The ABA suggests that the security policies, protection from outside hackers, and privacy policies restricting internal OSP access, could affect whether a user has

95. *Id*. at 2.

96. The ABA issued an almost identical opinion in 2008, adding some requirements for outsourcing attorneys. ABA Standing Comm. on Ethics and Prof'l Responsibility, Formal Op. 08-451 (2008).

97. *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 1 (1999).

98. *Id*.

99. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).

100. *Id*. at 3–6.

101. *Id*. at 1.

a reasonable expectation of privacy. The ABA then generalized that providers like AOL to have "a formal policy that narrowly restricts the bases on which system administrators and OSP agents are permitted to examine user e-mail"—that is, the ABA assumed the ISP had a privacy policy that protects the user's privacy, as AOL's did.[102]

The ABA also claimed that "irrespective of the OSP's formal policy," access is limited by law. The ABA cited the ECPA to claim that "federal law imposes limits on the ability of OSP administrators to inspect user e-mail, irrespective of the OSP's formal policy. Inspection is limited by the ECPA . . . Further, . . . disclosure of those communications for purposes other than those provided by the statute is prohibited."[103] The ABA confidently concluded that "[t]he same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail."[104]

As with similar opinions, the ABA suggested an exception that threatened to swallow the entire rule. Attorneys should consult their clients when "information being transmitted is so highly sensitive that extraordinary measures to protect the transmission are warranted."[105] ECPA is, of course, the law in question.

It is difficult to overstate experts' reliance on ECPA for the expectation of privacy. Hricik, the ABA, and state bars all explicitly rely on ECPA protections to support a reasonable expectation of privacy.[106] The ABA states that it is unreasonable to avoid unencrypted email "when unauthorized interception or dissemination of the information is a violation of the law."[107]

Professor Hricik was deeply concerned with malicious interception, and he used ECPA to show an expectation of privacy in this type of hacker interception.[108] I agree with him on this point, but not on his broad categorization of ECPA as a watertight barrier to a third party's inspection of private emails.[109] The ABA, at least in 1999, also rested on ECPA as protecting communications, emphasizing the business requirements as limiting OSP access under ECPA.[110]

---

102. *Id*. at 7.

103. *Id*. at 8.

104. *Id*. at 1.

105. *Id*. at 10.

106. Liebesman, *supra* note 73, at 894.

107. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 1 (1999).

108. *See* Hricik, *supra* note 4, at 471–72.

109. Hricik & Fallingham, *supra* note 6, at 283 ("In addition, while an on-line ISP could, theoretically, read every single message sent within its system, it is unlawful to do so. Under federal law, a provider of electronic communications services may intercept messages only if it is 'in the normal course of his employment . . . .'").

110. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 8 (1999). ("Moreover,

Shortly after, many local bar associations followed the ABA's lead and issued opinions that encrypted email was not necessary to comply with ethical obligations, often with a requirement to warn clients or discuss risks including Delaware, Florida, Maine, Utah, and Virginia.[111] To this day, Texas has no opinion related to the matter, causing conflict with other state ethical obligations of diligent representation and of confidentiality.[112]

After this opinion, many industry and information specific data privacy laws passed around the world. These laws, not even considered in 1999, are now the focus of entire books, classes, conferences, and training programs.[113] Massachusetts implemented a 2010 data privacy law with exacting requirements for "personal information" of Massachusetts residents in any jurisdiction.[114] Though the requirements are not technology-specific, practitioners have interpreted them to require encryption of data and correspondence containing personal information.[115]

The ABA International Privacy Law Working Group has posted guides to many data privacy laws relevant to attorneys, including the FTC's requirements, the Gramm–Leach–Bliley Act, the Children's Online Privacy Protection Act, the Fair Credit Reporting Act, the Health Insurance Portability and Accountability Act (HIPAA), the EU/US Privacy Safe harbor, and privacy requirements in Australia, Canada, the European Union, Finland, Germany, Greece, Italy, Sweden, and the United Kingdom.[116] In February 2012, the ABA adopted a resolution

---

federal law imposes limits on the ability of OSP administrators to inspect user e-mail, irrespective of the OSP's formal policy. Inspection is limited by the ECPA to purposes 'necessary to the rendition of services' or to the protection of 'rights or property.' Further, even if an OSP administrator lawfully inspects user e-mail within the narrow limits defined by the ECPA, the disclosure of those communications for purposes other than those provided by the statute is prohibited.").

111. Delaware State Bar Ass'n, Comm. on Prof'l Ethics, Op. 2001-2 (2001); Florida State Bar Ass'n, Comm. on Prof'l Ethics, Op. No. 00-4 (2000); Maine Prof'l Ethics Comm'n, Op. 195 (2008); The Supreme Court of Ohio, Board of Commissioners on Grievances and Discipline, Op. No. 99-2 (199); Utah State Bar, Ethics Advisory Op. Comm., Op.No. 00-01 (2000); Virginia Legal Ethics, Op. 1791 (2003); Los Angeles Cnty. Bar Ass'n, Formal Op. No. 514 (2005) ("Lawyers are not required to encrypt e-mail containing confidential client communications because e-mail poses no greater risk of interception and disclosure than regular mail, phones or faxes.").

112. *See* Tom Mighell, *The Cyber-Ethical Criminal Defense Lawyer (Or, How Not to Commit Malpractice with Your Technology)*, 73 TEX. B.J. 540 (2010).

113. *See generally* DANIEL J. SOLOVE ET AL., INFORMATION PRIVACY LAW (2d ed. 2005). Information for practitioners can be found at the ABA website. ABA LEGAL TECHNOLOGY RESOURCE CENTER, http://www.americanbar.org/groups/departments_offices/legal_technology_resources/ (last visited Aug. 25, 2012).

114. Rodney S. Dowell, *Data Privacy Part I: Complying with New Regulations to Keep Confidential Personal Information Protected*, 17 MASS. LAW. J. 6Feb. 2010, at 6.

115. *See* Rodney S. Dowell, *Data Privacy II: Lock It Down*, MASS LAW. J., Mar. 2010, at 8.

116. ABA SECTION OF INTERNATIONAL LAW,http://apps.americanbar.org/intlaw/committees/industries/information_services_technology/privac

that local courts should "consider and respect, as appropriate" foreign data privacy laws in civil litigation.[117] Any attorney dealing with sensitive information should be aware of the large and growing body of data privacy laws.

### *B. State Bar of California, Formal Opinion 2010-179*

In 2010, the State Bar of California issued a thoughtful, generally applicable opinion, alongside local bar associations issuing their own specific opinions.[118] The State Bar of California Formal Opinion 2010-179 is a considered dialogue on the risks of email and other technologies such as wireless networks.[119] This opinion is recognized as the authority on the issues of wireless computing for attorneys.[120] The California Formal Opinion is based on a scenario involving an attorney with a firm-maintained laptop using a public wireless connection, or his own personal wireless connection at his home.

The opinion starts with a warning that technology-based ethics opinions will become outdated, and then examines the issues carefully.[121] The State Bar of California is intentionally opaque about technology, suggesting that it is a fact-specific inquiry that will depend on many factors, and also that it will change.[122] The Opinion outlines six factors for attorneys to consider.[123]

First, the California Opinion weighs the attorney's own ability to "assess the level of security afforded by the technology."[124] These security factors include consideration of how the technology differs from others, whether reasonable precautions may increase the level of security, and limitations on who can access the communications.[125] The Opinion notes that this is an inquiry that requires technical knowledge and finds that attorneys owe clients a "basic understanding of the electronic protections afforded by the technology they use," even

---

y.shtml (last visited Aug. 25, 2012).

117. ABA H.D. Res. 103 (2012).

118. Kristina Horton Flaherty, *Ethical Issues Bedevil Lawyer E-Mail*, CAL. B. J., May 2001, *available at* http://archive.calbar.ca.gov/calbar/2cbj/01may/page16-1.htm.

119. Cal. State Bar Comm. on Prof'l Responsibility & Conduct, Formal Op. No. 2010-179 (2010).

120. Ben Kerschberg, *Your Ethical and Legal Duties When Using Wireless Networks*, FORBES, Dec. 21, 2011, *available at*, http://www.forbes.com/sites/benkerschberg/2011/12/12/your-ethical-and-legal-duties-when-using-wireless-networks/.

121. Cal. State Bar Comm. on Prof'l Responsibility & Conduct, Formal Op. No. 2010-179 at *1 (2010).

122. *See id*.

123. *Id*. at *3–6.

124. *Id*. at *3.

125. *Id*. at *3–4.

seeking outside advice to do so.[126] This technology knowledge is critical to allow the attorney to make an informed decision and consider the technical factors demanded by the Opinion.[127]

The remaining five factors are the legal impact of third-party access, the sensitivity of the information, the possible impact of inadvertent disclosure on privilege or confidentiality, urgency, and the client's instructions.[128]

To address the hypothetical scenario, the committee finds that the attorney can use the firm laptop for confidential information because of the restricted access to appropriate authorized agents at the firm, including other personnel trained in this area. However, the court finds that he should not use his personal wireless network without "appropriate security features." He may need encryption, firewalls, or other security features to use the public network, or "avoid using the public wireless connection entirely," depending on the information's sensitivity.[129] In all situations, the Opinion requires attorneys to inform their clients of the risks of technologies.

The advice to protect confidential information on a public and attorney's own home router is based on illegal, "hacker" interception into systems as well as the easily intercepted unencrypted data transfer.[130] This access is either clearly illegal, such as a hacker stealing information from the router, or questionably legal, such as access by a hotspot owner with clear privacy policies. In either context, the California Bar Association nevertheless finds an ethical duty for attorneys to avoid or mitigate the risk.

The California Opinion shows the danger of technology-specific ethics opinions. The ABA's 1999 opinion's specific combination of privacy policies, technology, and law may collapse when technology changes. In this case, carelessly sending unencrypted email to a public server, which violated no duty in 1999, becomes an unacceptable risk when combined with a new, technical security risk: a public wireless router. Unlike the ABA, the State Bar of California places an explicit duty on attorneys to stay informed about the technologies and to be able to explain risks.

### *C. 2011 ABA Formal Opinion 11-459*

In 2011, the ABA responded to issues with privilege and ethic duties

126. *Id*. at *5.
127. *See id.* at *5.
128. *Id.* at *5–6.
129. *See id*. at *7.
130. *Id*. at *7 n.21.

in employee email and issued Formal Opinion 11-459, warning attorneys to advise clients to avoid workplace email and computers.[131] In this opinion, the ABA carved out a specific exception to its previous 1999 opinion. This Opinion is an excellent start toward security and email and acknowledges serious risks arising from corresponding with clients using their employer's resources. Employees and their attorneys should never assume an expectation of privacy in work email.

Employers have long used email monitoring to monitor everything from work activities to company regulations concerning extracurricular behavior for all levels of employees. A chief executive of Boeing was fired when email showed an affair with a subordinate, as well as language inappropriate under company policy.[132] Many company policies spell out that email belongs to the employer, not the employee.[133] Many employee contracts and user agreements specifically show employees that their email and use of the employer network is not private.[134] A 2002 report to Congress of Fortune 500 companies found that every company stored both business and personal employee email, more than 40% routinely monitored it, and the remaining companies inspected it when needed.[135] Some companies use software to search for keywords and evaluate email.[136]

In recent years, courts have battled through the unsettled issue of workplace email.[137] Some have found very serious waivers associated with employees using workplace email and workplace computers for private communications, while some have maintained privilege despite employer policies. The opinions show a case-by-case inquiry, muddling through privacy issues in email, sometimes deferring to the employer's policies, and sometimes not.

Early opinions favored employers. At the time of the 1999 ABA opinion, employers had been virtually undefeated in courts, obtaining rights to emails and other employee communication. At the time, a commenter in the ABA Journal analogized invasive employer rights to

131. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011).

132. Jared Sandberg, *Monitoring of Workers Is Boss's Right but Why Not Include Top Brass*?, WALL ST. J., May 18, 2005, *available at* http://online.wsj.com/article/0,,SB111636541232736178,00.html.

133. NANCY FLYNN & RANDOLPH KAHN, E-MAIL RULES: A BUSINESS GUIDE TO MANAGING POLICIES, SECURITY AND LEGAL ISSUES FOR E-MAIL AND DIGITAL COMMUNICATION (2003).

134. U.S. GEN. ACCOUNTING OFFICE, EMPLOYEE PRIVACY: COMPUTER-USE MONITORING PRACTICES AND POLICIES OF SELECTED COMPANIES (2002).

135. *Id*. at 6.

136. *Id*. at 7–8.

137. *See generally* Michael Z. Green, *Against Employer Dumpster-Diving for Email*, 64 S.C. L. REV. 323 (2012).

snoop on email to installing a camera in the men's room.[138] Courts consistently found that employee emails were subject to interception and adverse use.

In 1996, a Pennsylvania court found that despite an expectation of privacy in threatening and vulgar emails sent using an employer's email address and network, that interception was not a substantial and highly offensive invasion of privacy.[139] In 1998, an Illinois court upheld a client of Andersen Consulting divulging Andersen's emails sent over the client's mail system to the public via the Wall Street Journal.[140] Two unpublished California cases also recognized the rights of an employer to intercept and use email, even with California's unique privacy laws.[141] By the late 1990s, it seemed employees had no statutory remedy for employer snooping on their email.[142]

Later, some courts did protected employee emails on a case-by-case basis, especially with unclear privacy policies or efforts by employees to maintain privacy. New York courts protected a limited amount of material sent through a personal email address when the employee attempted to remove the material from an employer's laptop,[143] as well as an employee using personal email at work.[144] Massachusetts courts protected well-labeled documents on a company laptop, as well as email sent through a personal email address, even when company policy warned about employee privacy.[145] A District of Columbia District Court even protected a Department of Justice prosecutor who used his work email address for personal, attorney–client communication, based on his ignorance of the Department policies and attempts to delete the mail.[146]

Other cases found sweeping waivers of privilege when employees used company email or company equipment for personal emails. Widely followed cases decided in 2006 and 2007 enforced employers' terms of service and allowed not only interception but adverse use

138. Don J. DeBenedictis, *E-Mail Snoops*, A.B.A. J., Sept. 1990, at 27.

139. Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996).

140. *See* Andersen Consulting LLP v. UOP, 991 F. Supp. 1041 (N.D. Ill. 1998).

141. Peter Schnaitman, Comment, *Building a Community Through Workplace E-mail: The New Privacy Frontier*, 5 MICH. TELECOMM. & TECH. L. REV. 177, 197–201 (1999) (citing Bourke v. Nissan Motor Co., No. B068705 (Cal. Ct.. App. July 26, 1993); Shoars v. Epson, America, Inc., No. SWC 112749 (Cal. Super. Ct. Mar. 26, 1990)).

142. Schnaitman, *supra* note 141, at 216.

143. Curto v. Med. Commc'ns, Inc., No. 03CV6327 (DRH)(MLO), 2007 WL 1452106 (E.D.N.Y. May 15, 2007).

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

145. Fiber Materials Inc. v. Subilia, 974 A.2d 918 (Me. 2009); Nat'l Econ. Research Assocs. v. Evans, 24 Mass. L. Rptr. 436 (Sup. Ct. 2008).

146. *See* Convertino v. U.S. Dept. of Justice, 674 F. Supp. 2d 97 (D.D.C. 2009).

against employees. In *Scott v. Beth Israel Medical Center*,[147] a physician had corresponded with his personal attorney using the hospital's network. The hospital policy stated that all messages were property of the hospital and that no personal use was allowed.[148] The New York trial court found that these policies diminished any expectation of confidentiality, allowing the hospital to use those e-mails in a later suit claiming wrongful termination.[149]

In *Kaufman v. Sungard Investment Systems*, a New Jersey court applied New Jersey privilege law to determine privilege in emails sent on a company email system.[150] In that case, the policy 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.[151]

The company also warned that it "reserves the right to monitor and inspect network or Internet usage and e-mail" and "e-mail may be subject to monitoring, search, or inspection at any time."[152] Under New Jersey law, disclosure to a third party "without coercion and with knowledge of his right or privilege" waives the privilege.[153] The court found that disclosure to an employer by using an employer's email system was deliberate and waived privilege.[154]

In 2011, two cases decided within months of each other reached radically different conclusions about privilege in emails sent by personal attorneys to employer-provided networks. In *Holmes v. Petrovich Development Co.*, an employee used her work email and computer to communicate with her attorney about a work dispute.[155] The court easily found that these emails were not privileged, comparing it to "consulting her attorney in one of [her employer's] conference rooms, in a loud voice, with the door open, yet unreasonably expecting that the conversation overheard by [her employer] would be privileged."[156]

At the same time, in *Stengart v. Loving Care, Inc*., a New Jersey court

147. 847 N.Y.S.2d 436, 438–39 (Sup. Ct. 2007).

148. *Id*. at 439.

149. *Id*. at 441.

150. Kaufman v. SunGard Inv. Sys., No. 05-cv-1236, 2006 WL 1307882 (D.N.J. 2006).

151. *Id*. at *4.

152. *Id*.

153. *Id*. at *3 (citing N.J. STAT. ANN. § 2A:84A-29 (1960)).

154. *Id*. at *4.

155. Holmes v. Petrovich Dev. Co., 119 Cal. Rptr. 3d 878, 886–87 (App. 2011).

156. *Id*. at 896.

found that emails sent with a personal, Internet-based email account from a work terminal remained privileged, where the employer's policy about privacy in such situations is unclear.[157] In that case, an attorney had used a work computer to access a personal, password-protected email service. The court found that the employee was "unsophisticated in the use of computers and did not know that [her employer] could read communications sent on her Yahoo account."[158] Further, the court found an ethical violation with the intercepted messages. These messages were recorded in temporary storage on the laptop's hard drive, in a "cache" folder, without the employee's knowledge.[159] The employer forensically recovered and used their contents claiming they were "left" on the laptop.[160] The court found that the attorneys who discovered these messages violated their ethical duty by not treating them as "inadvertent" disclosures and notifying opposing counsel.[161]

In response to this conflict, the ABA issued two opinions based on the same fact pattern, resembling *Holmes* and *Stengart*. In 2011, the ABA issued Formal Opinions 11-459 and 11-460 to address concerns with client communications and also how to treat recovered documents.[162] The ABA described the status of the law as "evolving" and stated that courts have reached "different conclusions."[163] The formal opinions are based on the same hypothetical situation: a client seeking counsel in an employment dispute, where waiver through use of the employer's resources is clearly problematic.[164] She has a company laptop assigned for her exclusive use.[165] Employees regularly use their laptops for personal email, even though the company has a right of access to any information on the laptop.[166] Opinion 11-459 addresses the issues with the client using her work computer and email address; Opinion 11-460 addresses the duties of the attorney regarding the contents of the laptop, containing privileged information.[167]

Opinion 11-459 takes on the issues of privacy in employee email. Employers regularly require employees to waive privacy rights in employer email and devices. The ABA notes danger when an employer

157. Stengart v. Loving Care Agency, Inc., 990 A.2d 650 (N.J. 2010).

158. *Id*. at 665.

159. *Id*. at 666.

160. *Id*. at 665–66.

161. *Id*. at 666.

162. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011); ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-460 (2011).

163. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011).

164. *Id*. at 1–2.

165. *Id*. at 1.

166. *Id*.

167. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-460 (2011).

can freely view confidential information, as well as the risk of third-party subpoenas for the employer's stored data.[168] The ABA finds that an attorney should assume employers can access all emails sent to a workplace email address, as well as private mail accessed on a workplace device, threatening confidentiality and possibly privilege.[169]

The ABA warns attorneys about employers' restrictive privacy policies, and advises attorneys to assume that employees have contracted away their expectation of privacy in employer emails and devices. Given the risk of access by others and possible waiver of privilege, attorneys should "typically" advise their clients to avoid workplace email and all workplace devices.[170] Appropriate actions include refraining from sending email to a workplace email address, as well as cautioning the client against using the workplace email or a workplace device to communicate, "at least for substantive e-mails with counsel."[171] The ABA's conclusion is for all seasons, all technologies, and all clients. The ABA finds:

> Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice to the client.[172]

Formal Opinion 11-460 settles that Model Rule 4.4, related to inadvertent document disclosure, does not apply in this context. "[A] document is not 'inadvertently sent' when it is retrieved by a third person from a public or private place where it is stored or left."[173] The Opinion does acknowledge that other ethical or evidentiary rules might govern in a particular jurisdiction.[174]

The ABA's scenario contains an obvious conflict, because the employee's dispute is with the party that controls the e-mail. The ABA warns in this context that "even seemingly ministerial communications involving matters such as scheduling can have substantive ramifications."[175] The ABA suggests that in other contexts, risks may

168. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011).

169. *Id*. ("Unless a lawyer has reason to believe otherwise, a lawyer ordinarily should assume that an employer's internal policy allows for access to the employee's e-mails sent to or from a workplace device or system.").

170. *Id*.

171. *Id*.

172. *Id*.

173. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-460 (2011).

174. *Id*.

175. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011).

vary, and that attorney's should advise their clients about the danger of third-party access to these communications.[176]

The Opinion suggests that other contexts could allow third-party access as well, such as a shared family computer in a matrimonial dispute, a borrowed computer, or a public computer, including a library or hotel computer.[177] Though these situations are obviously problematic to privacy, the ABA does not offer specific guidance for these situations. The ABA does not mention any technical solution, such as encryption, in the context of third-party access, nor discuss the attorney's duty to understand technology.

The ABA's newfound concern about privacy policies in employer networks updates the broad assumptions in the 1999 opinion. In 1999, the ABA did not even consider the policies of a "private system," instead worrying about careless misdirection within the system, such as "throughout a law firm."[178] The ABA had previously assumed that messages on a private network would relate to a common entity, because private networks contained only users with a duty to that common entity.[179] Thus, all the users within the firm would have a common duty to the confidences of the firm clients. This assumption about the technology proved to be false. The 2011 opinion showed a world in which the network's common duty fails to match the content of the message, that is a private network message used for unintended purposes.

The 2011 opinion was also forced to address the provider's duty to an individual user's mail. The ABA had only considered this in the context of consumer mail and Internet providers. The ABA had assumed that service providers would have a duty of privacy to their account holders, as AOL did. This presents a situation the 1999 opinion did not contemplate: the provider has no duty of privacy to its user; in fact, it has contracted for the exact opposite.

The ABA also reversed its position on the power of ECPA to protect email users. Adverse access and use of employer email or private mail accessed on an employer's device would be impossible under the ECPA interpretation solidified in the ABA's 1999 Opinion, which claimed that inspection and disclosure were prohibited by federal law "irrespective of the OSP's formal policy."[180] All relevant provisions of ECPA have

176. *Id*.

177. *Id*.

178. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999).

179. *Id*. ("[A]ll members of a firm owe a duty of confidentiality to each of the firm's clients. Further, unintended disclosures to individuals within a client's private e-mail network are unlikely to be harmful to the client.").

180. *Id*.

always contained exceptions for consent, so the OSP's formal policy is critical to decide what access is authorized. Thus, the ABA reconsidered in 2011, finding that the limits were not irrespective of employer's policies. Privacy policies are indeed able to override the federal law the ABA previously trusted.

In 1998, Professor Hricik compared email to a package sent through a commercial service, such as Federal Express, which warns in fine print that FedEx can inspect any package.[181] He claimed that obtaining truly informed consent about authorized access before using FedEx was unreasonable, and compared FedEx's rights to an OSP's "limited right to monitor lawfully e-mail."[182] As time went on, those limits became less limiting as courts found that providers could contract for their right to monitor, assuming policies were clear, at least in the case of employers. The privacy policy can now control that right, removing ECPA's limitations by consent.[183]

The 2011 Formal Opinion is critical because it shows that a user's consent is able to override the law's default privacy limits and to eliminate the general, assumed expectation of privacy. This Opinion destroys generalized conclusions and requires focusing on the policies of the service provider, not the character of the technical specifications, as the most important element to determine user's privacy. Unlike in 1999, this suggests privacy must be determined on a case-by-case basis, and that provider's policies are critical.

181. Hricik, *supra* note 4, at 492. The current FedEx terms are that "[Fedex] may, at our sole discretion, open and inspect any shipment without notice." *FedEx Services Express Terms and Conditions*, FEDEX, http://www.fedex.com/us/service-guide/terms/express-ground/index.html (last visited Sept. 5, 2012). These terms have been upheld to serve a legitimate business interest. United States v. Young, 153 F.3d 1079, 1080–81 (9th Cir. 1998). These terms have also been held to reduce expectation of privacy, at least for a spilled shipment of drugs. United States v. Barry, 673 F.2d 912, 917 (6th Cir. 1982).

182. Hricik, *supra* note 4, at 492.

183. Perhaps one critical distinction is sealing the message. In a confidential FedEx delivery, perhaps even a FedEx delivery to a client's workplace, the envelope is sealed and presumably labeled, as reasonable measures taken to ensure confidentiality. Even in 1998, email was considered "unsealed" and compared to a postcard, which never carries an expectation of privacy. Hricik himself was only able to overcome the postcard analogy with the assumption that ECPA prohibited access and that email ends with storage on the recipient's private computer alone. Both are untrue in the context of modern employee email. Am. Civil Liberties Union v. Reno, 929 F. Supp. 824, 834 (E.D. Pa 1996), *aff'd*, 521 U.S. 844 (1997) ("Unlike postal mail, simple e-mail generally is not 'sealed' or secure, and can be accessed or viewed on intermediate computers between the sender and recipient (unless the message is encrypted)."); Hricik, *supra* note 4, at 461 ("Some say that sending an Internet e-mail is like sending a postcard, not a sealed envelope. Others disagree, stating that 'e-mail is inherently more secure than ordinary mail since it is delivered right to the computer of the recipient.'").

### *D. ABA Commission on Ethics 20/20 Technology and Confidentiality Rule Changes*

After years of preparation, papers, and comments, in February 2012, the ABA Commission on Ethics 20/20 released a final revised draft of the commission's proposals to update rules relevant to technology and confidentiality issues.[184] The relevant proposals included amendments to Model Rule of Professional Conduct 1.1 Competence; Rule 6, Duty of Confidentiality; and Rule 4.4, Respect for the Rights of Third Persons.[185] In August 2012, the ABA passed the amendments to the Model Rules with only small modification.[186]

The most fundamental amendment is to the Rule 1.1, Competence, Comment 6, Maintaining Competence. Previously the comment required attorneys to "keep abreast of changes in law and practice." The amendment adds "including the benefits and risks associated with technology."[187] This mirrors the California requirement that attorneys must be knowledgeable about technology in order to inform clients of risks or obtain consent. The Committee describes this requirement as "some awareness of the basic features of technology" and notes that the amendment "does not impose any new obligations on lawyers."[188]

Rule 1.6, Confidentiality, has a change, adding a section (c): "A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to representation of a client."[189] Adding reasonable security measures for stored electronic data has an intuitive quality that makes one wonder why it was previously relegated to Comment 16 for disclosure by an attorney or his agents, or to Comment 17 for transmissions only. Obviously, it is illegal to break into a law firm and steal documents, but shouldn't an attorney at least lock the door? The Committee describes this rule as needed "in light of the pervasive use of technology to store and transmit confidential client information."[190]

---

184. ABA COMM. ON ETHICS 20/20, FOR COMMENT BY APRIL 2, 2012: FINAL REVISED DRAFTS OF FIRST SET OF COMMISSION PROPOSALS (Feb. 21, 2012).

185. The proposals also address issues in technology use in client development, outsourcing, practice pending admission, and admission by motion. *Id.*

186. ABA COMM. ON ETHICS 20/20, REPORT TO THE HOUSE OF DELEGATES, 105A REVISED (2012), *available at* http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120808_revised_resolution_105a_as_amended.authcheckdam.pdf; Bloomberg BNA, *Ethics 20/20 Rule Changes Approved by ABA Delegates With Little Opposition*, Aug. 15, 2012.

187. ABA COMM. ON ETHICS 20/20, REVISED DRAFT RESOLUTIONS FOR COMMENT: TECHNOLOGY AND CONFIDENTIALITY 5 (Feb. 21, 2012).

188. *Id*. at 15–16.

189. *Id*. at 8.

190. *Id*. at 15.

The Committee describes three scenarios that encourage adoption of Rule 1.6(c): misdirection of e-mail, hackers accessing client data, and employee agents posting confidential information on the Internet. This Rule is intended "to make clear that lawyers have an ethical obligation to make reasonable efforts to prevent these types of disclosures, such as by using reasonably available administrative, technical, and physical safeguards."[191] The Committee declined to offer technology-specific recommendations in the rules, instead outlining general principles.

The Committee adds a lengthy provision to Comment 16.[192] The Comment clarifies that inadvertent or unauthorized disclosure is not a violation if "the lawyer has made reasonable efforts to prevent the access or disclosure." This analysis uses four factors: sensitivity of the information, likelihood of disclosure without security measures, cost of security measures, and the extent to which the safeguards would affect the lawyer's ability to represent clients. However, the Committee leaves the bulk of Comment 17 unchanged. Comment 17 applies to "transmitting a communication" and states that "[t]his duty, however, does not require that the lawyer use special security measures if the method of communication offers a reasonable expectation of privacy."[193]

Comments 16 and 17 add notes that federal and state privacy laws are beyond the scope of the rules, and that lawyers may need to take additional steps while communicating information and after unauthorized access. The Committee added these statements to "remind lawyers that other laws and regulations impose confidentiality-related obligations beyond those that are identified in the Model Rules of Professional Conduct."[194]

Rule 4.4, Respect for Rights of Third Persons, addresses an attorney's duty to notify a sender of inadvertent document disclosure. The

191. *Id*. at 17.

192. *Id*. at 11–12 ("The unauthorized access to, or the inadvertent or unauthorized disclosure of, confidential information does not constitute a violation of paragraph (c) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g. by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forego security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.").

193. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2009).

194. *Id.* at 18.

amendments add "electronically stored information" to the previous "documents."[195] Amendments to Comment 2 defines electronically stored information as "email and other forms of electronically stored information, including embedded data (commonly referred to as 'metadata'), that is subject to being put into readable form." "A document of electronically stored information is inadvertently sent when it is accidentally transmitted to an unintended recipient, such as when a letter is misaddressed or when a document or electronic stored information is accidentally included in discovery."[196] As before, Rule 4.4 requires attorneys to notify the sender, but other requirements will vary. The Committee describes this information as "intentionally sent, but to the wrong person."[197] At passage, the suggestion in Comment 3 was modified to suggest that attorneys may wish to "delete" instead of "return" misdirected email.[198]

The Committee also recommended that the ABA sponsor a centralized website to host the many resources and projects the ABA has undertaken regarding technology in law practice, including data security standards. The ABA has several resources with information on these issues, including the ABA Legal Technology Resource Center. The Committee found that practitioners sought a central location for this information.[199]

The ABA amendments are much-needed amendments to the Model Rules, including a critical provision requiring attorneys to maintain knowledge of technology. The amendments reflect the need to protect electronic communications, just as attorneys would paper documents, and to consider the risks for confidentiality in use of technology.

## III. CONTINUING PRIVACY ISSUES IN EMAIL

Years after the ABA's confident conclusion that the existing law protected privacy in email identically to other means of communication, and that interception was difficult and illegal, the issue of email privacy remains unresolved. Privacy in email has eroded in at least one category, employer mail, and remains in flux generally speaking. Email forces a case-by-case inquiry because email providers can have clear policies about expectations for users, as the ABA acknowledged in 2011. Attorneys should be wary of this uncertainty, of the danger of

195. *Id*. at 13.

196. *Id*.

197. *Id*. at 19 (emphasis omitted).

198. BNA Bloomberg, *supra* n. 186. This suggestion was made by Ellen Flannery, a partner at Covington & Burling.

199. *Id*. at 14.

privacy policy waivers, and of unrelated disclosure to third parties in compliance with other cases.

### *A. No Settled Expectation of Privacy in Email*

The general expectation of privacy in email in Fourth Amendment jurisprudence remains unresolved. Though expectation of privacy is not identical to confidentiality, the concepts are related and courts often rely on Fourth Amendment protections to analyze confidentiality. When "reasonable expectation of privacy" is not settled, neither is privacy for confidential information between attorneys and clients. Statutes allow warrantless searches to email, and the challenge to these statutes in the context of the Fourth Amendment is ongoing.[200] In 2013, Google announced a bold policy that it would require warrants for cloud or email data, though contrary to current law.[201]

Email has found itself at a rough intersection between fundamental search and seizure principles: the generalized, person-based *Katz* inquiry of reasonable expectation of privacy, the "third party" doctrine of *Miller* and significant statutory challenges, with outdated, unclear guidance from Congress. When analyzing expectation of privacy in a Fourth Amendment context, courts follow *Katz*, finding whether individual has a subjective expectation of privacy and whether society would consider that expectation reasonable. In *Katz v. United States*, the Supreme Court changed the dialogue about the Fourth Amendment with a new framework.[202] Instead of focusing on the object searched, the Court turned to the target, developing the "reasonable expectation of privacy test," as developed in Justice Harlan's dissent and subsequent cases. This analysis, now used in all Fourth Amendment inquiry, asks whether a subject has an actual expectation of privacy (subjective prong) and whether society considers it reasonable (objective prong).[203] The subjective prong requires an intent to keep the information private as well as reasonable efforts to maintain privacy.[204]

In *United States v. Miller*, the Court established the third party rule, finding a subject forfeits privacy in information known to and divulged to a third party. Miller contested a subpoena for bank records, which the

200. *See generally* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, U. CHI. LEGAL F. at 121 (2008).

201. David Kravets, *Google Tells Cops to Get Warrants for User E-Mail, Cloud Data*, WIRED, Jan. 23, 2013.

202. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).

203. *Id*.; *see also* Kyllo v. United States, 533 U.S. 27, 33 (2001).

204. *Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

Court found were "revealed to a third party," and thus the Fourth Amendment did not prohibit disclosure to government authorities.[205] "All of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[206] Depending on the facts and the steps taken by the parties, third-party access can also destroy confidentiality—for example, documents that could have been inspected by an accountant.[207]

The conflict of *Katz* and *Miller* is ongoing in this context. Email is technically accessible by third parties, ISPs, yet resists easy classification as information freely given to others. Email also has its own very complicated set of privacy policies and obsolete statutes. This issue is surprisingly unsettled, and is the subject of much commentary and speculation.[208] Today, only one published, circuit court opinion addresses the issue of general privacy expectations in email, over ten years after the ABA confidently established privacy interest in email.[209]

The unlikely hero of email privacy has become Steven Warshak, infomercial peddler of the erectile dysfunction drug "Enzyte" and star of an episode of CNBC's dramatic "American Greed" featuring elaborate financial scams.[210] In 2005, federal agents investigated Warshak's company, Berkeley Premium Nutraceuticals, Inc. As part of that investigation, the government requested email from Warshak's Internet service provider, NuVox, and an email account supplied by that company, as well as email provided by Yahoo for Warshak and others.[211]

Federal agents used an order authorized by ECPA, the Stored Communications Act, 18 U.S.C. § 2703(f), to order NuVox to preserve all incoming and outgoing mail.[212] Warshak accessed his mail by downloading it to his personal computer and deleting it from NuVox's servers; without this order, no copies would exist.[213] The government

205. United States v. Miller, 425 U.S. 435, 442–43 (1976).

206. *Id*. at 442.

207. *See* First Interstate Bank of Or., N.A. v. Nat'l Bank & Trust Co., 127 F.R.D. 186, 189 (D. Or. 1989).

208. *See generally* Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-Mail*, U. CHI. LEGAL F. at 121 (2008).

209. *See* Casey Perry, *U.S. v. Warshak: Will Fourth Amendment Protection Be Delivered to Your Inbox?*, 12 N.C. .J. L. & TECH. 345, 348–49 (2011).

210. *American Greed*, CNBC, http://www.cnbc.com/id/35988285/ (last visited Sept. 5, 2012).

211. Warshak v. United States, 490 F.3d 455, 460 (6th Cir. 2007).

212. Warshak v. United States, 631 F.3d 266, 283 (6th Cir. 2010); 18 U.S.C. § 2703(f) (2009) ("A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.").

213. *Warshak*, 631 F.3d at 283 n.14.

then obtained a subpoena using ECPA, 18 U.S.C. § 2703(d), for disclosure of the information.[214] NuVox was required to surrender 27,000 emails with no warrant.[215]

In 2008, Warshak went to trial with several others on a 112-count indictment for the fraudulent activities of the company. Warshak was convicted of most counts and sentenced to 25 years imprisonment, and fines and forfeitures of more than half a million dollars.[216] The government used many of Warshak's own documents, including his emails, but did not use any privileged material.[217] During the trial, Warshak's motion to exclude the emails was denied.[218] The Sixth Circuit had found a privacy interest in the emails before the trial, but the opinion was vacated for being unripe.[219] After the trial ended, Warshak again appealed the government's warrantless seizure of his emails to the Sixth Circuit.

The Sixth Circuit's opinion is thoughtful and aware of its novel precedent, written by the scholarly and thoughtful Justice Boggs.[220] The Sixth Circuit used broad strokes in an overview of general Fourth Amendment principles, with no real precedent in this area. It started with a *Katz* inquiry as to whether Warshak had an expectation of privacy in his email and whether that expectation was reasonable.[221] The court found that Warshak "plainly manifested an expectation that his emails would be shielded from outside scrutiny" based on their content.[222] The court found the emails were "often sensitive and sometimes damning."[223] The court found this expectation on the content alone, and did not consider any technological protections for this expectation. The court did not even mention, for example, password protections on the account.

---

214. *Warshak*, 490 F.3d at 460; 18 U.S.C. § 2703(d) ("A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.").

215. *Warshak*, 631 F.3d at 282.

216. *Id*. at 281–82.

217. Brief for Plaintiff-Appellee United States, United States v. Warshak, 631 F.3d 266 (2010) Nos. 08-3997, 08-4085, 08-4087, 08-4212, 08-4429, 09-3176, 2009 WL 3392997, at *33–34.

218. *Warshak*, 631 F.3d at 281.

219. Warshak v. United States, 532 F.3d 521 (6th Cir. 2008).

220. *Warshak*, 631 F.3d at 274. The case had two briefs by amici. Brief for Professors of Electronic Privacy Law and Internet Law as Amici Curiae Supporting Appellee, United States v. Warshak, 631 F.3d 266 (2010) (No. 06-4092), 2006 WL 4670944 [hereinafter Brief for Professors]; Brief for Electronic Frontier Foundation et al as Amici Curiae Supporting the Appellee, United States v. Warshak, 631 F.3d 266 (2010) (No. 06-4092), 2006 WL 4670945.

221. *Warshak*, 631 F.3d at 285.

222. *Id*. at 284.

223. *Id*.

For the second prong of the *Katz* inquiry, the court was forced to decide whether society would find a privacy interest in email as reasonable. The court was well aware of the impact of this decision, calling it "of grave import and enduring consequence, given the prominent role that email has assumed in modern communication."[224] The court starts by noting that the Fourth Amendment must keep pace with technology and that surveillance through technology requires Fourth Amendment safeguards.

The court analogized email to both phone conversations and sealed letters, both with well-established reasonable expectations of privacy.[225] The court finds similar sensitive communication, similar technological risk, and historically found that the email search is protected by the Fourth Amendment.[226] Though the court found the search was a violation of the Fourth Amendment, it did not exclude the evidence because agents relied on ECPA's statutory authorization for a warrantless search in good faith.[227]

The court distinguished Warshak's emails from *Miller* based on their content. Unlike in Miller's banking requests, in the ordinary course of business, Warshak sent "confidential" communications.[228] The court also explained that NuVox was the "intermediary, not the intended recipient of the emails."[229] In this case, NuVox provided Warshak's Internet connection as well as his email address,[230] as opposed to an ISP which only provides Internet access. Both Warshak's and Nuvox's actions made NuVox more of an intermediary than an endpoint. If Warshak had not deleted mail from the server, or if NuVox had always preserved emails, NuVox would have been a storage facility for Warshak. In either situation, labeling the provider as simply an intermediary would have been more challenging.

The court used strong quotes from other sources about recognizing privacy in email: recognizing the desire to "eliminate the strangely disparate treatment of mailed and telephonic communications on the one hand and electronic communications on the other"; that "a search of [an individual's] personal e-mail account" would be just as intrusive as "a wiretap on his home phone line"; and that "[t]he privacy interests in

224. *Id*.

225. *Id*. at 285–87.

226. *Id*. at 287–88.

227. *Id*. at 292.

228. *Id*. at 288.

229. *Id*. (citing Bellia & Freiwald, *supra* note 200, at 165 ("[W]e view the best analogy for this scenario as the cases in which a third party carries, transports, or stores property for another. In those cases, as in the stored e-mail case, the customer grants access to the ISP because it is essential to the customer's interests.")).

230. Warshak v. United States, 490 F.3d 455, 460 (6th Cir. 2007).

[mail and e-mail] are identical."[231] The opinion, however, was significantly tempered.

The court was forced to address NuVox's policies, which stated that "NuVox *may* access and use individual Subscriber information in the operation of the Service and as necessary to protect the Service."[232] The court also noted Nuvox's practice that it did not keep copies of emails once downloaded onto account-holders' computers.[233] The court avoided Hricik's Federal Express analogy altogether and instead compared this to the policy of a hotel. Even though staff often enter hotel rooms, and have the ability to enter a room, guests have a reasonable expectation of privacy.[234] The court found that "some degree of routine access is hardly dispositive."[235]

The court found that Warshak was protected by NuVox's policies that it would access emails only under limited circumstances.[236] Recognizing the importance of NuVox's policy to the expectation of privacy, the court stated, "[W]e are unwilling to hold that a subscriber agreement will never be broad enough to snuff out a reasonable expectation of privacy."[237] The court cited to a decision in which an employee had no right of privacy in files on his office computer, and another in which a university had much less restrictive privacy policy.[238] An intention by an ISP to "audit, inspect, and monitor" might negate a user's expectation.[239] Thus, the court engaged in a subtle, case-specific inquiry, suggesting that the privacy policy is critical to this distinction.

Of course, the court here is speaking about a reasonable expectation of privacy from government searches and from the government compelling the ISP to turn over information, not from the ISP itself. The court cited experts in the field, Professors Patricia Bellia and Susan Freiwald, concerning the role of the ISP as intermediary in this transaction. They compare the ISP to a case in which "a third party carries, transports, or stores property for another."[240] This is satisfying in the context of warrantless government searches, but perhaps not for

231. *Warshak*, 631 F.3d at 286 (citing Bellia & Friewald, *supra* note 200, at 135; City of Ontario v. Quon, 130 S.Ct 2619, 2631 (2010); United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008)).

232. *Id*. at 287.

233. *Id*. at 287 n.16.

234. *Id*. at 286–87.

235. *Id*. at 287.

236. *Id*.

237. *Id*. (emphasis omitted).

238. *Id*. (citing Warshak v. United States, 490 F.3d 455, 472–73 (6th Cir. 2007)).

239. *Id*.

240. *Id*. at 288 (citing Bellia & Freiwald, *supra* note 200, at 165). Professors Bellia and Freiwald also argued in the professors' amicus brief before the court. *See* Brief for Professors of Electronic Privacy Law and Internet Law as Amici Curiae Supporting Appellee, United States v. Warshak, 631 F.3d 266 (2010) No. 06-4092, 2006 WL 4670944.

confidentiality. In the Article cited by the court, Bellia and Freiwald continue and explain the expectation of privacy with respect to the ISP itself:

> To be clear, users may lack a reasonable expectation of privacy with regard *to those third party intermediaries* who discover information in the course of exercising their rightful access to the users' packages, storage lockers, rental properties, or stored e-mail accounts. That implies that if the third party *chooses* to disclose the information so discovered to the government without requiring a warrant, the user cannot complain. When the user assumed the risk that the intermediary would discover incriminating information or property in the course of its business, she also assumed the risk that the intermediary would choose to turn that information over to the government. If the user mistakenly trusted the intermediary to protect its incriminating information, there is no reason for the Fourth Amendment to protect that misplaced trust.[241]

This grave warning, from the stalwart defenders of email privacy, shows that ISPs are the weakest link in email privacy. Bellia and Freiwald suggest a service provider less protective than NuVox which may turn over information without being compelled by the government. This brings to mind the long line of cases in which criminals mistrusted third parties who then turned over communications to the government.[242] Service providers may also be that unreliable third party which turns over information to law enforcement. Bellia and Freiwald's article suggest that a cooperative ISP would have the right to voluntarily turn over information, at least under the Fourth Amendment jurisprudence, but the government would still need to obtain a warrant to compel disclosure.

In their brief to the court, professor amici, including Bellia and Freiwald, argued:

> Terms of service set forth the ways in which a service provider may need to protect its system and business from fraud, hacking, unauthorized use, and the like. Whatever rights the service provider might have to access communications to perform those functions, those rights do not give the service provider the right to disclose communications for the fundamentally different purpose of assisting law enforcement investigations of unrelated crimes . . . .
>
> Notwithstanding its terms of service, a service provider's right to protect its own property does not release the Government from the constraints of the Constitution. Any third party that holds property on behalf of

241. Bellia & Freiwald, supra note 200, at 166–67.

242. *See* United States v. White, 401 U.S. 745, 752 (1971) (holding government agent can reveal contents of conversations); Hoffa v. United States, 385 U.S. 293, 302 (1966) (holding incriminating statements to an informant required misplaced confidence in the informant).

> another, such as a storage company, may retain the right to inspect units to prevent damage that might occur to its property or that of other customers. The fact that the storage company has or exercises such a right, however, says nothing about the relationship between the storage customer and government agents.[243]

Though these policies were not at issue in these cases, providers often do have such provisions, allowing ISPs to voluntarily disclose under certain conditions to third parties, including the government. Service provider policies usually explicate reasons ISPs can disclose communications, including criminal activity or emergencies, in part to be able to comply with mandatory reporting laws.[244] Service providers are required by law, for example, to report known child pornography, and are subject to fines for failure to do so.[245] In this case, NuVox did not invoke such a provision, but ISP policies regularly allow for disclosure to others in certain situations.[246]

Because NuVox did not assert it, the brief did not consider whether violation of terms of service, such as committing a crime through NuVox's service, would forfeit Warshak's right of privacy with respect to both the ISP and the government.[247] This broader issue, though not at issue in this case, could have widespread consequences for Fourth Amendment law and in confidentiality.

Bellia and Freiwald's general deference to ISP policies regarding privacy is consistent with recognizing ISP rights, established by policies and contracts. The Sixth Circuit's ruling in *Warshak* can only be compatible with the line of cases establishing employer's rights if the user can waive his rights by agreeing to the policy. The distinction between NuVox, which resisted accessing and disclosing communications, and an employer, who intentionally stored and used communications adversely, is the provider's policies.

In the context of confidentiality, *Warshak* may offer false reassurance for attorneys, as the landmark case offering a headline-worthy "reasonable expectation of privacy" in email, just as Professor Hrick's 1998 article did. Comment 17 to Model Rule 1.6 allows attorneys to communicate with no security precautions if the medium "offers a

243. Brief for Professors, *supra* note 220, at 8.

244. Even in 1997, AOL allowed disclosure "to comply with applicable law" and "in emergencies when AOL, Inc. believe[d] that physical safety [wa]s at risk." AOL, REVISED AMERICA ONLINE PRIVACY POLICY (1997), *available at* http://epic.org/privacy/consumer/aol_revised_policy.html.

245. 18 U.S.C. § 2258A (2008).

246. NuVox's current Privacy Policy does contain a term that they may disclose information "to identify, contact, or bring legal action against someone who may be violating our Acceptable Use Policy." NUVOX, NUVOX'S PRIVACY POLICY, *available at* http://home.nuvox.net/privacy.html.

247. Brief for Professors, *supra* note 220, at 8 n.12.

reasonable expectation of privacy."[248] At least for the Sixth Circuit, *Warshak's* Fourth Amendment holding shows a reasonable expectation of privacy from the government alone, not third party ISPs. ISP access, as a private party, does not implicate the Fourth Amendment. Confidentiality is concerned with more than just government access; attorneys must consider access by non-governmental third parties, including ISPs. For an expectation of privacy from ISPs, users must consult their policies.

### *B. Read Your Privacy Policy Lately?*

Perhaps the persistent elephant in the room in the court opinions, bar association opinions, academic discussion, or any discussion about email privacy at all is the case-specific inquiry of the provider's policies: user agreements, terms of service, usage policies, and privacy policies.[249] Even if there might be an expectation of privacy, that expectation can be contracted away by the user. In all cases, reasonable expectation of privacy will depend on the provider's policies.

Professor Hricik believed users can rely on the privacy of their email by contract and that attorneys should inspect the privacy policy of their service provider.[250] This policy should set some rights to mail which Hricick assumes will further protect users' privacy, relying on the then-robust AOL privacy policy. Professor Hricik treated his email, while waiting to be downloaded to its final resting place at his computer, as property in bailment, subject to a contract.[251] The ABA agreed, citing ISP policies as a key factor in maintaining privacy within a network, limiting even legal access, without citing a single privacy policy.[252] This assumption about privacy policies is obsolete, as acknowledged by the ABA in 2011.

---

248. MODEL RULES OF PROF'L CONDUCT R. 1.6 cmt. 17 (2009).

249. Mike McNerney, *Warshak: A Test Case for the Intersection of Law Enforcement and Cyber Security*, 2010 U. ILL. J. L. TECH & POL'Y 345, 351 (2010) ("Practically speaking, adjudicating cases such as these on a case-by-case basis isn't very satisfying. Outside of basic subscriber information, it seems hard to believe that the Fourth Amendment should only apply in so far as an ISP user agreement.").

250. Hricik & Fallingham, *supra* note 6, at 282–83.

251. Hricik, *supra* note 4, at 490 ("Assuming the provider is according e-mail content reasonable security from its own employees, e-mail should be deemed to be secure because it is similar to files stored at an off-site storage facility.").

252. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 99-413 (1999) ("The denial of external access ordinarily is ensured by the use of password-protected mailboxes or encryption. The threat to confidentiality caused by the potential inspection of users' e-mail by OSP system administrators who must access the e-mail for administrative and compliance purposes is overcome by the adoption of a formal policy that narrowly restricts the bases on which system administrators and OSP agents are permitted to examine user e-mail.").

Privacy policies are now longer, meaner, and more vague since Hricik's articles. The assumed privacy protections are now hazy or even hostile to privacy interests, and the assumed practices to keep email confidential will obviously depend on the privacy policy. Today's user should be very concerned about the case-specific policies relating to email. Privacy policies, such as employer policies discussed above, may offer no privacy at all.

Professor Hricik confidently relied on the AOL Privacy Policy, as an example of a service provider dedicated to privacy. This policy has been updated several times in the past years, always acting retroactively. In 1997, AOL's privacy policy promised to delete mail within twenty-five to thirty days, and explicitly promised confidentiality.[253] While that 1997 privacy policy is reassuring, the 2012 AOL privacy policy is hazier, and much, much longer. It states, in part:

> The contents of your online communications, as well as other information about you as an AOL Network user, may be accessed and disclosed in response: to lawful governmental requests or legal process (for example, a court order, search warrant or subpoena), in other circumstances in which AOL has a good faith belief that a crime has been or is being committed by an AOL user, that an emergency exists that poses a threat to the safety of you or another person, when necessary either to protect the rights or property of AOL, or for us to render the service you have requested.[254]

AOL, like all providers, can also monitor for violation of the Terms of Service:

> To prevent violations and enforce this TOS and remediate any violations, we can take any technical, legal, and other actions that we deem, in our sole discretion, necessary and appropriate without notice to you.

The AOL Terms of Service require users to comply with many vague requirements, including "[c]omply with applicable laws and regulations and not participate in, facilitate, or further illegal activities" and not use sexually explicit speech.[255] AOL maintains its general focus on user

253. Hricik, *supra* note 4, at 489.

254. *AOL Privacy Policy*, AOL (Sept. 7, 2012, 10:51 AM), http://privacy.aol.com/privacy-policy/.

255. *Terms of Service*, AOL (Sept 7, 2012, 10:53 AM), http://legal.aol.com/terms-of-service/full-terms ("To use our Services, you must: a. Comply with applicable laws and regulations and not participate in, facilitate, or further illegal activities; b. Immediately notify us if you learn of a security breach or other illegal activity on the Services; c. Protect your username and password; d. Not post content that contains explicit or graphic descriptions or accounts of sexual acts or is threatening, abusive, harassing, defamatory, libelous, deceptive, fraudulent, invasive of another's privacy, or tortious; e. Not engage in an activity that is harmful to us or our customers, advertisers, affiliates, vendors, or anyone else; f. Not use any automated process to access or use the Services or any process, whether automated or manual, to capture data or content from any Service for any reason; and g. Not

privacy and limits access and disclosure to business purposes, legal processes, and issues such as furtherance of crime or an emergency. Of course, this dedication to the mail's privacy assumes the mail complies with the terms of service.

The issue of whether a user forfeits an expectation of privacy when he violates terms of service is unclear.[256] Certainly, an employee violating a policy of no personal use is considered in cases involving personal use of employer mail.[257] AOL does not describe violation of terms of service as an enumerated category subject to disclosure, but AOL does reserve the right to "any technical, legal, and other actions" for violations of terms of service.[258] Whereas the previous policy was black and white, the new AOL policy is tinged with gray.

ISPs may offer no privacy at all. Beyond employer networks, there are many large networks in which users may contract away their expectation of privacy. Public sector emails are subject to become public documents, as we all have seen with constant, high-profile disclosures of inappropriate emails as public documents. In 2007, D. Kyle Sampson, then chief of staff for Attorney General Alberto Gonzalez, resigned after emails became public showing plans to remove certain U.S. Attorneys.[259] Harris County, Texas District Attorney Chuck Rosenthal also resigned when his emails showed an improper relationships and racially derogatory content.[260]

Emails held by public entities, including public universities, are at risk to become public documents under open records and freedom of information laws.[261] These laws generally exempt privileged information, but not the broader category of confidential information. Further, the entity reviewing for exceptions may not have the same interests as the communicating parties. Thus, when a public entity, including a university or law clinic, discloses documents, its privilege review can be very challenging, based on the reviewer's attorney status and relationship to the attorney–client communications.[262]

---

use any Service or any process to damage, disable, impair, or otherwise attack our Services or the networks connected to the Services.").

256. The amici brief in Warshak did not address this issue. Brief for Professors, *supra* note 220, at 8 n.12.

257. *See* Scott v. Beth Israel Med. Ctr. Inc. 847 N.Y.S.2d 436, 439–40 (Sup. Ct. 2007).

258. *Terms of Service*, *supra* note 255.

259. Joshua Poje, *Sanctions Just a Click Away: Email's Ethical Pitfall*s, 7 PUB. SERVANT 1, 5 (2009).

260. *Id*.

261. *See* Gregory C. Sisk & Nicholas Halbur, *A Ticking Time Bomb? University Data Privacy Policies and Attorney–Client Confidentiality in Law School Settings*, UTAH L. REV. 1277, 1305 (2010).

262. *Id*. at 1305, n.114. Privilege may be also able to override a clearly written privacy policy when the work is internal, serving the public entity itself. In *City of Reno*, a city labor relations employee authorized a memorandum emailed to the chief deputy city attorney, two deputy city

Public university legal clinics have a uniquely difficult burden with freedom of information laws. Rutgers School of Law, a public New Jersey university, recently challenged its responsibilities under the New Jersey Open Public Records Act.[263] Rutgers argued that the disclosures would put the clinics at a disadvantage, compared to private legal services, because their files may be subject to disclosure.[264] In 2010, a New Jersey Court found the law applied to the Rutgers legal clinic as to any other state-funded program, as written, with the "specifically delineated twenty-one exemptions."[265] The New Jersey law provides exemptions for information that must be produced, including attorney–client privilege, and specific types of information, such as social security numbers and driver's license numbers.[266] These exceptions would likely not apply to many documents actually requested in the case: time records for attorneys and staff, payment records, minutes of meetings, and broad categories of documents.[267] Public disclosures, such as those required in New Jersey, can be troubling for attorneys' ethical standards and for maintaining client confidence. Professor Gregory Sisk claims these disclosures "would likely prevent clinics at a public university form continuing to represent clients."[268] Rutgers' Acceptable Use Policy was amended after the decision to add a privacy exception for information subject to the New Jersey Open Public Records Act.[269]

In 2010, Professor Gregory Sisk and Nicolas Halbur published a thoughtful discussion of university privacy policies within the context of clinical work by law school faculty members.[270] They found that universities often have counterintuitive policies, restrictive for institutions thought to encourage a protected space for free thought and speech.[271] Most universities provide some privacy for users, requiring exigency or some judgment call to prompt inspection of a user's information.[272] However, a "significant minority . . . begin from the

attorneys, and an assistant city manager. The privacy policy stated that city employees had "no expectation of privacy" and that email "may be classified as public documents." In this case, the Court found the email memorandum confidential, and thus privileged, despite the privacy policy. City of Reno v. Reno Police Protective Ass'n, 59 P. 3d 1212, 1218–19 (Nev. 2002).

263. Sussex Commons Assocs., LLC v. Rutgers, 6 A.3d 983 (N.J. 2010).

264. *Id*. at 989–90.

265. *Id*. at 993.

266. N.J. STAT. ANN. § 47:1A-1.1 (2005).

267. *Rutgers*, 6 A.3d at 986–87.

268. Sisk & Halbur, *supra* note 261, at n.114.

269. Rutgers, the State University of New Jersey, Acceptable Use Policy for Computing and Information Technology Resources, at C(2) (2010), http://policies.rutgers.edu/PDF/Section70/70.1.1-current.pdf.

270. Sisk & Halbur, *supra* note 261, at 1278.

271. *Id*.

272. *Id*. at 1295–96.

stated premise that users of computer systems are not guaranteed or should not expect privacy."[273] This departure from traditional expectations in email, or even as compared to commercial email service providers, is critical.

Kansas State University's privacy policy states that all users, including employees and students, have "no expectation of privacy" in anything on the university network.[274] Villanova School of Law, a private school, agrees, stating, "[w]hile the Law School attempts to keep email messages secure, privacy is not guaranteed and users should have no general expectation of privacy in email messages sent through the Law School system."[275] These policies are problematic for attorney's expectation of privacy and contradict the basic principles of a university's unique setting, valuing privacy and academic freedom.[276]

An attorney inspecting these terms of service should be cautious about sending sensitive information, encrypted or not, to a network with no reasonable expectation of privacy. These network owners, like employer–owners of private networks providing email to employees, could not be more clear about the terms of their proprietary networks, and there is no room to claim a reasonable expectation of privacy with such a clear policy explaining otherwise. These policies are a grave risk for a client's private information as well as an attorney's reputation and ethical standards.

The Villanova School of Law policy mirrors the less private undergraduate policy, attached to Villanova's assignment of university-affiliated Gmail accounts, which appear to be from @villanova.edu, but are served in part by Google.[277] "While the University will make every attempt to keep email messages secure, privacy is not guaranteed and users should have no general expectation of privacy in email messages sent through a University Email Account or through a Gmail Account."[278] Villanova University is an early adopter of Google's "Google Apps," which includes cloud based services targeted at

273. *Id*. at 1296.

274. Kansas State University, *Electronic Mail Policy*, *in* POLICIES AND PROCEDURES MANUAL Ch. 3455 § .020 (2010), *available a*t http://www.k-state.edu/policies/ppm/3455.html ("To the greatest extent possible in a public setting individuals' privacy should be preserved. However, there is no expectation of privacy or confidentiality for documents and messages stored on University-owned equipment.").

275. *Web and Email Policies*, VILLANOVA UNIV. SCH. OF LAW (Sept. 7, 2012, 12:09 PM),Email, http://www.law.villanova.edu/current%20students/technology%20services/web%20and%20email%20policies.aspx.

276. Sisk & Halbur, *supra* note 261, at 1301.

277. *Villanova Gmail*, VILLANOVA UNIV. (Sept. 7, 2012 12:14 PM), http://www1.villanova.edu/villanova/unit/accounts/email/vugmail.html.

278. *Email Policy*, VILLANOVA UNIV. (Sept. 7, 2012, 12:16 PM), http://www1.villanova.edu/villanova/unit/about/policies/emailpolicy.html.

universities.[279] In this case, Villanova's privacy policy clearly conflicts with Google's generally privacy-focused policies, though carrying Google's branding. In such a case, users need to be aware of their overlapping and possibly conflicting privacy policies, which may require investigation.

Others, such as University of North Carolina, may appear to hold the same intent, but more vaguely. "There is no guarantee of privacy or confidentiality for data stored or for messages stored or sent on University-owned equipment."[280] This "no guarantee" could be a statement about technical vulnerability; we all know that nothing is guaranteed in technology. However, this acceptance of limited rights may also be considered a waiver. An attorney should carefully consider staking his professional ethics on such vague policies.

Most university policies contain exceptions that allow university administrators, such a provost or a vice president, the ability to inspect emails.[281] Yale's policy allows access with approval by the provost and appropriate dean for faculty, or the appropriate dean for students.[282] Professor Hricik's current institution, Mercer University, allows even more access:

> [S]ystems support staff, systems operators, supervisors, and designated University officials may access information resources to locate and protect business information, maintain system and network resources, ensure system and network security, provide technical support, comply with legal requirements, or administer Mercer University policies.[283]

Many universities have similar policies that allow high-ranking, non-attorney administrator access, with or without some form of cause.[284]

In the context of attorney–client email, non-lawyer access is problematic for confidentiality as well as for an attorney's ethics obligations under Model Rule 5.3, which requires attorneys to supervise all non-attorney access.[285] Attorneys have an ethical duty to make sure their systems staff are appropriately trained to maintain confidences and appropriately bound to keep those confidences.[286] These university

279. *See E-Mail*, VILLANOVA UNIV. (Sept. 7, 2012, 12:17 PM), http://www1.villanova.edu/villanova/unit/accounts/email.html.

280. University of North Carolina at Chapel Hill, *Policy on the Privacy of Electronic Information*, *in* POLICIES AND PROCEDURES (2002), *available at* http://www.unc.edu/campus/policies/elec_info.html.

281. Sisk & Halbur, *supra* note 261, at 1297–98.

282. YALE UNIV. POLICY 1607 (Yale Univ. 2011).

283. *Information Technology Access and Use Policy*, in POLICIES AND PROCEDURES MANUAL (Mercer Univ. 2004).

284. *See* Sisk & Halbur, *supra* note 261, at 1302–04.

285. *See id*. at 1303–04.

286. *Id*. at 1307; *see also* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 95-398 (1995).

terms allow a stranger to the attorney–client relationship access to privileged material, without the required attorney supervision.[287]

This relationship is challenging, because although the university appears to be a private, secure network, it is not subject to the same security and confidentiality risks that attorneys must consider when establishing networks handling confidential information.[288] Unlike users of the law firm's network, the university does not have a common relationship to the clients. Instead, the information is at risk by an authorized, unrelated party with no relationship whatsoever to the attorney–client relationship. Well-crafted university policies would require, at a minimum, a review for privileged information by an attorney with no conflict of interest.[289]

Students also have a problematic relationship with their university privacy policies. In *Reichert v. Elizabethtown College*, a Pennsylvania district court easily reached the conclusion that a university's inspection of a student's email in the context of an expulsion dispute was not a violation of privacy, ECPA, SCA, or state wiretap laws.[290] The court did not even examine the college's privacy policy, as the student's email was provided by the college.[291] This court treated the student much more like an employee than a paying customer.

Even for providers generally focused on privacy, it is important for attorneys to read the terms. Gmail's recently revised Google Privacy Policy adds changes an attorney should consider:

> We may use collect information about the services that you use and how you use them, like when you visit a website that uses our advertising services . . . .
>
> We may share aggregated non-personally identifiable information publicly and with our partners.
>
> We will share personal information with companies, organizations or individuals outside of Google if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to . . . protect against harm to the rights, property, or safety of Google, our users or the public as required or permitted by live . . . Google processes personal information on our servers in many countries and around the world. We may process your personal information on a server located outside the country where you live.[292]

287. Sisk & Halbur, *supra* note 261, at 1304.

288. *Id*. at 1303–05.

289. *Id*.

290. Reichert v. Elizabethtown Coll., No. 10-2248, 2011 WL 3438318 (E.D. Pa. Aug. 5, 2011).

291. *Id*. at *4–5.

292. *Privacy Policy*, GOOGLE (Sept. 7, 2012, 1:28 PM), http://www.google.com/privacy.html.

This Privacy Policy is upfront and clear, and shows Google's dedication to privacy in most circumstances, but it adds another wrinkle: explicit acknowledgement that confidential information might be leaving the country where another jurisdiction's laws apply.

Google's transparency is refreshing compared to general silence about the location of user data, but should raise questions about other providers' terms for storage and for processing private information. As off-site storage, or "cloud computing" increases, these jurisdictional issues will become more pervasive and thus more important for attorneys to consider. Other services may store information offshore as well, but may not even notify users. Many users, and thus their attorneys, may be completely ignorant of where their data is being stored. Villanova's Gmail-serviced accounts may be on servers in Pennsylvania, they may be on Google servers in California, or they may be somewhere else completely. Privilege is a location-specific inquiry, often dependent on state-specific standards of confidentiality and ethics, and the location of this information could be critical, especially with providers less focused on privacy than Google.

Other privacy policies have a host of terms that may or may not support a finding of privacy once a user has violated the terms. These policies can contain all sorts of terms. For example, Yale requires users to decrypt encrypted messages on request and staff must have approval to send any encrypted mail.[293] Yale prohibits everything from "chain letters" to "reckless distribution of unwanted mail" to "harassing or threatening uses" as violations of the network's terms.[294]

AOL and Google attempt to be straightforward and transparent about their policies. However, other providers' policies can be flung across several documents. Yale has over a dozen documents on the main "Policies, Procedures, and Guidance" page for all kinds of technology policies as well as unlinked, isolated documents, such as Procedure 1607 PR.01, which contains specific technical guidelines to allow Yale to decrypt all encrypted mail.[295] Simply finding a provider's complete policies could be quite an endeavor, if possible at all.

Just these few examples of privacy policies raise serious questions about what kind of expectations are reasonable for users. Attorneys should look for clear explanations of when the ISP can access information itself, and when it can disclose it to others. It may be unreasonable for some users to have any expectation of privacy at all, or to be able to understand the terms at all. The ABA draws great comfort

293. *Endorsed Encryption Implementation Procedure*, *in* YALE UNIVERSITY POLICY 1607 PR.01 (Yale Univ. 2010) [hereinafter *Encryption*].

294. YALE UNIV. POLICY, *supra* note 282.

295. *Encryption*, *supra* note 293.

from privacy policies, which could protect messages, but could just as easily contract away privacy.

### *C. The Enron Problem—Discovery & Disclosure*

Attorneys sending information to third party servers just don't know where they will end up. Hackers aside, there are many venues for legal disclosure at the hands of a third party. The Federal Energy Resource Commission (FERC) confiscated Enron's Microsoft Outlook database as part of its investigation into Enron's illegal activities. It then took an unprecedented step to comply with its FOIA responsibilities. On March 23, 2003, the FERC published 1.6 million emails, calendar entries, and tasks, sent to and by 176 former and current Enron executives and employees.[296] Importantly, not everyone in the corpus was an Enron employee, such as Kenneth Lay's daughter Elizabeth, or Enron's outside counsel. These senders lost privacy interests by sending *to* Enron's network.

The set of data, later known as "The Enron Corpus," was originally released in full, until unwitting participants objected to releasing private mail.[297] The corpus was taken offline, and FERC used filters for terms like divorce or social security numbers, removing parts of the corpus assumed to be the most private mail, though not necessarily the most embarrassing.[298] FERC claimed to respond to claims of privacy and privilege in subsequent redaction of thousands of emails, now missing from the final version and not used when analyzing the data.[299]

The Enron Corpus, freely available at the FERC website,[300] still contains email to in-house counsel and outside attorneys, many with their sad disclaimers uselessly attached from Vinson & Elkins,[301]

---

296. FEDERAL ENERGY REGULATION COMMISSION,FINAL REPORT ON PRICE MANIPULATION IN WESTERN MARKETS (2003).

297. *See generally InBoxer Case Study of Enron Email Reveals Email Liability Remains a Significant Risk; Audiotreive CEO Roger Matus Presents 'Monsters in Your Mailbox' at Inbox East 2004 Conference*, BUSINESS WIRE, Nov. 17, 2004, http://www.businesswire.com/news/home/20041117005035/en/InBoxer-Case-Study-Enron-Email-Reveals-Email.

298. *See generally E-mails Can Pose Risks to Big Corporations*, ECON. TIMES, Nov. 21, 2004, http://articles.economictimes.indiatimes.com/2004-11-21/news/27380997_1_e-mails-roger-matus-enron-corp; *The Enron E-mail Corpus*, SGI (Sept. 7, 2012, 2:53 PM), http://sgi.nu/enron/index.php.

299. Interview with Mark Hershfield, Federal Energy Regulatory Commission, Apr. 4, 2006.

300. *Information Released in Enron Investigation*, FED. ENERGY REGULATORY COMM'N, http://www.ferc.gov/industries/electric/indus-act/wec/enron/info-release.asp.

301. *Id.* (browse to *Enron Corpus* website; follow "Enron E-mail" hyperlink; select "Enron E-mail" and then click the "Open" button) ("CONFIDENTIALITY NOTICE . . . The information in this e-mail may be confidential and/or privileged. This e-mail is intended to be reviewed by only the individual or organization named above. If you are not the intended recipient or an authorized representative of the intended recipient, you are hereby notified that any review, dissemination or

Skadden Arps,[302] and international firms.[303] The redacted version of the Enron Corpus contains the word 35,621 uses of the word confidential,[304]

This very public email release shows that lawyers simply don't know where email will end up. For Enron's outside counsel, their confidential email ended up next to Elizabeth Lay's embarrassing comments about weddings, crunched by spam software vendors, pawed through by journalists and gawkers worldwide, and run in academic computer labs from Berkeley to MIT for projects from mail pattern visualization to social networking.[305] The Enron Corpus is an extreme example of compromised privacy, but legally, it is absolutely sound, a choice in the discretion of the investigating agency dealing with now-public documents.

Email will be critical in other kinds of investigations, and documents containing every aspect of personal and professional lives existing on a mail server could be turned over.[306] Future corpuses could be disclosed in many other contexts, such as the White House's voluntary release of Solyndra emails from inside and outside the White House.[307] Sarbanes–Oxley requires retention of many kinds of documents for public

---

copying of this e-mail and its attachments, if any, or the information contained herein is prohibited. If you have received this e-mail in error, please immediately notify the sender by return e-mail and delete this e-mail from your system. Thank You.").

302. *Id.* ("This e-mail, and any attachments thereto, is intended only for use by the addressee(s) named herein and may contain legally privileged and/or confidential information. If you are not the intended recipient of this e-mail, you are hereby notified that any dissemination, distribution or copying of this e-mail, and any attachments thereto, is strictly prohibited. If you have received this e-mail in error, please immediately notify me at (212) 735-3000 and permanently delete the original and any copy of any e-mail and any printout thereof. Further information about the firm, a list of the Partners and their professional qualifications will be provided upon request.").

303. *Id.* ("This e-mail is sent by or on behalf of Linklaters, 10/F Alexandra House, Chater Road, Hong Kong. A list of the firm's principals will be provided to the recipient(s) of this e-mail upon request. This statement is made in compliance with the Law Society of Hong Kong's Practice Direction on the Format of Electronic Communications. This message is confidential. It may also be privileged or otherwise protected by work product immunity or other legal rules. If you have received it by mistake please let us know by reply and then delete it from your system; you should not copy the message or disclose its contents to anyone.").

304. Neil Cooke et al., *IP Protection: Detecting Email Based Breaches of Confidence*, *in* IEEE THIRD INTERNATIONAL SYMPOSIUM ON INFORMATION ASSURANCE AND SECURITY (2007).

305. Ryan Singel, *Science Puts Enron E-Mail to Use*, WIRED NEWS Jan. 30, 2006, http://www.wired.com/science/discoveries/news/2006/01/70100?currentPage=all.

306. Seward, *supra* note 1, at 44 ("Prof. Arthur R. Miller of Harvard was quoted as saying: 'Today, as computers document almost every aspect of our clients' professional and personal lives, electronic discovery becomes essential in every type of legal case.' Miller, a pioneer of early cyber law, made that observation several years ago, and indeed the reality of that statement shall be felt on Dec. 1, 2006, when the new proposed changes to the Federal Rules of Civil Procedure (FRCP) on electronic discovery become law.").

307. *See* Neela Banerjee & Matea Gold, *Obama Fundraiser Took Active Interest in Solyndra Loan, E-mails Show*, L.A. TIMES Oct. 8, 2011, http://articles.latimes.com/2011/oct/08/business/la-fi-solyndra-white-house-20111008.

companies, including emails for long periods of time.[308] Attorneys must request that documents produced to the SEC in an SEC investigation be treated as confidential, or the emails are also subject to FOIA requests.[309] A third party responding to such an inquiry may not even know the material is privileged, or care to spend resources defending privilege in an unrelated matter because an unrelated attorney was careless about the destination of his mail.

Email on third-party servers is also at risk for disclosure in unrelated civil matters,[310] as the ABA warned in 2011.[311] After December 2006, the Federal Rules of Civil Procedure expanded electronic discovery. The amendments changed Rule 26(b)(2)(B)–(c) for electronic discovery requests.[312] All "reasonably accessible" data must be provided absent a showing of "good cause."[313] If privileged information is on a third-party server, that third-party, with no duty to the attorney or the client, may be more concerned about its production requirement than potential privilege in an unrelated case. When the information is on a third-party server, it may be impossible for an attorney to defend confidential or privileged information. Disclosure of unrelated material, or a "document dump," may even be strategic.[314] This scenario is problematic for privacy and for privilege, especially given jurisdictional and case-by-case interpretations of waiver.

When email is on a third-party server, both sender and recipient risk disclosure of confidential information and privilege waiver through unrelated disclosure. When the entire server is released, the confidential material is in another's hands or even on the official record, like the Enron Corpus.

## IV. FINDING SOLUTIONS

"[I]t is not asking too much to insist that if a client wishes to preserve the privilege . . . he must take some affirmative steps to preserve

308. Wiliam R. Baker III & Michele D. Johnson, *Defending a Broker Dealer in SEC Investigations after Dodd–Frank*, 1914 PLI CORP. 1019, 1038–39 (2011).

309. *Id*. at 1040.

310. Jonathan Rose, Note, *E-Mail Security Risks: Taking Hacks at the Attorney Client Privilege*, 23 RUTGERS COMPUTER & TECH. L.J. 179, 205 (1997).

311. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 11-459 (2011) ("[O]ther third parties may be able to obtain access to an employee's electronic communications by issuing a subpoena to the employer.").

312. Daniel B. Garrie et al., *Hiding the Inaccessible Truth: Amending the Federal Rules to Accommodate Electronic Discovery*, 25 REV. LITIG. 115 (2006).

313. *Id.*

314. Sharon D. Nelson & John W. Simek, *Data Dumps: The Bane of E-Discovery*, 71 OR. ST. B. BULL 36, 36 (2011).

confidentiality."[315] Every ethics opinion, court case, and academic recognizes that an attorney must use his judgment, and that there are situations when an attorney needs to use caution. Technology-based solutions may be the best practice available and part of reasonable measures to preserve confidentiality.

### *A. Technology-Based Solutions*

In networked systems, no one security measure can offer security, and no network can have perfect security.[316] I discuss one method of technological protection for e-mail, encryption, as only part of a larger plan of best practices.[317] However, all encryption systems can theoretically be broken or can be implemented incorrectly.[318] Thus, I speak about encryption as a best practice only, not as failsafe protection.

Encryption guards the contents of an email from any third party, including an intercepting party or a third party accessing the stored messages. Thus, a copy of encrypted email in the hands of a third party, even a user's ISP, is useless. Public key cryptography uses pairs of keys, with one widely distributed "public key" that is not secret and corresponding "private key" that only its owner holds.[319] Users can use the public key to send messages that only the private key can read, and the private key sends messages that only the private key owner can send. Users can exchange their public keys and transmit using public keys in otherwise insecure environments, but use private keys to decrypt.[320]

Email encryption on a mail client can be more difficult to use than, say, a secure webpage. In 1999, a study evaluated naïve users' use of a new email encryption system for Macintosh computers.[321] Of the twelve participants, four were able to send properly sealed mail, and

315. *In re* Horowitz, 482 F.2d 72, 82 (2d Cir. 1973).

316. TANSU ALPCAN & TAMER BAŞAR, NETWORK SECURITY: A DECISION AND GAMER-THEORETIC APPROACH 6–7 (2011) ("Networks are man-made systems. Since the system engineersare human beings who make mistakes, future networks will have vulnerabilities in some form, no matter how carefully they are designed. As long as there are people who would benefit from exploiting vulnerabilities for selfish reasons, there will always be security threats and attacks.").

317. For articles on additional security measures, see the thorough technical descriptions in the articles cited *supra* Note 8.

318. STEVE BURNETT AND STEPHEN PAYNE, RSA SECURITY'S OFFICIAL GUIDE TO CRYPTOGRAPHY 13 (2001) ("All crypto can be broken, and, more importantly, if it's implemented incorrectly, it adds no real security.").

319. A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49, 51 (1996).

320. *Id*. at 51–52.

321. Alma Whitten & J.D. Tygar, *Why Johnny Can't Encrpyt: A Usability Evaluation of PGP 5.0*, *in* SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE (L. Cranor et al. eds. 2005).

only one could complete all the tasks the authors consider minimal encryption procedures.[322] This level of failure posed a serious risk to the entire system, in the authors' view.[323]

Since that time, major mail clients have all embedded encryption support.[324] These programs have increased usability with simpler interfaces, automatic unsealing, and better error messages. Many of the failures in the study, such as sending a message without the appropriate keypair, are impossible in many modern applications. In a 2005 study repeating the 1999 study, most of the fourteen lay participants were able to use Microsoft Outlook's encryption features functionally.[325]

As with all new technologies, lawyers can be trained to adapt. In part, thanks to HIPAA, encryption solutions for email are now commercially available for small business networks, and even for services like Gmail.[326] Today, implementing email encryption is not the barrier it once was.

### *B. Technology-Based Solutions as Reasonable Measures*

Encryption may be a part of best practices for protecting a message from a third party. Even if encryption is not failsafe, encryption is a good way for attorneys to use technology to clearly explicate their expectation of privacy in sensitive data. Encryption may be an actual barrier to interceptors, legal or otherwise. Encryption is also a clear label of who is authorized to read a confidential communication.

Common sense tells all attorneys that there is some information that probably just should not be in email, or some that is sensitive enough to require special effort. For example, law firms dealing with information such as pending mergers know to have a "healthy paranoia" about this highly sensitive information.[327] Health professionals and finance

322. Simson L. Garfinkel & Robert C. Miller, *Johnny 2: A User Test of Key Continuity Management With S/MIME and Outlook Express*, SYMPOSIUM ON USABLE PRIVACY AND SECURITY 22(2005), *available at* http://cups.cs.cmu.edu/soups/2005/program.html ("In our experience, most e-mail users are not aware of the fact that a message can be intentionally and maliciously modified as it moves through a computer network or waits for delivery on a mail server. Although we did not specifically ask our users if they realized this possibility, only one (S39) of the users in the study raised this possibility in either the 'thinking out loud' or in the follow-up interviews. That user was so paralyzed by the notion that a malicious attacker might be modifying the e-mail messages she was receiving that she was unable to complete the majority of the experiment.").

323. Whitten & Tygar, *supra* note 321, at 3 ("It is well known the security of a networked computer is only as strong as its weakest component. If a cracker can exploit a single error, the game is up.").

324. Garfinkel & Miller, *supra* note 322, at 2.

325. *Id*. at 11.

326. *See, e.g.*, PENANGO, www.penango.com (last visited Sept. 7, 2012).

327. Michael A. Riley & Sophia Pearson, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, BLOOMBERG, Jan 31, 2012, http://www.bloomberg.com/news/2012-01-31/china-based-

professionals face similar issues with highly confidential information. Health professionals have a great deal of experience implementing these systems after health care privacy laws, mainly HIPAA, which, while not technology-specific, has far greater restrictions than legal standards.[328]

Common sense also tells attorneys that information in danger of harmful interception should be protected, whether that interception is legal or not. "Even if interception is illegal, if it is easy to intercept messages, the law is of cold comfort to clients and counsel."[329] This situation might be true for divorce documents accessed on a shared computer, the public wireless router at the coffee shop, or other situations where email might be subject to adverse interception, legally or illegally.

Technical solutions may work. Today's encryption takes significant resources to break.[330] Technologists predict that in a matter of years, routine matters may use virtually unbreakable encryption.[331] Even if the law or the privacy policy may not protect your communication, encryption may. Even a legally authorized snooper may technically fail at attempts to intercept messages.

Encryption is also a very clear label about expectations of privacy. Encryption may be insufficient in the Fourth Amendment context to legally protect in the context of law enforcement decrypting a message already accessed.[332] However, in the context of confidential attorney–client communications, encryption is a clear message that an attorney has made efforts to conceal the communication. In the context of confidentiality, encryption easily analogizes to whispering in a courtroom hall to prevent others from overhearing the messages. This effort may be meaningless to a Fourth Amendment inquiry, but does show efforts to maintain confidentiality between attorney and client.

Like opening a sealed FedEx package, decrypting an encrypted email requires affirmative action to violate what has been sealed, in spite of its labels of intended recipients. This action may change the ethical

---

hackers-target-law-firms.html.

328. Sarah S. Mir, *HIPAA Privacy Rule: Maintaining the Confidentiality of Medical Records, Part 2*, 13 J. HEALTH CARE COMPLIANCE 35 (2011); Bryan Bergeron, MD, *Where is HIPAA Taking Physician Practices?*, 7 MEDSCAPE GENERAL MEDICINE 65 (2005).

329. Hricik & Fallingham, *supra* note 6, at 299.

330. Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 503 (2001) ("Because encryption keys are in most cases impossible to guess—trying to guess a single key could occupy a supercomputer for millions of years—encryption offers Internet users a degree of privacy in Internet communications that remains unequaled in the physical world.").

331. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 866 (2004).

332. *See* Kerr, *supra* note 331, at 513 ("The courts have not yet faced a direct Fourth Amendment challenge to the decryption of encrypted Internet communications.").

requirements for inadvertent communications, and may show that the mail was not intended for third-party consumption. In ABA Opinion 11-460, the ABA refused to protect unencrypted emails abandoned on an employer's system as inadvertent disclosures, but encrypted emails carry their own clear message about confidentiality. An attorney encountering encrypted data would face a challenging technical and ethical dilemma.

Technology-based solutions will change over time, and will solve only current issues, but they will remain part of best practices to address some security issues. Informed attorneys need to be vigilant about learning about new risks and finding security measures that work with new technologies.

## V. CONCLUSION

Before jotting off a quick email, attorneys need to consider the risks of email technology with their clients. Privacy expectations in email now depend on case-specific variables. Attorneys must be aware that these expectations may vary depending on local data privacy laws, privacy policies, and the devices used to access information. Model rules now require attorneys to be aware of the risks of the technology they are using and to educate themselves about technology. Using email for confidential or privileged communication requires an attorney's judgment, along with the client's informed consent.

Attorneys need to discuss email's risks with clients to mutually create a solution for that client's needs. Obviously, security needs will vary, but even the most benign content, such a scheduling email sent to an employee's email, may be devastating to a client. Before an attorney can make such a judgment call, he needs to understand the risks involved and discuss them with his client. Clients must work with their attorneys to decide what precautions are appropriate, as it will be the client filing the grievance.

Attorney and client levels of sophistication may vary; some clients may demand security measures or have their own policies for securing data.[333] Some law firms have the best security measures in the world and the personnel and training to enforce it. Unsophisticated clients and smaller practices may be less equipped to handle evolving technology. Attorneys need to educate themselves about the risks in email and consider their security policies and whether they know if their policies truly safeguard client's confidential information.[334] Attorneys should

333. Martha Neil, *Corporate Clients Should Ask Specific Questions About Law Firm Security, Experts Say*, ABA J. Feb. 21, http://www.abajournal.com/news/article/corporate_clients_must_ponder/.

334. Poje, *supra* note 259, at 5.

consider policies about encryption and also about acceptable email use. When using third-party email services, attorneys should consider privacy policies and what types of data are appropriate to send to those systems.

Most importantly, attorneys must be able to educate their clients about the risks of technology they choose to use, including the risks of using third-party services to do so. When an attorney or his firm is unable to understand the risks, or if the burden of this education is too severe, email may not be the proper medium to communicate with clients. Technology-based ethics opinions can never be the solution for long, and it is dangerous to rely on their assurances. In a world with a battery of data privacy laws, evolving ethical guidance, and lengthy privacy policies, an attorney may wish to err on the side of caution, instead of risking his professional license on technology he does not understand.