Brooklyn Law Review

Volume 66
Issue 2
The Second Circuit Review: 1999 - 2000 Term

Article 4

12-1-2000

What Would Learned Hand Do? Adapting to Technological Change and Protecting the Attorney-Client Privilege on the Internet

Joseph W. Wood

WHAT WOULD LEARNED HAND DO?: ADAPTING TO TECHNOLOGICAL CHANGE AND PROTECTING THE ATTORNEY-CLIENT PRIVILEGE ON THE INTERNET*

Joseph W. Rand†

INTRODUCTION

Technological change invariably poses unique challenges to lawyers and judges confronting its often jarring effects. Technical evolution puts pressure on our prevailing legal doctrine (since the new processes or systems create novel, complicated problems) and also on lawyers as they adopt new technology into their practices.[1] For example, the unprecedented explosion of electronic mail or "e-mail," the most popular application on the Internet, has spawned myriad legal problems crossing the doctrinal spectrum, from the privacy concerns implicated by the review of e-mail by employers in the workplace to the evidentiary issues relating to admission and authentication.[2]

---

† Instructor of Law, Brooklyn Law School. J.S.M., Stanford Law School; J.D. Georgetown University Law Center; B.A., Georgetown University. I would like to thank my Brooklyn Law School colleagues Ted Janger and Claire Kelly for their help with earlier drafts; Carey Heckman, Christopher Corey, and Joshua Masur for their shared insights during the development of this Article; and Brooklyn Law School student Ilysa Ivler for her research and technical assistance. I also thank the Brooklyn Law School summer research program and extend my deepest appreciation to the editorial staff at the *Brooklyn Law Review* for its patience and editorial assistance. Finally, I dedicate this Article to the late Honorable Frank X. Altimari of the United States Court of Appeals for the Second Circuit, for whom I was privileged to clerk from 1992 through 1994 and who often discussed his great admiration for his predecessor, Judge Billings Learned Hand.

[1] *See* Lawrence P. Wilkins, *Introduction: The Ability of the Current Legal Framework to Address Advances in Technology*, 33 IND. L. REV. 1, 1 (1999) (identifying two contexts in which inquiries of technological change arise: the "adoption and use of technology in non-legal endeavors which enable new human capabilities," and the "adoption and use of technology by lawyers, judges, and others working in and with the law").

[2] *See, e.g.*, Laurie Thomas Lee, *Watch Your E-Mail! Employee E-Mail Monitoring and Privacy Law in the Age of the "Electronic Sweatshop,"* 28 J. MARSHALL L.

But the ubiquity of e-mail has also challenged lawyers integrating the new technology into their practices, principally spurring an animated debate about the propriety of using e-mail for confidential communications with clients without violating the attorney-client privilege.[3]

And it is not just e-mail that raises these concerns regarding confidentiality. With the advent of online document repositories, cellular phones, handheld wireless computers, and instant messaging, lawyers have all sorts of new and exciting ways in which they can inadvertently breach their clients' confidences. While these new technologies perform wonders for uninterrupted, perpetual attorney-client communication, they come with risks not only to the personal lives of lawyers—whose marriages and other relationships may not survive yet another technological innovation that allows them to work evenings, weekends, and vacations—but also of exposure of sensitive attorney-client confidences. Lawyers learned long ago not to chat about their cases in elevators or in crowded restaurants, and a series of decisions within the Second Circuit have taught them to take proper precautions in their document production procedures lest they, say, inadvertently include an internal confidential memorandum as an exhibit to a motion.[4] But protecting a privilege that is now so easily violated at the mis-touch of a button is difficult, and even more bewildering is the uncertainty as to the precautions that should be taken by the diligent and fashionably-wired attorney in using these new

---

REV. 139, 139-40 (1994) (discussing rights of employees to privacy in their email); Andrew Jablon, Note, *"God Mail": Authentication and Admissibility of Electronic Mail in Federal Courts*, 34 AM. CRIM. L. REV. 1387, 1387-89 (1997) (discussing evidentiary issues pertaining to e-mail).

[3] *Compare* David Hricik, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-Mail*, 11 GEO. J. LEGAL ETHICS 459, 506 (1998) (arguing against a bright-line standard requiring encrypted e-mail) *with* Joshua M. Masur, Comment, *Safety in Numbers: Revisiting the Risks to Client Confidences and Attorney-Client Privilege Posed by Internet Electronic Mail*, 14 BERKELEY TECH. L.J. 1117, 1158 (1999) (arguing that unencrypted e-mail is subject to interception).

[4] *See* Local 851 of the Int'l Bhd. of Teamsters v. Kuehne & Nagel Air Freight, Inc., 36 F. Supp. 2d. 127, 132-35 (E.D.N.Y. 1998) (finding that counsel's attaching a privileged letter to a court filing, which had the same date and letterhead as intended letter, waived privilege where counsel failed to take reasonable precautions by failing to label the letter as confidential, to employ a procedure for separating confidential communications, and to adequately review documents before they left the office).

communication technologies.

In the last five years, the American Bar Association (the "ABA") and many state ethics boards have adopted a position that sending confidential information through e-mail is no more a violation of the attorney-client privilege than making a telephone call or sending a facsimile, and that attorneys need not take measures to secure their communications through encryption or other protective technologies.[5] This consensus, though, has developed without even one definitive court ruling—indeed, a court has never considered the issue of whether confidential e-mail communications are protected by the attorney-client privilege.[6] Moreover, the consensus developed at a time when the alternative to allowing privileged communications through e-mail was to either bar such communications altogether, which was not a particularly popular choice among lawyers enamored of the ease and simplicity of the medium, or to allow the use of e-mail only if encrypted, which was similarly unpopular because of the complexity and cost of encryption programs at the time. Encryption technology protects the contents of the e-mail, preventing anyone but the intended recipient from reading it, but the technology of encryption in the late 1990s seriously lagged behind e-mail technology, undermining the ease and simplicity that was e-mail's appeal.

Several problems exist, though, with the position that e-mail communication does not endanger the attorney-client privilege. First, the fundamental assumptions underlying the ABA's oft-cited opinion that e-mail is a secure-enough medium[7] are technologically dubious and represent a reliance on an inappropriate analogy between e-mail and land-line telephone calls.[8] The safety of e-mail communications is overstated, and attorneys who entrust sensitive material to the medium are unnecessarily risking inadvertent disclosure. Second,

---

[5] *See* ABA Comm. on Ethics and Prof'l Responsibility, Formal Op. 99-413, at Intro. (1999), *available at* http://www.abanet.org/cpr/fo99-413.html [hereinafter "ABA Opinion"]; *see also infra* Part II.B.

[6] *See, e.g.*, Michael R. Arkfeld, *E-Mail—Revisiting Security Issues*, 37-Sep. ARIZ. ATT'Y 12, 13 (2000) ("No one yet knows whether or not courts will determine that sending an email message over the internet waives the attorney-client privilege.")

[7] ABA Opinion, *supra* note 5, at § C.4.

[8] *See infra* Part II.C.3.

this permissive standard could become a precedent for the new generation of Internet applications that allow for attorney-client communication, particularly with regard to shared online documents and repositories. Lawyers are now enlisting the services of online document repositories to enable lawyers to share databases and working drafts from distant offices,[9] and lawyers are also creating "extranets," self-contained web-like environments shared by attorneys and their clients, to provide a common working space in which to exchange correspondence and share documents.[10] Essentially, the concern is that lawyers, under competitive pressure to ensure the kind of immediate contact clients come to expect, will disregard security concerns, assuming that Internet media is inherently safe because the most visible Internet medium of e-mail has been declared secure.

In this uncertain state of affairs, lawyers face the challenge of determining the appropriate set of precautions they should take for protecting the attorney-client privilege in these new communications media. Unfortunately, few courts have established guidelines for protecting privilege when implementing new technologies, requiring that we turn to other doctrinal areas in which courts have established principles for adapting to technological change. In this inquiry, on the fortieth anniversary of his passing, we can turn to the guidance of Judge Learned Hand, who famously articulated principles for setting a reasonable standard of care in implementing new technologies in two landmark tort cases.[11] The cases, *The T.J. Hooper v. Northern Barge Corporation*[12] and *United States v. Carroll Towing Co.*,[13] together establish what I will call Judge

---

[9] *See infra* Part III.A.1.

[10] *Id.*

[11] Billings Learned Hand, who passed away in 1961 at the age of eighty-nine, is not only one of the greatest judges to sit on the Second Circuit Court of Appeals, but is often "numbered among a small group of truly great American judges of the twentieth century." *See* GERALD GUNTHER, LEARNED HAND: THE MAN AND THE JUDGE xv (1994). Judge Richard A. Posner, in a review of Gunther's biography of Judge Hand, found that characterization to be somewhat understated, recognizing that many consider Judge Hand to be "the third-greatest judge in the history of the United States, after [Oliver Wendell] Holmes and John Marshall." Richard A. Posner, *Book Review: The Learned Hand Biography and the Question of Judicial Greatness*, 104 YALE L. J. 511, 511 (1994).

[12] 60 F.2d 737 (2d Cir. 1932).

[13] 159 F.2d 169 (2d Cir. 1947).

Hand's principles of technological integration: (1) reliance on custom is no defense for a failure to adapt feasible and applicable new technologies and (2) whether to integrate these new technologies into practice depends on their costs versus the severity and probability of injury. These principles were conceived in negligence cases, but they nonetheless provide wisdom for examining whether attorneys should take precautions when transmitting confidential client information through the Internet. Essentially, lawyers should consider that their failure to integrate available new technologies of encryption into protecting the attorney-client privilege will not necessarily be mitigated by their reliance on prevailing custom that those new technologies are not necessary; rather, in considering whether it is feasible to adopt the new technologies, they should consider the cost of integrating them in light of the probability of accidental disclosure and the harm that would result.

Indeed, these principles nicely enhance the test that courts within the Second Circuit have established for evaluating whether an attorney has inadvertently waived her client's privilege, which depends primarily on the appropriateness of the precautions set up to protect against disclosure.[14] But because no court has had to consider the types of precautions necessary for new technologies, and the precedents are mostly document productions cases that are not especially analogous, Judge Hand's principles provide the most effective guidance for determining whether lawyers should be charged with keeping up with the state of the art.

The thesis of this Article is that in considering the level of precautions necessary for transmitting information through the new Internet technologies, lawyers applying these principles of technological integration will find that the state of the art requires implementing viable encryption software, for e-mail as well as other online document transmissions. At the very least, I submit that attorneys should pay careful attention to security protocols when adapting new technologies into their practices, especially where the technologies are complex and can rapidly

---

[14] *See* SEC v. Cassano, 189 F.R.D. 83, 85 (S.D.N.Y. 1999) (identifying factors including level of precautions taken to protect privilege, scope of disclosure, time taken to rectify error, and the overriding interests of justice). *See infra* Part III.B.

change. Part I of this Article explores the dynamic of technological change, and establishes a four-factor analysis for evaluating new technologies and how they might impact the prevailing legal doctrine. Part II applies these principles to e-mail, discussing how e-mail and encryption work, explaining the consensus that developed regarding e-mail security and the attorney-client privilege, and showing how that consensus misunderstands the dynamic of technological change. Finally, Part III examines applicable attorney-client jurisprudence within the Second Circuit and explains how Judge Hand's principles can guide attorneys through difficult and complex choices.

I. EXAMINING TECHNOLOGICAL CHANGE: A FOUR-PART MODEL

An examination of the legal effect of a technological change requires an understanding that "technology" is an ongoing, dynamic system. Physical tools and materials are the corporeal representations of technology, but more important for our purposes are the processes of technology: the science, attitudes, design, and activities that revolve around technological change.[15]

One of the ways in which technological change affects society, of course, is through its impact on law.[16] The extent to which law is reactionary is debatable, insofar as some question whether technology actually spurs a true legal paradigm shift—the development of completely new legal doctrine, theory, or regulatory regimes—or simple evolution in existing legal

---

[15] One commentator noted:

> In some sense, technology is the quintessential human activity. Humanity's ability to craft tools is an important aspect of what distinguishes us from the cows, pigs, cockroaches, and the rest. We are able to think, abstract, and use tools to shape our environment. When we talk about technology in the broadest sense, this is what we are talking about. In more practical terms, technology is the products, processes, devices, systems, and networks that we use to help us individually and collectively pursue our goals and our dreams.

Christopher T. Hill, *The Public Dimension of Technological Change: Impact on the Media, the Citizenry, and Governments—A U.S. Perspective*, 25 CAN.-U.S. L.J. 153, 153 (1999).

[16] *See, e.g.*, Wilkins, *supra* note 1, at 1 (addressing "how legal work can be done using state-of-the-art technology and whether adjustments must be made in the legal system to accommodate the changes that technology enables").

rules to adapt to new factual complexities.[17] The argument that technology foments revolutionary legal change (so-called "law-forcing") posits that technology changes the material nature of our existence, undermining established legal settlements and thereby stimulating changes in the laws that govern how we live.[18] For example, there were few laws protecting workers until the growth of industrial manufacturing; indeed, the law did not even reflect an understanding of an individual laborer as a category needing particular protection. Similarly, the growth of the telecommunications industry required an enormous regulatory apparatus that changed the way in which the state interacted with media. Commentators now see the same dynamic developing with the growth of the Internet, which spawns new issues regarding property in cyberspace and individual privacy rights, and in such technological advancements as the human genome project or cloning that might change societal views of personal identity:[19]

> But the old ways of doing, teaching, and thinking about law are fundamentally obsolete. Nary a legal doctrine or jurisprudence will survive intact the present ferment. The information revolution underway will change law as nothing in our experience or understanding has. It took a millennium to develop a sophisticated common law regime, one based on rights, property, and regulation. It may take less than a decade for that regime to unravel, as core concepts lose meaning . . . . The advent of the Internet has already pressed many existing rules to the breaking point; more are surely to follow.[20]

Some argue, though, that technology merely spurs new rules within an existing legal paradigm.[21] Even though technologi-

---

[17] *Compare* Frank Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996) (arguing against the idea that the Internet will compel creation of new law) *with* Lawrence Lessig, *The Law Of The Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 501-03 (1999) (arguing that Internet technology will create new challenges for legal doctrine).

[18] Alan Heinrich et al., *At the Crossroads of Law and Technology*, 33 LOY. L.A. L. REV. 1035, 1037 (2000).

[19] *Id.* at 1036-41 (discussing various forms of new technologies and their capacity to challenge established legal settlements).

[20] *Id.* at 1036.

[21] *See* Monroe E. Price & John F. Duffy, *Technological Change and Doctrinal Persistence: Telecommunications Reform in Congress and the Court*, 97 COLUM. L. REV. 976, 1015 (1997) ("Change in technology, even massive change, is not a sufficient reason for changes in judicial doctrine. As we have seen, there is confusion over which elements of technological change affect which elements of categorical approach.").

cal change sometimes requires adjustments in specific regulatory laws affecting use of that technology, it does not shake the basic underpinnings of society. For example, the invention of the wire tap necessitated laws for its practical use and limitations, but it was still governed within the existing constitutional framework.[22] Indeed, Professors Price and Duffy have argued, in the context of the Supreme Court's modern telecommunications jurisprudence, that judges and lawyers use the excuse of technological change as a subterfuge for "reopening old legal schisms or reorganizing economic relationships for reasons only tangentially concerned with technological advancements."[23] When we examine the effects of technological change on law, then, we have to be mindful of whether we are talking about a radical, revolutionary shift or simply a shiny new box containing the same old legal paradigm.[24]

In examining the nature of a technological change, it is helpful to create a model for the analysis, breaking the dynamic down and examining four characteristics of technological change in isolation: (1) the complexity of the technology, (2) the rate of speed at which it develops, (3) how deeply it penetrates into the society, and (4) how much it challenges the established societal and legal analogical status quo. The extent to which a technology will challenge established legal settlements is based on a combination of those conditions: a new technology that is complex, that changes rapidly, that penetrates deep into the

---

[22] As W.G. Sumner noted, in a different context, "stateways cannot change folkways." W.G. Sumner, *Folkways* (1907), *in* John Morison, *How to Change Things with Rules*, *in* STEVEN LIVINGSTONE & JOHN MORISON, LAW, SOCIETY AND CHANGE 5 (1990) (explaining that government is generally responsive to changing social mores and evolving technologies, not that it is a cause of social change). Curtis E. A. Karnow, in his book about computer technology and the law, framed the idea this way:

> [T]he problem becomes one of assaying the ability of the legal system to deal with new issues posed in the realm of human interaction by the development of technology . . . . [But] [w]ith respect to some problems the resolution, if one is at hand, may simply be a matter of applying existing principles of law to the issue posed by the new technology.

CURTIS E.A. KARNOW, FUTURE CODES: ESSAYS IN ADVANCED COMPUTER TECHNOLOGY AND THE LAW 12-13 (1997).

[23] Price & Duffy, *supra* note 21, at 980.

[24] Of course, law is also sometimes a spur for creating new technology. This is called "technology-forcing," a situation in which lawyers, such as regulatory agencies, establish standards that cannot be met with current technology. Heinrich et al., *supra* note 18, at 1036.

culture, and that is unique and radical is going to pose the most difficult problems for law and society.

A. *Complexity*

In any examination of new technologies, we have to ensure that we have a full understanding of the technology and its societal effects. This means not just understanding the technical specifications of the technology, but also its place in society. This can pose particular challenges in that much of modern technology is baffling, especially with regard to computers in general and the Internet specifically. Most of us understand the rudimentary workings of, for example, an automobile, even though we might not be able to diagnose the cause of smoke coming out of our engines as we sit on the side of the road. But how the entirety of digital communications can be reduced to a series of "1's" and "0's" escapes most of us, and even those with the basic skills to surf the web or even build a web page have little grasp of the technical intricacies of the machines sitting on our desks. We need, though, to know such things if we are to assess the effect of technological change because that examination greatly depends on our ability to recognize the properties and limitations of the technology. The more complicated the technology—and the Internet is an extremely complicated technology—the more difficult this task.

This issue has particular efficacy when we are discussing the types of precautions a particular user must take in implementing the new technology.[25] In making that kind of judgment, we need to understand how people interact with the technology, what their legal expectations for it are. "[U]ser understandings and expectations of the capabilities of local area networks, for example, will directly affect users' beliefs on the privacy and security of their data, whether a user is truly anonymous, and so on."[26] Again, the more complicated the technology, the more difficult it is for users to come to consensus about these expectations and the more difficult it is for us

---

[25] As Karnow noted, "The law delights in tests that ask whether a defendant took 'reasonable precautions' under all the circumstances to ensure something was done or avoided," a calculation that depends entirely on the "widely different levels of knowledge about the technology." KARNOW, *supra* note 22, at 8-9.

[26] KARNOW, *supra* note 22, at 9-11.

to assess the legal effect.

B. *Velocity*

This characteristic refers to the need to be aware of the pace of technological change, which can quickly render established legal settlements obsolete, and the evenness of that change (i.e., whether it evolves in fits and starts or more gradually). A quickly evolving technology is going to pose special challenges to the legal system, which is inherently bound to a slow, reactive rhythm.[27] Most of the systemic reaction to a changing technology will not even involve formal legal actors such as the legislature or the courts. Rather, most disputes arising from new technologies will be resolved in private settlements, not public litigations. The formal systemic reaction is always going to be delayed, given that it takes time for technological change to give rise to an unresolvable dispute between parties, requiring public judicial or legislative resolution.[28] This is, of course, arguably as it should be, since systemically we prefer that most disputes result in private settlements and that legislatures and courts should only get involved as necessary when the concerns have gained sufficient visibility and universality.[29] We do not generally want courts and legisla-

---

[27] KARNOW, *supra* note 22, at 8 ("Slowly developing technologies, by definition, have more time to percolate through the culture than do the quick ones. And when the pace of change is especially fast, segments of the culture will simply not assimilate.").

[28] *See* Heinrich et al., *supra* note 18, at 1041 (arguing that "legislative bodies must confront the very real possibility that their responses to technologically driven challenges will become obsolete upon their enactment"). Some argue, in fact, that the pace of rapid technological change makes the established judicial procedure—in which appellate courts are forced to rely on factual findings by trial courts made perhaps years earlier—singularly ill-suited to effectively render legal settlements. *See* Stuart Minor Benjamin, *Stepping into the Same River Twice: Rapidly Changing Facts and the Appellate Process*, 78 TEX. L. REV. 269, 279 (1999).

[29] Professor Goldberg, for example, explains that this lag is inevitable because of the law's emphasis on process and science's emphasis on progress:

> Thus the fundamental difference in values between science and law is subtle, but important. Science is not a compendium of timelessly true statements. It is, in a sense, a process for formulating and testing hypotheses that are not always open to revision. But in science this process is a means to an end, and that end is progress in our knowledge of the world. In law, process is not simply or primarily a means to an end. In

tors rushing in to make decisions that might strangle the new technology in its crib.[30]

Since the legal system is always going to be reactive, not proactive, with regard to technological change, the rate of that change is going to further complicate matters. A slowly evolving technology gives time for the legal system to catch up and perhaps regulate future growth. But a radically fluctuating technology is constantly going to leave the law behind, rending established legal settlements. Lawyers trying to advise clients about how to act within such a radically changing technological environment find themselves, like Hercules, trying to slay the nine-headed "Lernaen Hydra," finding that two new heads grow in place of every one cut off.[31] This is especially true if the technology evolves at an uneven rate—or if some aspects of the technology change more quickly than others—because that will make the rate of change even more unpredictable.

C. *Penetration*

A third characteristic of technological change is how deeply it penetrates into society. The greater the infiltration, the more seismic the legal impact. Essentially, penetration depends on the cost of using the technology, its convenience, its ease of use, and its reliability.[32] If a technology is costly or difficult to use, it will have only marginal impact on a society and compel very little legal change; but a technology that is easily accessed, cheap, and useful will obviously penetrate deeply.[33] The Internet, for example, existed for over twenty years without creating even a blip on our societal radar screen,

---

an important sense, process is the end.
STEVEN GOLDBERG, CULTURE CLASH: LAW AND SCIENCE IN AMERICA 19 (1994).

[30] *See* Ira Magaziner, *Keynote Address: At the Crossroads of Law and Technology*, 33 LOY. L.A. L. REV. 1165 (2000) (arguing for governmental restraint in confronting new technologies).

[31] In Greek mythology, one of Hercules' labors was to slay the nine-headed Lernaen Hydra. Whenever Hercules cut off one of the heads, two new heads grew back on. Hercules ultimately killed the serpent by burning the neck stumps after lopping the heads off, not a particularly helpful analogy at this point for legal assimilation of new technology. *Paradigm Busters: Hercules, Alexander, & You, at* http://www.ganesha.org/leading/hercules.html.

[32] Wilkins, *supra* note 1, at 7.

[33] *Id.* at 5-7 (discussing various technologies).

resulting in virtually no legal ramifications. This was mainly because it was cumbersome, slow, and difficult for all but the truly technically sophisticated to use. But following the innovations related to the creation of the World Wide Web, browsers, high speed connections, and search engines, and the concomitant commercial frenzy of the late 1990s, the Internet has penetrated as deeply as any technological change in generations. As a result, we have witnessed an explosion of Internet-related legal issues as society comes to grasp with the medium's abilities and limitations.[34]

This dynamic will repeat itself with any new technology. The extent to which it penetrates into the culture will help determine if it has any impact on the prevailing legal paradigm.

D. *Uniqueness*

A unique technological change is one that does not have an easy antecedent upon which to base legal doctrine. Unprecedented technologies pose greater challenges for legal assimilation because they reduce our ability to predict their societal effects.

In confronting technological change, especially when it comes to new communication media, we need to recognize that our ability to understand the implications of that assimilation will be limited because of our experience with existing media. Humans are more comfortable with the recognizable rather than the strange. Lawyers in particular are always likely to "fight the last war," to adapt to new media with particular reference to old media. Part of this inclination is caused by the cognitive tendency to be over-influenced by the information that is most easily recalled and salient (the "availability heuristic").[35] That is, we adapt to new technologies by relying on

---

[34] For example, I conducted two online searches for law review articles that mentioned the word "Internet" or "Arpanet," the precursor to the Internet, in their text. My first search was for the terms in any article prior to January 1, 1990. It turned up 13 documents. My second search was for the terms in any article after January 1, 1990, which was the year in which browser software was first introduced. *See* Hricik, *supra* note 3, at 462-63. The search was stopped at 10,000 documents.

[35] *See, e.g.*, Timur Kuran & Cass R. Sunstein, *Availability Cascades and Risk*

reference points provided by older, established technologies with which we are familiar.[36] The invention of radio, for example, was a staggering technological change, far more unique than the later invention of television, simply because users of televisions could think of them as "radios with pictures." Although television has arguably had a more lasting impact on our society (perhaps because of its penetration), radio posed a far greater challenge to existing legal paradigm at its inception simply because there had been nothing like it before. Similarly, the Internet, for all its glamour, may not have nearly the uniqueness as the anteceding invention of the personal computer.

The uniqueness of a technological change is even more problematic for our legal system than for society as a whole, simply because of the style of analysis in which lawyers engage. Our legal system is predicated on argument by analogy, training us to search intently for the closest available factual precedent.[37] Analogies are both our strength and our weakness—our strength because of the analogical potential to render the complex more simple and accessible, but our weakness because analogies by their nature shear off the rough edges of dissimilarity and can often place boundaries on our thinking. Especially when confronting technological change, we can reach the limitations of analogical usefulness; this happened, for example, in *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*,[38] where the Court, in considering

---

Regulation, 51 STAN. L. REV. 683, 705 (1999) (discussing availability heuristic); *see also* SCOTT PLOUS, THE PSYCHOLOGY OF JUDGMENT AND DECISION MAKING 121 (1993) (defining heuristics).

[36] Linda Hamilton Krieger, *The Content of Our Categories: A Cognitive Bias Approach to Discrimination and Equal Employment Opportunity*, 47 STAN. L. REV. 1161, 1188 (1995) (discussing cognitive biases and "schemas," which are ways people can process information).

[37] KARNOW, *supra* note 22, at 5 ("this 'reasoning from analogy' to which lawyers are trained presupposes a lurking metaphor and overarching imagery, shared assumptions as between the old and new contexts.") As Justice Cardozo once wrote, "I do not mean that the directive force of history, even when its claims are most assertive, confines the law of the future to uninspired repetition of the law of the present and the past. I mean simply that history, in illuminating the past, illuminates the present, and in illuminating the present, illuminates the future." BENJAMIN CARDOZO, THE NATURE OF THE JUDICIAL PROCESS 53 (1921).

[38] 518 U.S. 727 (1996) (finding that permitting operator to prohibit patently offensive or indecent programming on leased access channels is consistent with First Amendment).

limitations on cable television, forewent analogy as inapposite, and instead it conducted a fact-intensive review of the technology.[39] Indeed, because of the peculiarly accelerated nature of technological change, analogies can be singularly misleading:

> Analogical reasoning plays a profoundly important role whenever a court must decide the proper legal rules to apply to a new technology. Sadly, however, courts usually stumble before they find the correct analogy for new technologies. The law of copyright has provided several notorious examples. Piano rolls were not originally understood to be analogous to sheet music. Software stored in read only memory was not understood to be the same as software stored on disk .... When a court fails to use analogical reasoning and attempts to regulate a new technology without the guidance of history, it risks creating bad law. Although such determinations are almost always eroded over time or reversed later, they may cause harm in the intervening years.[40]

This is the dynamic we have seen constantly with the Internet, as lawyers and judges toil endlessly for the proper analogy: is a web page similar to a newspaper, a town crier, or a radio station or is e-mail like a postcard sent through the mails or a whispered conversation in a crowded room?[41] How the analogy plays out often determines the applicable legal standards,

---

[39] The Court did not conduct its traditional forum analysis, and it refused to categorize the applicable standard of review. *See* Heinrich et al., *supra* note 18, at 1045 (reviewing the *Denver Area* decision and concluding that "[j]urisprudence in an era of dynamic change may well proceed on an increasingly case-by-case basis"); Price & Duffy, *supra* note 21, at 979-980 (discussing how the *Denver Area* decision represented ideological preferences).

[40] Jonathan Wallace & Michael Green, *Bridging the Analogy Gap: The Internet, the Printing Press, and Freedom of Speech*, 20 SEATTLE U. L. REV. 711, 720-21 (1997); *see also* ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM 100 (1983) ("When the telephone was invented, the question was whether, at law, the telephone was a new kind of telegraph or something different. If the phone was a telegraph, a body of law already existed that would apply. The decisions sometimes went one way, sometimes the other; but the model of the telegraph was always there to be considered."); Heinrich et al., *supra* note 18, at 1045 ("Arguably, judicial decision-making may be challenged at a more radical level in coming years. Traditional rule-based, categorical reasoning, one of the hallmarks of the judicial decision-making process, is ill-suited to address areas of dynamic change.").

[41] Wallace & Green, *supra* note 40, at 720. With regard to new media, several commentators have pointed out the difficulty of defining categories that are intellectually defensible and stable. *See* Eric M. Freedman, *A Lot More Comes into Focus When You Remove the Lens Cap*, 81 IOWA L. REV. 883, 960 (1996) (stating that "there arises a widespread view that neither the doctrinal categories nor the substantive content of current First Amendment law are adequate to deal with emerging problems").

and our ability to develop appropriate analogical imagery and form accurate connections between old and new will depend on technological uniqueness.

E. *Conclusion*

Technological change creates ambiguity about the application of legal rules throughout our society. With our often incomplete comprehension of technological complexity, tentative, searching reliance on analogies, and our inability to judge the speed at which technology might change or penetrate into society, we are often in a state of flux, uncertain how to adapt to the changes. Having established principles of technological change, the next question becomes whether these difficulties have affected the legal response to the challenges posed by e-mail for the attorney-client privilege.

II. E-MAIL AND THE NO-ENCRYPTION CONSENSUS

A bit surprisingly, lawyers have rushed to adopt the Internet as a communications media. Usually, with new technologies, there is a feeling-out period in which professionals, particularly non-technologically-oriented lawyers, will take a wait-and-see approach.[42] But the Internet has been a phenomenon, and lawyers, like everyone else, have been seduced by its ease, convenience, and universal access.[43] Lawyers can now share and retrieve information with an ease not possible even five years ago; indeed, one recent survey found that every law firm contacted provided Internet access to lawyers at their own desks and that each of the firms used e-mail for business purposes.[44]

---

[42] *See* Paul Bernstein, *Bulletin-Board Systems Hold Accessible Pools of Information*, NAT'L L.J., Apr. 7, 1986, at 15 (pointing out that law firms have traditionally been behind the cutting-edge on technological issues).

[43] Indeed, some lawyers are forced to use the Internet by the clients whose confidences they are concerned with protecting. In one article, a lawyer was quoted as saying, "Sometimes we have to remind [clients] of the risks and suggest something be mailed or done on the phone to avoid a written record." Emily Tipping, *Internet and E-Mail Are Viewed as Indispensable Tools for Law Firms*, PITT. BUS. TIMES & J., June 2, 2000, at 36.

[44] *Id.* at 36 (reporting a survey of law firms conducted by the Financial Printers Network, a worldwide alliance of independent financial printers). One article cited an ABA small firm technology survey indicating that, even in 1997, almost

This Section examines how e-mail came to be generally accepted as a safe communication medium for lawyers. In determining what standards we should apply to protecting the attorney-client privilege for documents transmitted over the Internet, we need to examine the development of the no-encryption consensus for e-mail. Specifically, a review of that debate over the past five years shows that there was a rush to judgment on e-mail confidentiality that resulted in a virtual sanctification of the medium by the ABA, state ethics boards, and the few commentators who reviewed the subject in law review articles and notes. Without case law, virtual unanimity developed that attorneys can use unencrypted e-mail without waiving their client's confidences based on a misunderstanding of e-mail and technological change.

This Section reviews how this orthodoxy for e-mail developed, arguing that lawyers should avoid relying on the same flawed standard for developing Internet information technologies.

A. *E-mail and Encryption Defined*

The word "e-mail" can be broadly defined as a message sent over a computer network that usually includes text but can also enclose by means of attachment any sound, video, or text file.[45] E-mail is by far the most popular Internet application. Indeed, Forrester Research estimated in early 2000 that within two years, American users will send over 1.5 billion e-mail messages per day.[46] The appeal for lawyers is obvious because e-mail provides near-instantaneous communication for lawyers working in distant locations and an ability to share and exchange documents with relative ease.

---

two-thirds of small firms responding reported using the Internet. Mitchel L. Winick et al., *Playing I Spy with Client Confidences: Confidentiality, Privilege and Electronic Communications*, 31 TEX. TECH. L. REV. 1225, 1243 (2000) (relying on ABA, Legal Technology Resources Center, 1997 Small Firm Technology Survey (1997)).

[45] "E-mail" is defined as "the exchange of computer-stored messages by telecommunication." *Whatis.com?*, *at* http://www.whatis.com.

[46] Bob Tedeschi, *Wary of Hackers and Courts, E-Mail Users are Turning to Services that Keep Their Messages Secure*, N.Y. TIMES, Jan. 31, 2000, at C11 (citing estimates by Forrester Research, Inc.).

Understanding security issues concerning e-mail requires knowing a little about how e-mail works. Some e-mail, solely internal, is sent within private networks such as a law firm's local area network ("LAN") or "intranet,"[47] or over "closed" public proprietary networks such as America Online or Earthlink.[48] However, for the purposes of this Article, I will discuss "external" e-mail, or e-mail sent via the Internet. In these instances, the e-mail travels from the sender's computer through the networked internal e-mail server to external servers on the Internet.[49] The e-mail does not go directly from the sender's to the receiver's host server. Rather, once it leaves the host server, it is transmitted between networks that are connected to one another through a series of access points or "gateways."[50] Each network forwards the e-mail through a "router," a device that analyzes the transmission, examines the various network points to which it could send the message next, and sends the message on the most efficient path based on its understanding of the state of the networks to which it is connected. In this process, the e-mail might go through up to a dozen separate routers on its way to its destination server, and it might be stored for a brief time on an intermediate server

---

[47] An intranet is defined as "a private network that is contained within an enterprise" used to "share company information and computing resources among employees." A local area network or "LAN" is defined as "a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building)." *Whatis.com?*, *at* http://www.whatis.techtarget.com/WhatIs_Definition_Page.html (last visited Feb. 13, 2001).

[48] Generally speaking, an e-mail sent internally or between two members of the same proprietary service (e.g., two America Online members) does not have the same security concerns as an Internet e-mail. *See* Winick et al., *supra* note 44, at 1246 (stating that closed systems present "virtually no" confidentiality issues). Although an internal or proprietary network's e-mail system might be compromised by outsiders, and although there might be confidentiality issues that are raised by the ability of systems administrators to review confidential e-mail, those issues are outside the scope of this Article. *See* Lou Parker & Dave Gardner, *Using the Internet—Ethical, Privileged, or Malpractice?*, 8 NEVADA LAW., June 2000, at 20 (discussing ways of protecting e-mail through dedicated lines, firewalls, and virtual private networks).

[49] To some extent, I simplify the explanation of the process here. For more technical descriptions of e-mail technology, see Hricik, *supra* note 3, at 463-64; Masur, *supra* note 3, at 1141.

[50] Indeed, this interconnection of networks makes up what we think of as "the Internet."

while the router chooses a path for the next leg of its journey. During this time, the e-mail might also be broken down into chunks of information, or "packets," that might take different routes and get reassembled at the end of the journey.

These two features of the Internet—"dynamic routing" and packetization—are two of its defining characteristics, remnants of its inherently decentralized construction, which provides various redundant paths from one point to the other, originally designed to ensure that the physical destruction of any one set of servers would not cripple the system and prevent messages from getting through.[51] Indeed, these concepts have led some to believe that an e-mail journey's resulting randomness is its greatest protection because potential interceptors cannot predict with certainty the route a particular e-mail will take.[52]

There are numerous ways, though, in which an e-mail can still go astray. The most obvious, of course, is through simple human error: mis-addressing the communication. For example, one lawyer received an e-mail from a client attaching what she thought was the final draft of a document. She made comments on the draft and then replied to the distribution list for the original e-mail. Unfortunately, she had misunderstood the communication, which was actually the final draft of the document being distributed to both sides of the transaction, and she unwittingly communicated her thoughts to opposing counsel.[53]

An e-mail might also be subject to interception, either while being stored or being sent. An intruder could, for example, unauthorizedly access e-mail being stored on an insecure system, just as a hacker could compromise any improperly secured computer data. Also, the staff at an e-mail provider's ISP or internal network administrators have physical access to

---

[51] This aspect of the Internet derives from its origins as a Department of Defense project known as the Advanced Research Projects Agency Network (the "Arpanet"), which was designed to be an interlink of governmental academic networks protected from destruction by its redundant routing capabilities. *See* KATIE HAFNER & MATTHEW LYON, WHERE WIZARDS STAY UP LATE: THE ORIGINS OF THE INTERNET 71-73 (1996); Hricik, *supra* note 3, at 462-63 (describing the development of Arpanet and the eventual commercial development of the Internet).

[52] ABA Opinion, *supra* note 5, at § C.4; Hricik, *supra* note 3, at 468-69.

[53] This story, apparently true, was recounted in an article in the *New York Law Journal*. *See* Rose Auslander, *Keeping Sensitive Information Private*, N.Y.L.J., June 8, 1999, at 5.

transmissions between their LAN's and other Internet nodes, so they always have the ability to read or review any e-mail passing through their networks. Users can protect themselves from those types of security problems, though, by shoring up their own internal network protections.

E-mail is most vulnerable while it is traveling from network to network over the Internet. There are two particular methods of gaining unauthorized access to e-mails. The first is "sniffing"—using software to intercept an e-mail traveling through a network on its way to its destination by capturing it at a particular router on its path.[54] The router is programmed not just to read the e-mail for its destination address, but to look for information contained within; the router can also be programmed to look only for certain types of data or only for transmissions coming from or intended for particular machines.[55] Sniffers are normally benign tools used by network administrators to maintain their systems,[56] but they can also be put to unauthorized purposes. Reportedly, for example, some hackers set up a "sniffer" on an Internet node or router on the main New York to Washington routing hub to search for the word "merger," trying to access potentially confidential communications.[57] Another method of intercepting e-mail is through a "spoofer," a computer configured to waylay messages meant for a particular user by emulating the user's computer.[58] In spoofing, the hacker programs a computer on the network to impersonate the intended recipient's computer, thereby snaring the recipient's messages in transit. The spoofer might also even send back a message to the original sender, making

---

[54] Sniffer programs are easily downloadable off the Internet. For example, inputting "sniffer" into a major search engine revealed a program that would do all of the following: "Listen to all TCP/IP traffic on a subnet; Intercept all outgoing requests for Web documents and display them; Intercept all incoming requests for Web documents and display them; [and] Decode the Basic authentication passwords, if any." *Example Web Packet Sniffer, at* http://stein.cshl.org/~lstein/talks/WWW6/sniffer. The author apparently wrote the program to "show how vulnerable the Web is to sniffing." *Id.*

[55] Millington, *Decoding E-mail Encryption*, COLO. LAW., Mar. 1998, at 78.

[56] Masur, *supra* note 3, at 1155. Masur tells a story of how he once set up a sniffer to capture all the network traffic on a client's internal network, resulting in him discovering the company president's e-mail password. Masur, *supra* note 3, at 1155.

[57] Masur, *supra* note 3, at 1155.

[58] Masur, *supra* note 3, at 1154; *see also* Hricik, *supra* note 3, at 497.

it seem as if the e-mail was properly delivered.[59]

A user can protect e-mail from interception, though, in several ways. In addition to keeping e-mail from entering the Internet through the use of dedicated lines or internal networks—which would not be feasible for lawyers needing to communicate with someone through the Internet—users can take advantage of encryption technology. Encryption encodes and scrambles a message by translating it according to a secret mathematical formula (the "key"), rendering it unintelligible to anyone who does not know that formula.[60] For some encryption mechanisms, known as symmetrical key encryption,[61] the same secret key is used for both encryption and decryption; that is, the sender encrypts her message using a particular formula, and the recipient decodes the message using that same key.[62] The problem with single-key encryption is that both sides need possession of the key, which leads to the logistical difficulties of getting the same key to both sender and recipient without making the key itself vulnerable to interception by distributing it too widely, which would undermine the whole purpose of having only one key.[63]

---

[59] Hricik, *supra* note 3, at 499.

[60] RSA Labs defines the term as follows: "Encryption is the transformation of data into a form that is as close to impossible as possible to read without the appropriate knowledge . . . . Its purpose is to ensure privacy by keeping information hidden from anyone for whom it is not intended . . . ." *What is Public Key Cryptography*, *at* http://www.rsasecurity.com/rsalabs/faq/1-2.html (last visited Feb. 28, 2001).

[61] This type of encryption is also described as "private key" or "single key" encryption. *Id.*

[62] *Id.* For a thorough, accessible description of encryption, see JERRY LAWSON, THE COMPLETE INTERNET HANDBOOK FOR LAWYERS 226-33 (1999) (discussing private- and public-key encryption and recommending some form of encryption security for e-mail); *see also* Masur, *supra* note 3, at 1134 (describing public- and private-key encryption).

[63] RSA Labs describes the problem as follows:

> The main challenge is getting the sender and receiver to agree on the secret key without anyone else finding out. If they are in separate physical locations, they must trust a courier, a phone system, or some other transmission medium to prevent the disclosure of the secret key. Anyone who overhears or intercepts the key in transit can later read, modify, and forge all messages encrypted or authenticated using that key. The generation, transmission and storage of keys is called key management.

What is Public Key Cryptography?, *at* http://www.rsasecurity.com/rsalabs/faq/2-1-1.html (last visited Feb. 28, 2001).

Public-key encryption solves these logistical problems by giving each user a pair of keys—one public and one private—that are linked so that information encrypted with the public key can only be decrypted by the private key.[64] The public key associated with a particular user is published or otherwise made publically available on some trusted third party certification authority; meanwhile, the private key is kept secret. To take advantage of public-key encryption, a sender (or, more likely, the sender's e-mail software) determines what her recipient's public key is, then encrypts the message through that public key. The e-mail, as it wends its way through the Internet, is encrypted and unintelligible.[65] When the user receives it, though, he can decrypt it using the private key associated with the public one.

Used correctly, encryption is a virtually ironclad guarantor of e-mail security.[66] Traditionally, though, encryption software has been awkward or difficult to use, and managing the various public and private keys associated with each user is a significant burden on attorneys and support staff.[67] The question of whether attorneys using e-mail for confidential information should encrypt their e-mail to take advantage of that ironclad security has been the subject of active debate for the past five years.

---

[64] LAWSON, *supra* note 62, at 227-29 (describing fundamental public- and private-key issues); Masur, *supra* note 3, at 1134; Millington, *supra* note 55, at 73.

[65] *What is Public Key Cryptography?*, *at* http://www.rsasecurity.com/rsalabs/faq/2-1-1.html (last visited Feb. 28, 2001); Lou Parker & Dave Gardner, *Using the Internet—Ethical, Privileged, or Malpractice?*, 8 NEVADA LAW., June 2000, at 20.

[66] LAWSON, *supra* note 62, at 230 (stating that while encryption is not foolproof, it does provide the best security available); *accord*, Masur, *supra* note 3, at 1135-36. Some critics argue that encryption is not perfect. In one article, for example, a lawyer argued that encryption was not only awkward and expensive but also that it does not generally protect the identities of the sender or recipients, meaning that a sniffer could still single out messages by particular individuals. Hricik, *supra* note 3, at 494-95. Even Lawson, a proponent of encryption, notes that any system is "breakable." LAWSON, *supra* note 62, at 230.

[67] Auslander, *supra* note 53, at 5 (stating that "encryption is awkward enough that most firms do not use it . . . . The expense and difficulty would be multiplied where a law firm has several different clients who prefer several different forms of encryption").

B. *The Consensus on E-mail Encryption*

Formal recognition of the security issues related to whether using e-mail for privileged correspondence waived the privilege started developing in 1995 to 1996 in a series of state bar ethics opinions and law review or bar journal commentaries.[68] While the early signals were very cautious, later decisions, including an authoritative statement by the ABA, declared e-mail a safe medium for attorney-client correspondence.

The early opinions about e-mail usage by attorneys took relatively severe views. The strictest came in 1995, when the South Carolina State Ethics Board stated that an attorney could not use the Internet for client correspondence because of the presence of system operators who would have access to the communications.[69] This was a particularly extreme opinion, effectively barring the Internet as a communications medium because any network system is going to require a technical operator (who is almost certainly not going to be a lawyer

---

[68] According to an online database search, the first law review commentary on the issue was published in November 1996. *See* William P. Matthews, *Encoded Confidences: Electronic Mail, The Internet, and the Attorney-Client Privilege*, 45 U. KAN. L. REV. 273 (1996) (arguing that American legislatures and courts should recognize an expectation of privacy in electronic mail sufficient to sustain the attorney-client privilege). There were also some non-law review commentaries that came out during this time. *See, e.g.*, Ron Smith, *Lawyers Must Overcome Technophobia, Learn to Take Advantage of E-mail, Net*, 65 KAN. B. J. 3 (1996) (arguing for use of Internet and e-mail by lawyers); Charles R. Merrill, *E-mail for Attorneys From A to Z*, Practicing Law Institute, PLI Order No. G7-4697, at 187 (December 1996) (pointing out dangers of unencrypted e-mail); Peter R. Jarvis & Bradley F. Tellam, *The Internet: New Dangers of Ethics Traps*, OR. ST. B. BULL., Dec. 1995, at 7, 17 (arguing that e-mail service from reputable providers would protect privilege); Todd Flaming, *An Introduction to the Internet*, 83 ILL. B.J., 311, 311 (1995) (discussing e-mail use by attorneys).

[69] S.C. Bar, Advisory Op. 94-27 (1995) ("[T]he very nature of on-line services is such that the system operators of the on-line service may gain access to all communications that occur on the on-line service. Thus, the confidentiality requirements of Rule 1.6 are implicated by any confidential communication which occurs across electronic media, absent an express waiver by the client."). The opinion developed from a question concerning advertising online and using electronic bulletin boards. So it is possible that the board's opinion was not particularly centered on the issue of e-mail itself. Even those who argue that e-mail is not a particularly safe medium acknowledge that system operator access to e-mail is no different from, say, entrusting a confidential package to a Federal Express delivery person. *See* Robert A. Pikowsky, *Privilege and Confidentiality of Attorney-Client Communication Via E-Mail*, 51 BAYLOR L. REV. 483, 562 (1999) (asserting that operator access does not violate confidentiality).

within the confidential relationship). Other ethics boards in Iowa and Arizona took more cautious views, requiring or suggesting encryption protections in order for attorneys to send confidential or sensitive material over the Internet via e-mail.[70]

The momentum shifted in 1997, when both Iowa and South Carolina reconsidered their previous decisions and other states leaped in to declare e-mail a secure medium. The Iowa board amended its opinion, eliminating the encryption requirement and asking only that the lawyer and client should agree as to the means of adequate protection of e-mail correspondence.[71] The South Carolina ethics board reversed itself, partly on the ground that "use of e-mail has become commonplace, and there now exists a reasonable level of 'certainty' and expectation that such communications may be regarded as confidential."[72] The board indicated that there had been changes in technology that had made e-mail more safe, but did not identify what those technological advancements had been.[73]

Soon, a number of state ethics boards weighed in with opinions that e-mail was no less safe than other communications media such as facsimile machines or telephones. One of the most influential was from the Illinois State Bar Association, which in May 1997 explicitly disagreed with the initial Iowa and Arizona positions, finding that Internet e-mail was no less safe than traditional telephone calls.[74] The board justi-

---

[70] Iowa Sup. Ct. Bd. of Prof'l Ethics and Conduct Op. 96-01 (1996) ("[C]ounsel must have written acknowledgment by client of the risk of violation of DR 4-101 which acknowledgment includes consent for communication thereof on the Internet or non-secure Intranet or other forms of proprietary networks, or it must be encrypted or protected by password/firewall or other generally accepted equivalent security system."); Ariz. State Bar Ass'n, Comm. on Rules of Professional Conduct, Op. 97-04 (1997) ("E-mail should not be considered a 'sealed' mode of communication.").

[71] Iowa Sup. Ct. Bd. of Prof'l Ethics and Conduct, Op. 97-01 (1997) (amending opinion to omit requirement of encryption).

[72] S.C. Bar, Ethics Advisory Comm., Op 97.08 (1997). The opinion went on to say that "[w]hile there exists a potential for communications to be intercepted, albeit illegally, from a commercial network mailbox or an Internet "router," the Committee does not believe such a potential makes an expectation of privacy unreasonable. The same potential exists for the illegal interception of regular mail, the interception of a facsimile, and the unauthorized wiretapping of land-based telephone." *Id.*

[73] Masur, *supra* note 3, at 1125 (criticizing lack of technical analysis of e-mail in board opinions); *accord*, Auslander, *supra* note 53, at 5.

[74] Ill. State Bar Ass'n, Comm. on Prof'l Responsibility, Advisory Op. 96-10

fied its decision on its understanding of both the technology and the law. First, the board asserted that the technology of e-mail made interception as difficult as wiretapping phone calls, particularly because of packetization and the transmission over phone lines rather than over the open air waves.[75] Second, the board speculated that e-mail users had a reasonable expectation of privacy because intercepting an Internet transmission would be a clear violation of the Electronic Communications Privacy Act of 1986 (the "ECPA").[76] The board, in fact, flatly rejected the idea that it was necessary to discuss the possibility of encryption with clients to make sure they did not prefer to use encryption technology.[77]

The Illinois opinion presaged the developments in the state ethics boards, and it was followed and often cited by decisions in Alaska, the District of Columbia, Kentucky, North Dakota, Pennsylvania, and Tennessee.[78] Two state boards within the Second Circuit, Vermont and New York, adopted a similar rule.[79] The New York State Bar Committee on Profes-

---

(1997).

[75] *Id.*

[76] *Id.*; *see also* 18 U.S.C. § 2517(4) (1996) ("No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.").

[77] Ill. State Bar Ass'n, Comm. on Prof'l Responsibility, Advisory Op. 96-10 (1997) ("Nor is it necessary, as some commentators have suggested, to seek specific client consent to the use of unencrypted e-mail. The Committee recognizes that there may be unusual circumstances involving an extraordinarily sensitive matter that might require enhanced security measures like encryption. These situations would, however, be of the nature that ordinary telephones and other normal means of communication would also be deemed inadequate.").

[78] *See* Ala. Bar Ass'n Ethics, Op. 98-2 (1998) (holding that lawyers need not encrypt e-mail to ensure confidentiality); D.C. Bar Op. No. 281 (1998) (stating that transmitting confidential information via e-mail does not per se violate confidentiality); Ky. Bar Ass'n Ethics Comm. Advisory Op. E-403 (1998) (holding that absent "unusual circumstances" lawyers may use e-mail, including unencrypted Internet e-mail, to communicate with clients); N.D. State Bar Ass'n Ethics Comm., Op. 97-09 (1997) (stating that lawyers need not use encryption for routine e-mail); Pa. Bar Assoc. Comm. on Legal Ethics and Prof'l Responsibility, Informal Op. 97-130 (1997) ("[E]-mail does not appear to differ materially from current means of communication employed by lawyers to the extent that a new set of rules is required, or such that its use should be discouraged."); Bd. Prof'l Responsibility Sup. Ct. Tenn., Adv. Ethics Op. 98-650(a) (1997) (permitting the use of Internet e-mail because "the technology involved in e-mail is now better understood and the use of e-mail more widespread").

[79] *See* N.Y. St. Bar Ass'n Committee on Prof'l Ethics, Op. 709 (1997); Vt. Bar Ass'n Comm. on Prof'l Responsibility, Advisory Op. 97.5 (1997) ("Since [the] possi-

sional Ethics, for example, determined that encryption was not necessary on the grounds that (1) the "criminalization of unauthorized interception of e-mail certainly enhances the reasonableness of an expectation that e-mails will be as private as other forms of telecommunication"[80] and (2) "the developing experience from the increasingly widespread use of Internet e-mail persuades us that concerns over lack of privacy in the use of Internet e-mail are not currently well founded."[81] Similarly, the New York State legislature in 1997 adopted a statute ensuring that electronic communications did not lose their privileged character solely because of their electronic transmission.[82]

By 1999, the ABA Standing Committee on Ethics and Professional Responsibility (the "Committee") endorsed the use of e-mail by attorneys, stating that a "lawyer may transmit information relating to the representation of a client by unencrypted e-mail sent over the Internet . . . because the mode of transmission affords a reasonable expectation of privacy from a technological and legal standpoint."[83] The Committee further opined that the "same privacy accorded U.S. and commercial mail, land-line telephonic transmissions, and facsimiles applies to Internet e-mail."[84] The Committee did issue the disclaimer that the decision was based on the technology at the time, although it did not identify the particular technological limitations or qualities upon which the decision was based and that might change.[85]

---

bility of interception also exists for fax transmission and regular mail, no reason exists to treat e-mail differently.").

[80] N.Y. St. Bar Ass'n Committee on Prof'l Ethics, Op. 709. The board did note, though, that a "lawyer who uses Internet e-mail must also stay abreast of this evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost." *Id.*

[81] *Id.*

[82] *See* N.Y. C.P.L.R. 4548 (McKinney 1999) ("No communication privileged under this Article shall lose its privileged character for the sole reason that it is communicated by electronic means or because persons necessary for the delivery or facilitation of such electronic communication may have access to the content of the communication."); *see also* CAL. EVID. CODE § 954 (Deering 1999) (stating that otherwise protected communications will not lack confidentiality "solely because the communication is transmitted by facsimile, cellular telephone, or other electronic means between the client and his or her lawyer").

[83] ABA Opinion, *supra* note 5, at Intro.

[84] ABA Opinion, *supra* note 5, at Intro.

[85] ABA Opinion, *supra* note 5, at Intro.; *see also* Julie Brienza, *No Encryption*

The ABA's opinion was widely anticipated by the legal community, which was balky at the concept of having to encrypt all client e-mail, and which applauded the decision as a ratification of what by that time was common practice. As a reporter for the *New York Law Journal* stated, the "sigh of relief" that greeted the opinion from lawyers who had been using e-mail without encryption was "almost audible."[86] Similarly, what academic or professional commentary there was on the issue generally agreed with the consensus that e-mail was safe enough for attorney-client transmissions and that encryption should not be necessary. David Hricik, whose revealingly-titled article, *Lawyers Worry Too Much About Transmitting Client Confidences by Internet E-mail*, was cited by the ABA in its opinion, summed up the prevailing mood:

> The problem with arguments being made to demonstrate that the Internet is not secure is, when applied to existing modes of communication, even the most highly-regarded and most secure means of communication cannot be used without warnings, encryption, or both. Common sense seems to have lost its place in the debate . . . . Risk of interception subsists in every communication system, such as the telephone and the postal system. Some things should never be written; some things should never be mailed; some things should never be transmitted over the Internet without encryption. However, a bright-line requirement of encryption is unwarranted.[87]

Hricik's conclusions were generally repeated in other commentary in the three years preceding the ABA opinion, most of which either advocated a no-encryption standard or cautiously recommended encryption as a good idea for particularly sensitive documents.[88] While some of those arguments left open

---

Required for Attorney-Client E-Mail, TRIAL, July 1999, at 112 (reporting on ABA opinion, *supra* note 5, stating that it urges attorneys to take a common-sense approach to protecting the privilege).

[86] Wendy R. Leibowitz, *Why E-Mail Encryption May Be Necessary*, N.Y.L.J., May 11, 1999, at 5 (emphasis omitted).

[87] Hricik, *supra* note 3, at 507.

[88] *See* Martha Harris, *E-Mail Privacy: An Oxymoron?*, 78 NEB. L. REV. 386, 410 (1999) (stating that "use of unencrypted e-mail between attorney and client should not, in and of itself, result in a waiver of the attorney-client privilege"); Amy M. Fulmer Stevenson, Comment, *Making a Wrong Turn on the Information Superhighway: Electronic Mail, The Attorney-Client Privilege and Inadvertent Disclosure*, 26 CAP. U. L. REV. 347, 356 (1997) (tentatively calling encryption "worth the effort"); Harry M. Gruber, Note, *E-Mail: The Attorney-Client Privilege Applied*, 66 GEO. WASH. L. REV. 624, 655-56 (1998) (arguing for "some type of security

the possibility that encryption technology could improve to the point of making it a more feasible requirement, only a few recommended encryption.[89]

C. *Evaluating The No-Encryption Standard: E-mail as Technological Change*

This final Section of Part II examines the no-encryption consensus and shows how it relies on a fundamental misunderstanding of the technologies involved. In particular, the ABA and other decision-makers understood too little the complexity and pace of technological change and misjudged the relative penetration of e-mail and encryption technologies. Perhaps as a result, the analogies drawn between e-mail and established technologies did not account for the uniqueness of e-mail as a technological change, resulting in a standard that does not reflect the inherent insecurity of e-mail and the importance of the available remedy in encryption.

---

mechanism" to support precautions but not advocating encryption requirement); Jonathan Rose, Note, *E-Mail Security Risks: Taking Hacks at the Attorney-Client Privilege*, 23 RUTGERS COMPUTER & TECH. L.J. 179, 206 (1997) (arguing for encryption for all confidential information but saying that it may not be feasible). Even commentaries in the last few years accept unflinchingly the idea that encryption is too expensive or difficult to require for Internet transmission of e-mail. *See* Christopher C. Miller, Note, *For Your Eyes Only? The Real Consequences of Unencrypted E-mail in Attorney-Client Communication*, 80 B.U. L. REV. 613, 631-32 (2000) (arguing that encryption "should not be required" because "e-mail provides an efficient, fast and cost-effective means of communication").

[89] R. Scott Simon, *Searching for Confidentiality in Cyberspace: Responsible Use of E-Mail for Attorney-Client Communications*, 20 U. HAW. L. REV. 527, 571 (1998) (arguing that the responsible attorney should take precautions such as encryption when using e-mail); Masur, *supra* note 3, at 1159 (same). One recent commentator did not take a firm position on encryption but clearly warned attorneys to take a cautious approach to using e-mail for confidential client information. *See* Winick et al., *supra* note 44, at 1257 (concluding that attorneys should read into the ABA Opinion, *supra* note 5, that reasonable care requires an affirmative duty to evaluate appropriateness of e-mail for a particular communication). Similarly, Jerry Lawson, author of THE COMPLETE INTERNET HANDBOOK FOR LAWYERS, recommends that although the Internet is "probably secure enough" for most e-mail messages, lawyers should adopt encryption technology as it becomes easier to implement. LAWSON, *supra* note 62, at 237.

1. Complexity: Misunderstanding E-mail Technology

The main weakness in the no-encryption consensus is the lack of technological awareness the ABA and some ethics boards demonstrated, particularly concerning the difficulties in intercepting e-mail messages. One commentator called the debate "little more than an incestuous game of telephone"—inadequate or incomplete descriptions of technological concepts such as packetization and dynamic routing by lawyers in bar journals and law reviews morphed into keystones of ethics boards and ABA opinions that e-mail was an inherently secure medium.[90]

The technological foundation of the ABA's opinion that e-mail was safe was the understanding that dynamic routing and packetization ensured that intercepting an e-mail would be difficult, if not impossible.[91] The interceptor, according to the ABA, would not be able to predict with any real accuracy the path that an e-mail would take (because of dynamic routing) and would likely only get part of the message even if she succeeded (because of packetization).[92] Indeed, the ABA described routing not as dynamic but as "random," indicating a belief that routing patterns were impossible, not difficult, to predict. The ABA never undertook its own examination into the nature of the technology, instead relying on articles written by lawyers, not by technologists, for their technical understandings.

The ABA was not necessarily wrong in these conclusions, but it was perhaps a bit too overconfident that the technologi-

---

[90] Masur, *supra* note 3, at 1122.

[91] The ABA relied in part on the article by David Hricik, a lawyer, in the *Georgetown Journal of Legal Ethics*, in which Hricik identified the state of e-mail technology at the time (1998) and particularly discussed how routing and packetization made e-mail interception improbable. Hricik, *supra* note 3, at 466-67, 498; *see also* Rose, *supra* note 88, at 23 (discussing routing). The earliest articulation of this argument was found in a 1996 article written by a practitioner. *See* G. Burgess Allison, *Technology Update*, LAW. PRAC. MGMT., Apr. 1996, at 16, 18.

[92] ABA Opinion, *supra* note 5, at § C.4 ("[D]uring the passage of Internet e-mail between sender and recipient, the message ordinarily is split into fragments or 'packets' of information. Therefore, only parts of individual messages customarily pass through ISPs, limiting the extent of any potential disclosure. Because the specific route taken by each e-mail message through the labyrinth of phone lines and ISPs is random, it would be very difficult consistently to intercept more than a segment of a message by the same author.")

cal limitations of the Internet made interception as difficult as it believed. As one commentator with experience working as an Internet systems administrator found in an informal experiment, whatever "randomness" there was in dynamic routing and packetization has diminished considerably as the Internet infrastructure has developed.[93] From September to October, 1999, Masur, at the time a student at Columbia University, sent six different e-mail messages between his home computer and three remote computers and found little variety in the paths the messages took through the Internet, much less variety than would be sufficient to provide security.[94]

The technological foundation for the ABA's opinion, and the consensus that e-mail is safe enough, then, is questionably predicated on the state of the art circa 1998 or earlier, when the Internet infrastructure was not nearly as developed as subsequent commercial incentives have spurred.[95] As the Internet becomes more standardized and reliable, e-mail that might at one point have traveled a random, circuitous route to its destination might now take predictable, well-worn, and more easily monitored paths.

Moreover, the ABA's consensus was also grounded legally on the belief that sufficient protections for e-mail security are provided by the criminalization of interception of wire, oral, or electronic communications by the ECPA, and the statutory provision that otherwise privileged communications do not lose their privilege solely from interception.[96] There is little doubt that the ECPA criminalizes the interception of an electronic mail message while in transit, but the extent to which the ECPA protects the privilege of e-mail communications, or

---

[93] Masur, *supra* note 3, at 1147-48.

[94] Masur found that half the routers traversed by the packets were identical and that packets sent within twenty-four hours showed minor or nonexistent variance. Masur, *supra* note 3, at 1147-48.

[95] Moreover, both the ABA and the influential Illinois state ethics board might have mis-conceived the nature of packetization, which does not necessarily break the e-mail into unrecognizable or unintelligible parts; indeed, packetization often simply makes duplicates of the e-mail, increasing the security risk by sending multiple copies of the privileged document through various routers.

[96] 18 U.S.C. §§ 2510-21, 2701-11 (1996). The belief that the ECPA protects e-mail, thus vitiating security concerns, originated, apparently, with Albert Gidari. *See* Albert Gidari, *Privilege and Confidentiality in Cyberspace*, COMPUTER LAW., Feb. 1996, at 1-3.

makes e-mail use reasonable, is questionable. First, there is some debate as to whether accessing an e-mail that is stored on a server awaiting delivery, rather than an e-mail in transit, would be a violation of the ECPA.[97] To date, the only case considering the issue found that e-mail on a server was not protected by the ECPA.[98] Thus, certain types of interception may not be covered. Second, the ECPA may only protect against interception from certain types of networks that provide wire or electronic communications services, rather than networks, for example, set up by universities or other entities that do not, strictly speaking, provide public services.[99] Thus, the ECPA's coverage of an e-mail transmission may be uneven, protecting against interception for some legs of the journey but not for others.

Finally, regardless of the ECPA's coverage, the existence of criminal penalties for those who would intercept private communications does not absolve attorneys from the obligation to protect their confidentiality. 18 U.S.C. § 2517(4) provides that otherwise privileged communications do not lose their privilege solely because of interception,[100] but that does not preclude an inquiry into the seriousness with which an attorney protected the privilege from interception. If a lawyer knows that he is

---

[97] *See, e.g.*, Harris, *supra* note 88, at 398 (explaining why the ECPA may not protect Internet transmissions because the statute only covers messages in transit, not stored messages); *cf.*, United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998) (finding archived voice-mail covered by the Stored Communications Act, differentiating voice-mail from e-mail, covered by the ECPA).

[98] Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457 (5th Cir. 1994) (holding that the seizure of a computer used to operate an electronic bulletin board containing unretrieved private electronic mail stored on the bulletin board did not constitute an unlawful intercept under the ECPA); *see also* United States v. Reyes, 922 F. Supp. 818 (S.D.N.Y. 1996) (finding that turning on a pager to retrieve numbers on the page did not violate the ECPA).

[99] *See* Harris, *supra* note 88, at 399 (pointing out that "messages passed through the systems of organizations which are at best only incidentally 'providers' of electronic communications services (for example, universities and large corporations) may not be protected"); Masur, *supra* note 3, at 1141 (asserting that the electronic services provider provisions of the ECPA may only apply to entities that provide services to the public). A court within the Second Circuit, for example, ruled that the ECPA did not cover a corporation that used fax machines and computers as part of its business but did not sell those services to the public. State Wide Photocopy, Corp. v. Tokai Fin. Serv., Inc., 909 F. Supp. 137, 144-45 (S.D.N.Y. 1995).

[100] 18 U.S.C. § 2517(4).

communicating with his client over a compromised medium, he cannot argue that his conversation is privileged simply because the interceptor might be violating the law.[101] In any event, attorneys have more than a duty to simply avoid the evidentiary implications of waiver of privilege; the exposure of private, confidential information about a client poses immense risks to both client and attorney, and there is an independent ethical obligation to do what is necessary to prevent exposure.[102]

2. Velocity and Penetration: The Uneven Development of E-mail and Encryption Technology

The belief that encryption was not necessary for attorney-client communications through e-mail developed at a time when e-mail was easy to use, but encryption was cumbersome and expensive. The two technologies had not developed at the same rate of speed, resulting in commercial applications of e-mail that far outpaced available encryption methods. With encryption not being a feasible, or at least convenient, method of protecting e-mail from interception, the ABA and state ethics boards undoubtedly felt pressure to endorse unencrypted e-mail to both allow lawyers to take advantage of the useful e-mail technology and normalize what was already going on.

Two characteristics of technological change, velocity and penetration, are both implicated by the disparity between the development of e-mail and encryption technologies. Where two related technologies develop at an uneven rate, one resultantly achieving far greater penetration than the other, it makes sense that applicable rules for each would also develop at different rates. A judicial or legislative response to a technology can only occur if that technology achieves sufficient penetration that merits such a response, and even then the response

---

[101] As Wigmore said:

> All involuntary disclosures, in particular, through the loss or theft of documents from the attorney's possession, are not protected by the privilege on the principle that, since the law has granted secrecy so far as its own process goes, it leaves it to the client and attorney to take measures of caution sufficient to prevent being overheard by third persons. The risk of insufficient precautions is upon the client.

8 WIGMORE, EVIDENCE § 2325, at 633 (McNaughton rev. ed. 1961).

[102] MODEL CODE OF PROF'L RESPONSIBILITY D.R. 4-101(A), (B) (identifying duty of lawyers to protect client-related information).

will lag behind. Requiring encryption for attorney-client e-mail in 1998 or 1999 might have seemed an undue burden and an unnecessary expense for practitioners, considering how underdeveloped encryption technology was at the time.

There are also practical implications of the ABA's decision to consider. First, the ABA and state ethics boards are not composed of technologists; rather, they consist, for the most part, of practicing attorneys who live and work in their communities. Not only are they likely to misunderstand the nature of the technology, but they also have overriding incentives to draw inferences in favor of allowing the use of such a convenient new technology, especially where there were sufficient indications that e-mail was safe enough. Indeed, practitioners generally try to ensure the widest coverage possible for the attorney-client privilege, with a high threshold for waiver, because they never know when they will be the unlucky victim of accidental disclosure. Second, attorney use of e-mail for client communication was already a widespread practice by 1999. While lawyers may have worried about security, their concerns apparently did not prevent them from using the technology when they found it convenient or necessary. The "sigh of relief" that greeted the ABA decision, for example, implies that lawyers were reassured about the propriety about what they were already doing, not just that they were relieved of a complicated burden for what they might do in the future.[103] An ABA determination that encryption was required would have implicitly judged lawyers nationwide as previously having abandoned their clients' privilege.

The impact of the differing rates of development is easily illustrated. Had encryption technology developed at the same rate as e-mail technology, and achieved the same level of penetration, the result would clearly have been different. For example, if e-mail technology had developed in the mid-1990s with built-in encryption methods that were easy to use and included within commercial e-mail products, lawyers would never dream of using an e-mail system that did not provide for such protections. Similarly, if e-mail interception technology was more highly developed even now—if, say, someone wrote a foolproof sniffer program that was widely available—lawyers

---

[103] Leibowitz, *supra* note 86, at 5.

might be more inclined to secure their e-mail. It is only in an environment where e-mail technology far outpaced encryption and interception technologies that the no-encryption standard could have developed.

But to set a hard standard by which encryption is never going to be necessary ignores the pace of technological change. Even at the time that the ABA's opinion was released, some observers noted that attorneys should be aware of the potential changes in the state of the art that might make the ABA's opinion obsolete or impractical.[104] The New York ethics opinion made this clear, asserting an attorney's duty to "stay abreast of this evolving technology to assess any changes in the likelihood of interception as well as the availability of improved technologies that may reduce such risks at reasonable cost."[105] This would make sense because the alternative is a static, unchanging set of rules governing e-mail use that does not adapt to changing conditions.[106]

Nevertheless, some practitioners have argued that the New York ethics board was wrong to put this onus on lawyers, that lawyers do not have the expertise to make such judgments, and that, hence, they are under no obligation to keep up with the technology.[107] Indeed, one commentator said that the New York board's caveat would require lawyers to "scramble land line telephone conversations to foil wiretappers, line their office walls with lead to disable bug transmitters, upgrade to ever more powerful encryption, and so on."[108] But

---

[104] *Id.* (citing lawyers and technology experts who pointed out that ethical standards might change as the "technology changes over time"). As Charles R. Merrill, head of the computer and high-tech practice group at a New Jersey firm, stated in the article, "[M]aking a pronouncement without recognizing that tech standards may change is a little out of step" with reality. *Id.*

[105] N.Y. St. Bar Ass'n Comm. on Prof'l Ethics, Op. 709, at § D (1998).

[106] The board's caveat is also consistent with the principle articulated by Judge Hand in *The T. J. Hooper* case that custom of use based on prevailing technology might not control as the state of the art develops. *See infra* Part III.B.

[107] William Frievogel, *Internet Communications—Part II: A Larger Perspective*, ALAS LOSS PREVENTION J., Jan. 1997, at 2-3, as cited in Robert A. Pikowsky, *Privilege and Confidentiality of Attorney-Client Communication Via E-Mail*, 51 BAYLOR L. REV. 483, 559 (1999). According to Pikowsky's account of Frievogel's advisory, Frievogel argues that lawyers do not have an obligation to stay abreast of technological changes that might make using e-mail more or less secure because lawyers are unqualified to have the expertise to understand the technology and because they should have the freedom to rely on the legal protections available. *Id.* at 578.

[108] *Id.* It is uninspiring that Frievogel and the Attorney's Liability Assurance

asking that lawyers avoid using state-of-the-art technologies without being certain of their security or taking advantage of available safety precautions does not itself require lawyers to adopt every conceivable safety precaution for every possible communication technology.[109] The New York board's sensible reminder to stay abreast of the technology only applies to lawyers using state-of-the-art technology in Internet communications. If attorneys want to take advantage of those new types of communications, they should educate themselves about the security limitations. Lawyers talking in the sanctity of their offices, or over old-technology land-line telephones, are clearly respecting and protecting the privilege.[110] But lawyers who want to use "newfangled" equipment for its ease and convenience, who thereby cast their confidential information over an Internet system over which they or their agents have no dominion, who rely solely on the unpredictability of the e-mail's

---

Society (the "ALAS") would take the position that encryption is not necessary and that attorneys need not take special precautions to protect client security because the ALAS is in the business of underwriting legal malpractice insurance. *See* Winick et al., *supra* note 44, at 1254-55.

[109] Pikowsky also argues that analogies to Judge Hand's opinion in *The T. J. Hooper* are "irrelevant" because that case "is usually cited in maritime cases" and has not been cited "in the context of legal ethics, evidentiary privileges, or professional liability." Pikowsky, *supra* note 107, at 577. This argument does not really stand up to any analysis. No one argues that *The T.J. Hooper* is a binding precedent on issues of privilege (or that it is binding in any other jurisdiction), but the principles established therein are helpful when we have no direct binding precedent at all. *The T. J. Hooper* has become a landmark case in negligence theory generally, establishing the proposition that reliance on custom is not necessarily a defense to negligence, and the theory upon which the case is grounded has clear application to an attorney's ethical duty to use precautions appropriate for the technology she uses. Even Hricik, whose influential 1998 article found that encryption was unnecessary as a bright line rule, agreed that Judge Hand's "seminal opinion" was applicable for determining the level of precautions necessary. Hricik, *supra* note 3, at 506; *see also* LAWSON, *supra* note 62, at 233-34 (arguing for applying Hand principles). The examples of lawyers having to debug their conference rooms are simply silly, but more pernicious is the idea that lawyers should be able to blithely ignore the state of the art when taking advantage of modern technology. If a lawyer wishes to use e-mail, or a cell phone, she has a duty to ensure that her communications are secure.

[110] Moreover, as I demonstrate in Part III, *infra*, a lawyer who inadvertently does reveal her client's confidences is protected so long as she used reasonable precautions. If a lawyer in fact knew that her offices were bugged, she would indeed be under an obligation to put up tin foil around her room or otherwise find some way to protect the privilege. But a lawyer is under no obligation to take ridiculously scrupulous precautions, like the ones suggested by Frievogel, as a general practice.

route through various unknown servers and networks, and who fail to keep abreast of emerging technologies like encryption that might make this trip more secure, are just as clearly trusting the confidentiality of their communications to a technology they do not understand and whose security is deeply questionable.

3. Uniqueness: The Limitations of Analogy

From its earliest inception, the debate over e-mail and attorney-client privilege, like all arguments about new technologies, was a debate about the applicable analogy. Indeed, the prevailing argument can be boiled down to two extremes: is e-mail like a postcard sent through the mails, visible to anyone who comes across it, or is it like a land-line phone call, interceptable but only by a dedicated, technically savvy criminal?

But the battle over e-mail has largely been about the inadequacy of these competing analogies and the failure by the ABA and other ethics boards to recognize the problems with trying to analogize new media to old. This is not a problem limited to e-mail and the attorney-client privilege, of course, because the Internet has been peculiarly besieged by inadequate analogical arguments.[111] This is probably because the Internet is no one particular medium; rather, it is a composite of media, all of which have their old-media predecessors. The static web page resembles a newspaper, streaming media compares to radio and television, online bulletin boards equate to their real-time counterparts, etc. The problem with trying to pigeonhole e-mail is the classic challenge of trying to detect the elephant blindfolded—it all depends on which part you examine. E-mail has the transparency of a postcard to anyone with access to the network server over which it passes, but for someone to have that kind of access she either belongs there (a system administrator) or most certainly does *not* belong there (a hacker), in which case the barriers to her access seem awfully similar to those between the wiretapper and the phone line.

---

[111] *See* Wallace & Green, *supra* note 40, at 720 (discussing analogical challenges of the Internet).

Admittedly, e-mail has certain similarities to land-line phone calls.[112] Both traditionally are communicated over a physical line that is outside the control of the sender (we have as little control over the physical phone lines for calls as we do the networks for e-mail) and both are compromised only by someone who is particularly technically gifted and armed with the appropriate tools. But e-mail is also different in several significant and material respects, particularly with regard to the lack of dominion and control that we have over an e-mail once it leaves our computers. Although a phone caller does not have any physical control over the telephone wires upon which her call is transmitted, we do have recognizable, identifiable carriers whose responsibility it is to maintain and control those lines. The "telephone company," whatever corporate entity that is, has dominion over those telephone wires, and any failure to maintain security over the wires is either the result of someone who physically intrudes on the wire or who compromises the entity itself. With the Internet, though, we do not send our e-mails over identifiable agencies, we do not get to control who it is that will forward our messages, and there is no one entity that is responsible for the accurate, safe transmission of our messages.[113] Moreover, when you place a telephone call, you establish an actual, exclusive connection between two points through which the communication travels, while e-mail messages travel an unforeseeable path with stops along the way. The proper analogy is not to our familiar phone system, but to an imaginary phone system that outsources all control over maintenance and security to various unknown entities, and has a virtually untraceable and unpredictable routing system for all calls.[114]

---

[112] ABA Opinion, *supra* note 5, at Intro.

[113] Although we can ultimately trace back the path that an e-mail takes, current technology does not allow us to predetermine that path.

[114] Mainstream Internet analogies proposed by e-mail friendly commentators seem to try to smooth over the Internet routing process, preferring to see it as an anonymous, mechanical process in which no human being has access to the confidential material. In contrast, like the analogy described above that takes into account the practical implications of sending an e-mail through the Internet, Winick compares Internet e-mail to "a postal system that opened, copied, and stored every letter as it passed through each post office or delivery station along the letter's route." Winick et al., *supra* note 44, at 1245.

Indeed, a far more applicable analogy is to compare e-mails to wireless phone calls using portable, cellular, or mobile digital technology.[115] Some commentators and state ethics boards have tried to distinguish cellular calls on the ground that they are broadcast,[116] which seems to be almost a facetiously literal distinction, like saying that newspapers are different from web pages because, well, they are published on paper. Differences in the inherent physical nature of two given media are important, but even more important are the similarities in the fundamental communicational dynamic: messages on both media are cast outside of the sender's control into an environment in which they are vulnerable to interception, they can only be compromised by someone with serious technical knowhow and the proper equipment,[117] they are protected by federal statutes from interception,[118] and they can be protected from interception through encryption technology.[119] Indeed, the major difference between the technologies is that the ABA has officially endorsed attorney use of unencrypted e-mails, but it has declined to render an opinion on wireless phones.[120] Numerous state ethics boards, though, have officially discouraged the use of wireless phones for confidential communications.[121]

---

[115] *See* Harris, *supra* note 88, at 402 (making the comparison between cellular phones and e-mail); Hricik, *supra* note 3, at 484 (discussing vulnerability of cellular phone calls).

[116] Miller, *supra* note 88, at 622 (drawing distinction between the Internet and cell/cordless phones because e-mail is not sent through public airwaves).

[117] *See* Wendy R. Leibowitz, *Cell, Cordless and Digital Phones Raise Privilege, Privacy Questions*, NAT'L L.J., Aug. 25, 1997, at B20; Auslander, *supra* note 53, at 5 ("Intercepted cell phone calls are instantly comprehensible, and current cell phone technology is highly susceptible to interception. Calls are broadcast on radio signals that can be picked up by other cordless phones, radios, even baby monitors.").

[118] *See* 15 U.S.C. § 5701 (1994).

[119] Hricik, *supra* note 3, at 485 (noting that improvements in cell technology might obviate privacy concerns).

[120] ABA Opinion, *supra* note 5, at § B.3; *see also* Auslander, *supra* note 53, at 3 (noting that Formal Op. No. 99-413 discussed cell phone use, but it declined to give an opinion).

[121] *See* Mass. Ethics Op. No. 94-5 (1994); N.H. Ethics Op. No. 1991-92/6 (1992); N.Y. City Bar Ass'n Op. No. 1994-11 (1994); N.C. Op. 215 (1995); Iowa Ethics Op. No. 90-44 (1994). In *United States v. Mathis*, the court held that a client's cordless phone conversation with his attorney was not protected, finding that the client could not have a reasonable expectation of privacy over a cordless phone. 96 F.3d 1577, 1583 (11th Cir. 1996).

The only practical justification for this distinction must be not in the security of the technology—they are equally secure or insecure, depending on your perspective—but in the penetration and complexity of the technology. Lawyers have a greater understanding of cellular phone vulnerabilities because the technology is more intuitive and familiar (i.e., lawyers understand the concept of broadcasting better) and there have been some high profile cases of interception that have acted as warnings.[122] But if we are to draw an analogy between e-mail and any other medium, wireless phones are a great deal closer to the mark than the land-line phones that have served as a point of comparison for the ABA and many state ethics boards.

Moreover, we have to begin recognizing that not all e-mail is transferred over traditional land-based telephone wires. The technology develops much more quickly than the law review editing process, so any article (including this one) addressing the "state of the art" is outdated by the time it is published. So virtually everything written to this point assuming that e-mail travels over land-based wires has to be re-evaluated to adjust for the explosion of wireless e-mail communications through BlackBerrys, hand-held wireless devices, such as the Palm personal digital assistant, and now even cellular phones.[123] Quickly, the consensus built around the analogy between e-mail and land-based phones now has to account for the probability that many of the attorney-client e-mails will be sent or retrieved through the air. And in many of those cases, one party or the other might not even know that her counterpart is using a wireless device and might not account for the increased security dangers. The analogy between e-mail and wireless phones, then, becomes even stronger as the technologies change.

Finally, e-mails can be differentiated from land-line phone calls in one seriously material way: the availability of an encryption option. This distinction rids the analogy of relevance because as encryption becomes an available, viable technology,

---

[122] For example, in one celebrated case, a cellular conversation with then Congressman Newt Gingrich was intercepted by a police scanner and recorded. 2 BNA Electronic Info. Pol'y & L. Rep., 151 (Feb. 7, 1997).

[123] *See* Amy Harmon, *E-Mail You Can't Outrun*, N.Y. TIMES, Sept. 21, 2000, at G12 (discussing wireless web appliances). The BlackBerry Pager is a wireless e-mail device that is continually connected to the Internet. *Id.*

there is no good reason *not* to use it. If every telephone came with automatic scrambling capable of defeating eavesdropping, attorneys would be likely to use that as well; that such technology is becoming reasonable for e-mail use practically compels attorneys to exceed the minimum requirements imposed by the ABA.

4. Conclusions

These factors—the incomplete understanding of the technology and the rate at which it would change, the uneven penetration of e-mail and encryption technologies in society, and the inadequacy of old media analogies—combine to undermine the reliability of the consensus on the no-encryption standard.[124] This consensus, and the ABA's seal of approval, gives attorneys a false sense of security in e-mail transmissions. Lawyers are, consequently, almost certainly using unencrypted e-mail for sensitive or confidential documents. Anecdotally, it is common for attorneys who are under tremendous time pressures to work on documents from home, and it is much easier to simply e-mail an attached document back and forth from office to home than it is to constantly worry about saving it to disk and carrying it around.[125] Even though encryption in those cases would be fairly simple, since the attorneys are generally using the same two computers and could easily install the appropriate software on both, lawyers have been lulled into believing that encryption is not necessary. That is to some extent a misreading not only of the ABA opinion, but also the cautious warnings made by most commentators on this issue, who have rejected a bright-line encryption standard

---

[124] At the very least, the absence of judicial guidance and the somewhat conflicted viewpoints expressed in academia and by ethics boards leads to some concern that the standards expressed in what I have called this "consensus" are in fact unreliable. One commentator noted that the lack of judicial authority on e-mail security, and the body of commentary warning of it, has itself "created a sense of unease regarding the use of e-mail for privileged and confidential communications." Harris, *supra* note 88, at 395-97. The uncertainty continues to the present day.

[125] *See, e.g.*, Rebecca Porter, *Technology Bloat? Become a 'Thin' Client*, 36-May TRIAL 92 (May 2000) (reporting that lawyers will often simply e-mail documents from their offices to their home to work on them there and save the time of saving the document to disk).

while still recommending encryption for particularly sensitive information.[126] While some lawyers might actually be following this advice in practice, encrypting particularly sensitive information or otherwise avoiding transmitting it through e-mail,[127] the ABA's opinion has still created blind assumptions among the profession that e-mail is generally safe.

Consequently, any lawyer, or anyone who has a friend who is a lawyer, is aware of the standard protection most law firms now provide for e-mail, a disclaimer appended to the bottom of every message, regardless of whether the e-mail is a privileged communication, a private letter between friends, or the umpteenth reiteration of some virus hoax or hoary joke: "The information contained in this e-mail message may be privileged, confidential, and protected from disclosure. If you are not the intended recipient, any dissemination, distribution, or copying is strictly prohibited. If you think that you have received this e-mail message in error, please e-mail the sender . . . ."[128] That disclaimer, also familiar to anyone who has received a facsimile from a lawyer in the last five years, is for the most

---

[126] Hricik, *supra* note 3, at 507 (agreeing that encryption might sometimes be appropriate); Simon, *supra* note 89, at 540-41 (saying that encryption is a reasonable alternative). Oddly, even the proponents of the no-encryption standard recognize that there are times when particularly important or confidential information should not be sent via non-encrypted e-mail. But that argument seems to concede the point at issue: when we discuss protecting the attorney-client privilege, we are certainly not especially worried about an e-mail between lawyer and client planning, say, the menu for lunch, or setting up a schedule of meetings. Obviously, trivial communications between attorney and client need not be encrypted because the privilege only applies narrowly to protect information exchanged in confidence to obtain counsel. *See* Fisher v. United States, 425 U.S. 391, 403 (1976) (holding that the attorney-client privilege only holds secret communications made in confidence to a lawyer to obtain legal counsel); *see also* United States v. Kovel, 296 F.2d 918, 922 (2d Cir. 1961). Conceding that truly important information should be encrypted gives away the argument, unless you are willing to say that some client confidences are more important than others.

[127] *See* Annemarie Franczyk, *Play it Safe to Keep E-Mail Secrets*, BUS. FIRST BUFFALO, May 15, 2000, at 37 (interviewing a lawyer who restricts "electronic correspondence to noncritical matters").

[128] E-mail from Joshua M. Masur, attorney, Heller Ehrman White & McAuliffe, to Joseph W. Rand, Instructor of Law, Brooklyn Law School (Oct. 4, 2000, 19:13.01 EST) (on file with author). The message was part of our correspondence on issues relating to e-mail security, none of which, of course, contained any confidential information. The irony that the automatic disclaimer was placed on messages describing the inherent inadequacy of the automatic disclaimer for protecting the privilege was not lost on us.

part the extent of security most attorneys put on their e-mail communications.[129] Although there are no published studies to date on the e-mail habits of attorneys, anecdotal evidence suggests that most attorneys rely on the consensus reached by state ethics boards and the ABA that encryption is not a necessary security precaution.[130]

One of the arguments in favor of the no-encryption standard, of course, is that the whole issue is a lot of smoke without any real fire, considering that there are no reported instances of actual e-mail interception and no courts that have even been called upon to weigh in on the issue.[131] But we have to remember that Internet e-mail, for all its ubiquity, is still a nascent medium, one that for practical purposes did not exist even five years ago; it is not surprising that disputes have not yet developed sufficiently to require judicial resolution, especially considering the pace of judicial response to technological change.[132] Moreover, arguments that there have been no published reports of interception are unpersuasive. Neither party to an e-mail interception has an incentive to report the incident because the victim has suffered a breach in security and potentially committed an ethical violation while the interceptor has potentially committed a crime.[133] Indeed,

---

[129] Eric G. Kraft, *The Increasing Use of the Internet In the Practice of Law*, 69 J. KAN. B.A. 15, Feb. 2000, at 19 (offering disclaimer as a protection for e-mail messages).

[130] As part of my research on this issue, I contacted a number of attorneys at law firms in New York and San Francisco, as well as litigation support specialists at several large law firms, and I found that none of them routinely encrypted Internet e-mail. *See, e.g.*, E-mail from Curtis E. A. Karnow, lawyer and author, to Joseph W. Rand, Instructor of Law, Brooklyn Law School (Oct. 5, 2000, 11:54.14 EST) (on file with author) ("It may be when encryption is as simple as clicking on a button that not using it will appear unreasonable; but right now that's not the case . . . . No lawyer I know does that.") [hereinafter Karnow e-mail]; E-mail from Christopher Corey, Systems Administrator, to Joseph W. Rand, Instructor of Law, Brooklyn Law School (Nov. 8, 2000, 19:56.36 EST) (on file with author) (indicating that firms generally do not use encryption for e-mail).

[131] Karnow e-mail, *supra* note 130 (indicating that a survey of a group of lawyers at a convention revealed that no one had heard of instances of e-mail interception).

[132] *See* KARNOW, *supra* note 22, at 5 ("Of course, the law is *always* 'behind the curve,' in a sense, regardless of the industry involved and regardless of the area of law.")

[133] LAWSON, *supra* note 62, at 222 (asserting that e-mail interception is more likely than lawyers think). Lawson also argues that e-mail tampering is a difficult crime to detect, leaving behind little physical evidence. LAWSON, *supra* note 62, at

actual cases regarding waiver of privilege of any type are unusual, and most cases involve accidental disclosures during document productions.[134]

At some point, though, there will come a test case. A lawyer's e-mail to her client is going to be inadvertently disclosed, either through interception or through misdirection, and her opponents are going to argue waiver of the privilege. When that happens, the court, like Judge Hand in *The T. J. Hooper*, might not be particularly satisfied if the only defense to the waiver is the argument that the lawyer was following the prevailing custom that security precautions were unnecessary.

III. ATTORNEY-CLIENT COMMUNICATION OVER THE INTERNET

The problem with the no-encryption standard is not just that it lulls attorneys into thinking that their e-mail communications with clients are safe and secure. Rather, the more pernicious result is that the consensus on e-mail sets a standard that might become the default rule for new information technologies on the Internet. Without a court deciding a case, attorneys and ethics boards might coalesce around the position that the Internet is an inherently safe medium because the most visible Internet application has been declared secure enough. Indeed, standards, once affixed, are difficult to dislodge, and any caveats or disclaimers are soon forgotten. The Supreme Court, for example, ruled in *Reno v. ACLU*[135] that

---

222.

[134] *See infra* Part III.B.

[135] Reno v. ACLU, 521 U.S. 844 (1997). The Supreme Court relied on facts adopted by the district court, which were based on stipulations of the parties and hearings in early 1996. Thus, the Court's opinion a year later was essentially decided on mid-1996 technology. *Id.* at 849 (indicating reliance on extensive findings of fact). The district court even had identified the types of communications technologies available at the time: one to one messaging, such as e-mail; one to many messaging, such as a listserv; distributed message databases, such as newsgroups; real time communication, such as chat; real time remote computer utilization, such as telnet; and remote information retrieval. ACLU v. Reno, 929 F. Supp. 824, 851 (E.D. Pa. 1996), *aff'd*, Reno v. ACLU, 521 U.S. 844 (1997). By the time of the Supreme Court's *Reno* decision, though, the technology of the Internet had advanced significantly due to the commercial explosion of Internet-based commerce. For example, streaming technology is not mentioned in the opinion, but by 1998 it was the focus of a great deal of commercial development. *See* William M.

the Internet should receive the highest First Amendment protections applicable to print media, not the lower protections applicable to radio or television. *Reno* was decided when Internet technology was decidedly newsprint-like, with its static web pages, e-mail media, and bulletin boards, but the holding will likely persevere despite the technological innovations, like streaming audio and video, that make the Internet look much more like broadcast media.[136] The same dynamic might hold for the no-encryption standard: if e-mail is safe, then all the other document transmission technologies becoming available might also automatically be considered safe without any sort of independent review by lawyers too technologically awkward to, in their minds, re-open the issue of Internet security.

This Part discusses the legal standard to which lawyers should be held in protecting the attorney-client privilege in light of these technological changes, starting with a brief look at some of the information and communications technologies lawyers are starting to use on the Internet and concluding with the development of a standard for assessing precautions lawyers should take in implementing these new technologies.

A. *The New Internet Communication Technologies*

The Internet is going to revolutionize the practice of law, both in the way that attorneys share, retrieve, store, and manage information, and in the ways they communicate with each other and with clients. Throughout this Article, I have been predominantly discussing e-mail technology, which is clearly the dominant method of file sharing and communication now available on the Internet. Indeed, e-mail may maintain that position for years, considering its various advantages in universality and ease of use. But there are other technologies that lawyers are already starting to integrate into their practices.

Bulkeley, *Radio Stations Make Waves on the Web*, WALL ST. J., July 23, 1998, at B1 (discussing development of netcasting).

[136] Student commentary following the decision made this point: "Several ongoing technological developments may affect the Court's conclusions regarding whether the Internet can be constitutionally regulated. The Internet is increasingly becoming more akin to radio and television." Note, *Indecent Speech—Communications Decency Act*, 111 HARV. L. REV. 329, 336 (1997).

1. Document Sharing and Storage

The new technological leap that lawyers are taking is in the management and storage of documents and information on the Internet. Lawyers have long used databases and intranets to store and share documents, but Internet technology is spurring superior methods of handling information. Lawyers are now being inundated with new commercial services called Application Service Providers ("ASPs") that will allow them to move more of their practices onto the Internet.[137] ASPs are Internet-based services that provide technical assistance for such mundane tasks, such as law firm accounting, billing, payroll, and office administration, and for such critical functions, such as case management, document assembly, document production, and legal research.[138]

The most significant type of ASP for purposes here is the online document repository, which is a third-party vendor that establishes a centralized, secure Internet site containing all case data.[139] For example, CaseCentral, Inc., one of the most well-known Internet-based document repositories, sets up such sites for individual litigation cases, particularly in situations involving multiple law firms or clients.[140] The individualized web site may contain transcripts of all hearings, depositions, or trial testimony, electronic scans of evidentiary documents, images of all exhibits, and databases containing internal mem-

---

[137] Robert J. Ambrogi, *ASPs Zero in on the Legal Market*, 43 RES GESTAE 25 (Apr. 2000). Ambrogi quotes the online resource "Webopedia" as defining ASPs as "third-party entities that manage and distribute software-based services and solutions to customers across a wide area network from a central data server." *Id.*; *see also* William R. Friedman, *The ABA Techshow: It's Not as Geeky as You Might Think*, 9 LAW. J. 5 (May 5, 2000) (describing ASPs).

[138] Cary Griffith, *More Methods to Managing Litigation Over the Internet*, CORP. LEGAL TIMES 21 (July 2000) (identifying various ASPs); Porter, *supra* note 125 (listing legal ASPs); Noel D. Humphreys, *Advent of 'Application Service Providers' Raises Many Potential Issues*, 22 PA. LAW. 40 (Jan./Feb. 2000) (same).

[139] Chris Santella, *Does the Web Change Everything?: Traditional Trial Support Software Still Has a Large Role to Play*, N.Y.L.J., Jan. 24, 2000, at T4 [hereinafter Santella, *Trial Support Software*]. For other news articles about online document repositories, see Cary Griffith, *Some Methods to Manage Litigation on the Internet*, CORP. LEGAL TIMES, June 2000, 17, at B1; Mark Voorhees, *The Market Has Spoken*, NAT'L L.J., Nov. 29, 1999, at B10; Mark Voorhees, *It's a Web World After All*, NAT'L L. J., Nov. 1, 1999, at A22.

[140] Santella, *Trial Support Software*, *supra* note 139, at T4 (describing CaseCentral's interface).

oranda, legal research, and docketing data.[141] The interface on document repositories is a standard web-based presentation, "as Yahoo-like as possible,"[142] to allow attorneys and clients to maneuver in a familiar environment.

Law firms have also been setting up their own private web sites, called "extranets," that they share with clients, usually for a particular case.[143] An extranet site is a secure environment that provides the same types of services as an online document repository, although it is mostly used to share documents between lawyers and individual clients.[144] The advantage of extranets is that they are easier to set up and often smaller, usually linked to the main firm web page, deal- or case-specific, and useful for specific transactions and smaller litigations.[145]

The advantages of moving document repositories and case files to the Internet are obvious. Lawyers can access transcripts or exhibits from anywhere in the country or the world from a web-connected laptop, collaborators can work on drafts of documents from remote locations, and firms can save on the

---

[141] Santella, *Trial Support Software*, *supra* note 139, at T4.

[142] Libby DeBlasio, *Taking it to the Web: Online Document Repositories Offer Mobility and Cut Out the Need for Couriers, But What About Security?*, THE RECORDER S4 (Nov. 1999) (quoting an employee of CaseCentral).

[143] Chris Santella, *Clients are Calling For Extranets: Providing Superior Client Service*, 16 TEX. LAW., Apr. 24, 2000, at 12 ("[E]xtranets offer an easy-to-use, more robust alternative to e-mail.") [hereinafter Santella, *Extranets*]; Judith Flournoy, *Going Beyond E-Mail for Collaboration Tools*, LAW TECH. PROD. NEWS, Apr. 2000, at 16 (describing adoption of extranet by law firm); Clarie Barliant, *The X Factor: What Firms Do With Extranets*, N.Y.L.J., Mar. 20, 2000, at T4 (noting that Davis, Polk & Wardwell and Weil, Gotshal & Manges are setting up extranets for individual clients, tailored to the client's industry); Alan Cohen, *"Extra Efficiencies": Law Firm Extranets Bring Teamwork On-Line*, N.Y.L.J, Sept. 13, 1999, at S3.

[144] *See* Barliant, *supra* note 143, at T4. Extranets are not exactly new technology because reports on them date back to 1998. In 1998, for example, the law firm Latham & Watkins developed a system that serviced 1700 users in 13 offices from Los Angeles to Moscow. M. Sean Fosmire, *Intranets and Extranets—The Extension of Web Technology to the Distribution of Private Information*, 77 MICH. B. J. 412 (1998); *see also* Allison Manning & Stephen Roussan, *Extranets Let Lawyers Plug into 'Case Site': Web Site Enables Remote Case Management and Collaboration*, N.Y.L.J., Apr. 13, 1998, at S5. Recent reports indicate, though, that law firms have not yet adapted to the new technology. *See* Barliant, *supra* note 143, at T4 (noting in March 2000 that only "a handful of true pioneers" have taken to extranets).

[145] Cohen, *supra* note 143, at S3 (describing adoption of extranet technology by Simpson, Thatcher & Bartlett).

enormous storage and reproduction costs associated with large litigations or corporate transactions.[146] The Internet provides an ideal environment for collaboration and communication between an attorney and client because it is platform-independent, allowing users of different computer systems and applications to work together without conflicting technical standards.[147]

The major problem in implementing such technologies, of course, is providing security for the information. Although no court has ruled definitively on the security of online repositories or extranets, and no ethics board to date has considered the issue, the privilege implications would seem to be even greater than for e-mail.[148] Although this Article has argued that e-mail is not a secure medium, e-mail starts looking much safer when you compare it to the dangers of putting confidential documents on web sites. First, an e-mail, for all its inherent insecurity, is transitory and dynamic, and although copies might be saved on servers in the "store and forward" method, an e-mail is generally only (or most) vulnerable during transmission. Documents stored on a web page, though, are perpetually available in a static form, continually vulnerable if unprotected. Second, e-mails are by their nature unlikely to convey all that much information (unless of course they attach memoranda), while the types of documents put in repositories or extranets are often exactly the sorts of information lawyers do not want to make publicly available.[149]

---

[146] Santella, *Extranets*, *supra* note 143, at 12 ("[T]here's little question that repository-based solutions will one day become the status quo. A web-based system affords easy access to road warrior litigators, co-counsel working on multi-district litigations, or counsel of the same firm working from disparate locations.").

[147] Using e-mail, attorneys and clients can have difficulties working on drafts of documents because there is no central, authoritative version upon which they can all comment. Using an online document repository, though, all the users comment on the same draft. Brett A. Balmer, *Web Sites Let Lawyers Discuss Cases and Collaborate on Documents*, LEGAL TIMES (Dec. 13, 1999).

[148] Hricik, *supra* note 3, at 486 (indicating that extranet communications are private, though relying on land-based phone line distinction rather than any security protocols). Hricik's description of the technology is naturally complete only for the time period in which it was written, but he does note that some state bar associations have specifically passed on intranets. Hricik, *supra* note 3, at 486.

[149] Making the documents available to the ASPs or extranet systems administrators themselves does not endanger the privilege because courts have extended its protection to any agent of the attorney. *See* United States v. Kovel, 296 F.2d 918, 921-22 (2d Cir. 1961).

Generally, though, reports indicate that ASP's providing document repositories and firms setting up extranets are aware of these security risks and are acting accordingly to provide online documents with protections generally not extended to Internet e-mail.[150] Although early reports on extranets indicated that some firms were setting them up with simple password protections (which are easily compromised either through human error or technical expertise),[151] most established vendors provide up to three types of security protocols: login names and passwords for all users, firewalls to secure data on safe servers, and secure socket layer encryption that assures that a third party intercepting a document download gets only encrypted text.[152] Some vendors even go a step further. For example, CaseCentral gives firms login names, passwords, and digital identification cards that contain a code number that changes every sixty seconds and is synchronized with the central network; users have to enter the code to log onto the network.[153]

2. Communications

The Internet is also developing new technologies for communications in addition to the ubiquitous e-mail. The most prominent developing technology is really just a variation on an established theme—the movement to wireless Internet communications. Several popular personal digital assistants like the BlackBerry pager and the Palm VII handheld provide wireless Internet access, allowing users to access e-mail from anywhere they can access their respective networks.[154] More-

---

[150] The Internet now also has all sorts of commercial file hosting services, such as Freedrive and Click2Send, which will store, for example, twenty megabytes of information for free under a user name and password, but those files are not sufficiently protected for any sorts of confidential material.

[151] *See* Fosmire, *supra* note 144, at 414 (indicating that one firm had set up an extranet with only password protection).

[152] John C. Tredennick, *Using Extranets to Build Client Relationships*, 9/00 LAW TECH. PROD. NEWS Sept. 2000, at 12; Santella, *Extranets*, *supra* note 143, at 12 ("An extranet that lacks robust firewalls and stringent encryption measures is next to worthless.").

[153] DeBlasio, *supra* note 142, at S4. As one attorney noted, "It's probably easier—and would reap greater success—if someone illicitly seeking information were to go through a firm's trash bins in order to find documents." *Id.*

[154] *See* Harmon, *supra* note 123, at G1 (stating that lawyers, "notoriously slow

over, vendors are now offering completely wireless local area networks,[155] indicating that lawyers might soon be using extranets that are partly accessible through the wireless Internet.

Wireless technology has enormous advantages for lawyers who cannot keep a laptop plugged constantly into a land-based Internet connection. In one report, for example a litigator was defending a deposition when he realized that opposing counsel was mischaracterizing a speech given by the deponent; he wrote a quick e-mail on his handheld computer to his secretary, who e-mailed him a copy of the speech within three minutes, allowing him to clarify the record on re-direct.[156]

Wireless technology, of course, undermines completely the argument that e-mail is analogous to traditional phone calls because much business e-mail will probably, in the near future, be retrieved from a wireless device. And wireless communications are as easily intercepted as mobile phone calls, although there are indications that the new wireless appliances come standard with encryption.[157] It is likely that wireless communications would be governed by the same precaution standards as mobile phones, with encryption as a standard safety protocol.[158]

---

to embrace e-mail in the office, have become enthralled by the BlackBerry"); Chris Santella, *E-Mail on the Run*, NAT'L L. J., Mar. 20, 2000, at B8 (describing available wireless handhelds); Alan Cohen, *Wireless Wonders: Small, Light, and They Do E-Mail, Too*, N.Y.L.J., Oct. 12, 1999, at T3 (describing evolution of wireless web).

[155] Lucent is advertising a "wireless, secure 11 Mbps broadband Internet/intranet access in public hotspots: hotels (lobbies and rooms), airports (lounges and gates), shared office spaces, multi-dwelling units, convention centers, and university campuses." Lucent.com, *at* http://www.lucent.com/ins/managedservices (last visited Feb. 13, 2001).

[156] Santella, *Extranets*, *supra* note 143, at 12.

[157] The home page for BlackBerry indicates that a high-end version of its pager has an "end-to-end security system whereby all corporate e-mail remains encrypted at all points between the desktop PC and the BlackBerry handheld, meeting standard corporate security guidelines." BlackBerry Wireless Email Solution, *at* http://www.blackberry.net/overview.

[158] Another technology joining the legal mainstream is called instant messaging, which could cause many of the same types of challenges as e-mail. Instant messages pop up on the receiver's screen as they are sent, rather than being stored on e-mail servers awaiting retrieval. Ashby Jones, *When E-mail's Not Fast Enough*, NAT'L L.J., Aug. 21, 2000, at B11. Jones' article indicated that two law firms were actively using instant messaging, but through a private network, not through commercially available services like the America Online instant messaging program.

B. *The Attorney-Client Privilege and New Technologies*

The final step in the analysis is to examine what guidelines lawyers should follow in incorporating these new information technologies into their practice while still protecting the attorney-client privilege. Judge Friendly defined the contours of the attorney-client privilege for the Second Circuit in 1961, quoting a famous formulation of Wigmore's—the privilege applies:

> (1) where legal advice of any kind is sought (2) from a professional legal advisor in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived.[159]

Although that articulation seems to protect only communications by the client to the attorney, courts within the circuit (and elsewhere) have applied it to advice rendered from attorney to client, so long as the advice reflects confidential information conveyed by the client.[160]

The privilege only attaches, though, if the parties contemporaneously intended to keep the communication confidential, and have not disclosed the communication to anyone outside the privilege: "[I]t is vital to a claim of privilege that the communications between client and attorney were made in confidence and have been maintained in confidence."[161] Because the privilege impedes the search for truth by restricting the ability of courts and the public to discover all relevant evidence, courts strictly confine it within the "narrowest possible

---

Id.

[159] United States v. Kovel, 296 F.2d 918, 921 (2d Cir. 1961); *see also* United States v. Int'l Bhd. of Teamsters, 119 F.3d 210, 214 (2d Cir. 1999) (reiterating formulation); *In re* Grand Jury Subpoena Duces Tecum, 731 F.2d 1032, 1036 (2d Cir.1984) (same); 8 WIGMORE, EVIDENCE § 2290 (McNaughton re. ed. 1961); *cf.* N.Y. C.P.L.R. § 4503(a) (McKinney's 1999) (codifying the attorney-client privilege under New York State law).

[160] *See* Bank Brussels Lambert v. Credit Lyonnais (Suisse), 160 F.R.D. 437 (S.D.N.Y. 1995). Weinstein and Berger note that the rationale behind the privilege is utilitarian because it encourages full disclosure from clients who might not otherwise seek legal advice. 3 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S FEDERAL EVIDENCE § 503.03[1] (Joseph M. McLaughlin ed., 2d ed. 1997).

[161] *In re* Horowitz, 482 F.2d 72, 81-82 (2d Cir. 1973).

limits" to protect only those actual confidences,[162] and courts put the burden of proof on the party trying to apply the privilege.[163] If a party breaches the confidentiality of a privileged communication, she risks waiving this evidentiary privilege; moreover, a lawyer who fails to protect confidential communications also violates her ethical obligations, exposing her client to the substantive harm caused by the disclosure of sensitive, private information.[164]

The relevant likely situation in which an attorney might have to confront the possibility of waiving the privilege over a document would be if an Internet-based transmission was either intercepted or inadvertently disclosed to someone outside the privilege. For example, if the attorney e-mailed a privileged document over the Internet without encryption, or through an unencrypted wireless device, the attorney might risk waiver if the document was intercepted by someone who invaded the privilege.

Most examinations of the issue of the attorney-client privilege vis-a-vis e-mail have focused on the doctrine of inadvertent waiver of privilege as the legal foundation for determining whether attorneys risk the privilege by using e-mail for confidential documents. Although the Second Circuit Court of Appeals has never specifically adopted an applicable test, courts outside the circuit have taken three distinct positions in determining whether an accidental disclosure waives privilege. The

---

[162] *Id.* at 81 ("[S]ince the attorney-client privilege stands in derogation of the public's 'right to every man's evidence, . . . it ought to be strictly confined within the narrowest possible limits consistent with the logic of its principle.' ") (quoting 8 WIGMORE, EVIDENCE §§ 2192, 2291).

[163] United States v. Schwimmer, 892 F.2d 237, 244 (2d Cir. 1989).

[164] Lefcourt v. United States, 125 F.3d. 79, 84 (2d Cir. 1997) (noting that attorney is bound to protect the attorney-client privilege under applicable ethical canons). *See* New York DR 4-101; Model Rule 1.6(a) (providing that an attorney may not reveal confidential client information unless the client consents after consultation and must take reasonable steps to protect that information from unauthorized disclosure or use to protect against waiver); *see also* Auslander, *supra* note 53. There is also, though, a question as to whether an attorney who received privileged material that she knows must have been inadvertently produced has an ethical obligation to return and not use it. *See* Kondakjian v. Port Auth. of N.Y. and N.J., 1996 WL 139782 (S.D.N.Y. 1996) (asserting that attorneys have ethical duty to return inadvertently produced documents); *cf.* Am. Express v. Accu-Weather, Inc., 1996 WL 346388 (S.D.N.Y. June 25, 1996) (finding that attorney who opened package after having been notified by opposing counsel that package contained inadvertently produced privileged material violated ethical duty).

first can be termed an "automatic waiver" rule, a bright line test simply dictating that any production of a privileged communication by counsel, whether inadvertent or not, waives that privilege.[165] Proponents of this position argue that once a document has lost confidentiality, it can never regain it (the idea that one cannot "unring a bell")[166] and that the attorney-client privilege should be narrowly construed only to protect actual confidences.[167] The second test protects the privilege from any truly unintentional disclosure, on the theory that the privilege belongs to the client, not the attorney, so an act of the attorney cannot effect a waiver.[168] Under this theory, a waiver is by definition an intentional relinquishment of a right, so there can be no such thing as an "inadvertent waiver."[169]

The district courts within the Second Circuit, though, have rejected both extreme positions to adopt a sensible balancing test that provides for waiver if the party "has been so careless as to surrender any claim that it has taken reasonable steps to ensure confidentiality."[170] In determining that level of carelessness, courts examine "(1) the reasonableness of the precautions taken to prevent inadvertent disclosure, (2) the time taken to rectify the error, (3) the scope of the discovery and the extent of the disclosure, and (4) overarching issues of fairness."[171] The balancing test is consistent with the goal of the

---

[165] *See, e.g.*, Wichita Land & Cattle Co. v. Am. Fed. Bank, 148 F.R.D. 456, 457 (D.D.C. 1992); Fed. Deposit Ins. Corp. v. Singh, 140 F.R.D. 252, 253 (D. Me. 1992); Int'l Digital Sys. Corp. v. Digital Equip. Corp., 120 F.R.D. 445, 449 (D. Mass. 1988). This is probably the viewpoint on inadvertent waiver that is closest to Wigmore's own because Wigmore felt that even an unknown eavesdropper could undermine application of the privilege. *See In re Horowitz*, 482 F.2d at 81 n.9 (rejecting Wigmore's view) (citing 8 WIGMORE, EVIDENCE § 2326).

[166] *Singh*, 140 F.R.D. at 253.

[167] *See Int'l Digital*, 120 F.R.D. at 449.

[168] Georgetown Manor, Inc. v. Ethan Allen, Inc., 753 F. Supp. 936, 938 (S.D. Fla. 1991); Helman v. Murry's Steaks, Inc., 728 F. Supp. 1099, 1104 (D. Del. 1990); *In re* Sealed Case, 120 F.R.D. 66, 72 (N.D. Ill. 1988).

[169] *See* Mendenhall v. Barber-Greene Co., 531 F. Supp. 951, 955 (N.D. Ill. 1988).

[170] SEC v. Cassano, 189 F.R.D. 83, 85 (S.D.N.Y. 1999).

[171] *Id.* The Second Circuit has recognized the development of this test without negative comment, but it has not specifically adopted or applied it. In *In re Grand Jury Proceedings*, the court mentioned the four-factor test but noted that the test was limited to carelessness in document production processes; the court found the test inapplicable for a case involving a witness who answered some questions in the grand jury that implicated privileged conversations but refused to answer

attorney-client privilege to ensure full and frank disclosure because clients might not be forthcoming if they knew that a truly inadvertent disclosure, a "minor mistake by otherwise competent counsel," would result in waiver of any confidences.[172] But the rule also creates incentives for lawyers to be careful and take sufficient precautions with client confidences because an accidental disclosure might waive privilege for the reckless or careless attorney.

The district courts within the Second Circuit have applied this test in over two dozen opinions, establishing the contours of the doctrine, but most of those cases involve fact patterns that are not particularly efficacious for the issues raised by online document transmissions. Rather, the vast majority involve inadvertent disclosure during routine document productions to opposing counsel during discovery. In *Aramony v. United Way of America*,[173] for example, the defendant produced 210 boxes of documents to the plaintiff after almost 800 hours of attorney and paralegal hours of review; included within those boxes were ninety-nine privileged pages that had been missed during that review.[174] Among the privileged documents, in fact, was an especially damaging memorandum from an attorney evaluating the merit of potential claims against his client.[175] In a thorough opinion that painstakingly reviewed the document production review procedures employed by the defendant's counsel, Judge Scheindlin of the Southern District of New York found that those procedures were adequate to imply a desire to protect the privilege, making the accidental production truly inadvertent.[176] *Aramony* is but one example of the dozen or so cases that have confronted virtually the same factual situation and determined that an accidental disclosure within a large document production does not waive privilege if attorneys used established procedures for review.[177]

---

others. 219 F.3d 175, 188 (2d Cir. 2000).

[172] Bank Brussels Lambert v. Credit Lyonnais (Suisse), 160 F.R.D. 437, 443 (S.D.N.Y. 1995).

[173] 969 F. Supp. 226, 230 (S.D.N.Y. 1997).

[174] *Id.*

[175] *Id.*

[176] *Id.* at 236-37 (finding the document review procedures "extensive and rigorous").

[177] *See, e.g.*, Laquila Constr. Co. v. Travelers Indem. Co., No. 98 Civ. 5920, 1999 WL 232901 (S.D.N.Y. April 21, 1999) (finding no waiver where attorney's

Similarly, there is another line of document production cases that differs only in that the attorneys demonstrated a lack of concern about procedures, resulting in waiver. In *SEC v. Cassano*,[178] for example, defense attorneys inspected about fifty cartons of documents at the SEC's regional office to determine what they wanted produced during discovery. An experienced staff attorney for the SEC had reviewed the cartons and removed privileged documents, but defense attorneys found a 100-page draft memo prepared by the SEC staff that weighed the evidence against the defendant, provided legal

---

precautions in reviewing short 400-page file were adequate, and where discovery was in early stages); Fry v. McCall, No. 95 Civ. 1915, 1998 WL 273035 (S.D.N.Y. May 28, 1998) (finding no waiver where handwritten note was disclosed in five cartons of documents, even though note was not marked confidential); Baker's Aid v. Hussmann Foodservice Co., No. 87 Civ. 0937, 1988 WL 138254 (E.D.N.Y. Dec. 19, 1988) (finding no waiver because the defendant took reasonable precautions to segregate and review documents and only one document out of 5,000 had been inadvertently produced); United States v. United Techs. Corp., 979 F. Supp. 108, 116 (D. Conn. 1997) (finding no waiver where company inadvertently turned over one document among thousands of pages that were produced, and asked for its return as soon as it realized the mistake a few weeks later); Bank Brussels Lambert v. Credit Lyonnais (Suisse), 160 F.R.D. 437, 448 (S.D.N.Y. 1995) (finding no waiver where lawyers took normal document production precautions, including segregating documents from privileged documents, moved quickly once they realized mistake, and litigation involved over 100,000 documents); Lloyds Bank v. Republic of Ecuador, No. 96 Civ. 1789, 1997 WL 96591 (S.D.N.Y. Mar. 5, 1997) (finding no waiver where attorneys reviewed documents carefully); Hydraflow, Inc. v. Enidine Inc., 145 F.R.D. 626, 628 (W.D.N.Y. 1993) (finding no waiver after brief examination of defensible security precautions); Martin v. Valley Nat'l Bank of Ariz., No. 89 Civ. 8361, 1992 WL 196798 (S.D.N.Y. Aug. 6, 1992) (finding no waiver where sufficient precautions, only a "negligible" sixteen days passed until discovery, and only five documents out of 50,000 pages were produced); Desai v. Am. Int'l Underwriters, No. 91 Civ. 7735, 1992 WL 110731 (S.D.N.Y. May 12, 1992) (finding no waiver where document was part of a large production, precautions were taken, and defendants moved promptly); Lois Sportswear, U.S.A., Inc. v. Levi Strauss & Co., 104 F.R.D. 103, 106 (S.D.N.Y. 1991) (finding no waiver where some precautions were taken, and only a few documents were produced in large selection of documents); Strategem Dev. Corp. v. Heron Int'l, No. 90 Civ. 6328, 1991 WL 274328 (S.D.N.Y. Dec. 6, 1991) (finding no waiver where defendant took precautions, and only produced three privileged documents out of a large production); *cf.* Prescient Partners v. Fieldcrest Cannon, Inc., No. 96 Civ. 7590, 1997 WL 736726 (S.D.N.Y. Nov. 26, 1997) (finding that joint agreement on confidentiality provided that both parties respect any claim of inadvertent production and, in dicta, finding that there was no waiver anyway because attorneys took precautions to have attorney review documents, moved quickly for a comprehensive review of all productions after learning that a claim of inadvertence would be challenged, production was large in scope, and there was no reliance on the documents).

[178] 189 F.R.D. 83 (S.D.N.Y. 1999).

analysis, and discussed the strengths and weaknesses of the case.[179] Having found the document, the lawyers asked the SEC's paralegal if she would photocopy and produce it for them, and she, in turn, asked the lead counsel for his permission.[180] Without reviewing the document, the SEC attorney gave her instructions to copy it.[181] The district court found that this failure to review that particular document waived privilege because the lawyer had a specific opportunity to ensure that a privileged document was not produced and yet did nothing.[182] Numerous other cases have also resulted in waiver, where the producing attorneys did not take sufficient precautions in document review procedures[183] or where the attorneys inadvertently disclosed confidential material in a court filing.[184]

---

[179] *Id.* at 83-84. The district court understatedly commented that "[d]efense counsel understandably were very much interested in this document." *Id.* at 84.

[180] *Id.*

[181] *Id.*

[182] *Cassano*, 189 F.R.D. at 85-86. The court stated:

> The document may have been in the materials intended for production, in which case the experienced staff attorney simply overlooked it. Alternatively, the document was not there when the review was made, the attorney missed nothing, but the document was inserted into the file after the review was completed. In the latter, [the SEC] took insufficient precautions—none, so far that the record discloses—to ensure that the integrity of the boxes that had been reviewed for privileged materials was maintained . . . . Any other precautions that were taken, and there certainly were some, fade into insignificance in the face of such carelessness.

Id.

[183] *See* Liz Claiborne, Inc. v. Mademoiselle Knitwear, Inc., No. 96 Civ. 2064, 1996 WL 668862 (S.D.N.Y. Nov. 19, 1996) (finding waiver where attorney took no precautions to create privilege log and never reviewed notes for privilege); Bank Brussels Lambert v. Chase Manhattan Bank, No. 93 Civ. 5928, 1996 WL 944011 (S.D.N.Y. Dec. 19, 1996) (finding waiver where attorney took no precautions to prevent documents from falling into opposing counsel's hands, including failing to mark documents as privileged and confidential); Zurn Indus., Inc. v. J.A. Jones Constr. Co., No. 90 Civ. 1161, 1992 WL 198139 (E.D.N.Y. Aug. 3, 1992) (finding waiver where the defendant failed to take sufficient precautions by failing to inventory own records before giving the other side access); Eigenheim Bank v. Halpern, 598 F. Supp. 988 (S.D.N.Y. 1984) (finding waiver where defendants inexplicably produced same privileged document twice).

[184] *See* Local 851 v. Kuehne & Nagel Air Freight, Inc., 36 F. Supp. 2d. 127, 134 (E.D.N.Y. 1999) (finding that counsel's attaching a privileged letter to a court filing waived privilege where counsel failed to label the letter as confidential, to employ a procedure for separating confidential communications, or to adequately review documents before they left the office); United States v. Gangi, 1 F. Supp.

Unfortunately, these cases do not provide particularly helpful guidance in determining the types of precautions that attorneys should take for transmitting documents through the Internet. A different dynamic is at work: although lawyers might indeed use the Internet to facilitate document production, and any privileged material accidentally transmitted that way would be reviewed in light of those precedents, the central question addressed in this Article is whether attorneys risk waiver if they are transmitting confidences that they do *not* intend to publish to the other side. Thus, cases involving document production might establish the fundamental contours of the applicable test—particularly in the focus on the importance of adequate precautions—but they are factually inapposite.

A better ground upon which to base the analysis, in fact, comes from a different type of case, one not involving inadvertent disclosure but centering instead on the types of precautions an attorney has to take to maintain a seal of confidentiality over a communication. In *In re Horowitz*, Judge Friendly, writing for the court, held that a party had waived privilege over a set of documents that had been left with an accountant for the attorney.[185] In this instance, the accountant was not holding the records so that he could assist the attorney in their understanding, which would have brought the accountant within the privilege as an agent of the attorney.[186] Rather, Judge Friendly indicated that the attorney had placed the documents in the accountant's possession as a matter of convenience and practical necessity, to help avoid their seizure by authorities.[187] Consequently, the court found that leaving the documents in the care of someone outside the confidential relationship eliminated "whatever privilege the communication may have originally possessed, whether because disclosure is

---

2d. 256, 264, 268 (S.D.N.Y. 1998) (finding waiver where the government inadvertently produced an internal memorandum to the other side because of a long series of internal mistakes).

[185] *In re* Horowitz, 482 F.2d 72, 81-82 (2d Cir. 1973).

[186] *See* United States v. Kovel, 296 F.2d 918, 922 (2d Cir. 1961) (finding that accountant working at the direction of attorney to assist in preparation of case was agent for purposes of the attorney client privilege).

[187] *See In re Horowitz*, 482 F.2d at 74. The court indicated that the client could not store the documents at his own house, because he was selling his house to "leave for parts unknown," presumably because of the ongoing criminal investigation that spurred the grand jury inquiry. *Id.*

viewed as an indication that confidentiality is no longer intended or as a waiver of the privilege."[188]

This seems a much more analogous situation than the document production cases to the arguments that could be raised about sending privileged communications through cyberspace. Like the client in *Horowitz*, who put the documents in a position where someone outside the privilege could view them, attorneys who use Internet-based communication technologies without encryption risk loss of the privilege. As Judge Friendly stated, "It is not asking too much to insist that if a client wishes to preserve the privilege under such circumstances, he must take some affirmative action to preserve confidentiality."[189]

The inquiry, then, boils down to what type of affirmative action, or what type of precautions, an attorney has to take if using new technologies to communicate with his clients. And that brings us back to Judge Hand and the two principles articulated in *The T.J. Hooper*[190] and *Carroll Towing*.[191] In those two opinions, Judge Hand presciently established a functional two-step analysis for determining whether and how we should adapt technological changes into our practices.

The T. J. Hooper involved two tug boats that ran into high seas off the coast of Atlantic City and lost a pair of coal barges, perhaps gambling (and presaging the spirit of the environs) that they could make it through a rough patch of sea.[192] The cargo owners sued the two tug boats, arguing in part that the tug boats were not seaworthy because they were not equipped with radios and could not access weather reports, dire predictions that would have dissuaded a reasonable ship's captain.[193] At the time, few ships were equipped with radio

---

[188] *Id.* at 81.

[189] *Id.* at 82.

[190] The T.J. Hooper v. N. Barge Corp., 60 F.2d 737, 739 (2d Cir. 1932).

[191] United States v. Carroll Towing, Co., 159 F.2d 169, 173 (2d Cir. 1947).

[192] *The T.J. Hooper*, 60 F.2d at 737. This was not the only claim from the cargo owners. Judge Hand also found that the barges themselves were not seaworthy, rendering the ship owners liable: "[T]he barges were certainly not seaworthy in fact, and we do not think that the record shows affirmatively the exercise of due diligence to examine them." *Id.* at 738.

[193] *See id.* at 739. The judge concluded that "prudent masters, who had received the second warning, would have found the risk more than the exigency warranted."

equipment, even though suitable sets were available and reasonably priced,[194] but Judge Hand, writing for the Second Circuit, decided that this "general custom" was no defense to negligence:

> Indeed in most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It may never set its own tests, however persuasive be its usages. Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission.[195]

Thirteen years later came *United States v. Carroll Towing, Co.*,[196] and another sinking barge, which this time raised the issue of whether the owner had been slack in caring for his own ship by failing to maintain a presence on board.[197] Judge

---

[194] *Id.* at 739. In a brief to the court, the cargo owners argued that "it is sufficiently well known to enable this court to take judicial notice of the fact that by March, 1928, radio receiving apparatus had reached a relatively high degree of development and was to be found everywhere." HENRY M. HART, JR. AND ALBERT M. SACKS, THE LEGAL PROCESS: BASIC PROBLEMS IN THE MAKING AND APPLICATION OF LAW, 409 (William N. Eskridge, Jr. & Philip P. Frickey eds., 1994) (citing Brief of Cargo Owners at 30, The T.J. Hooper v. N. Barge Corp., 60 F.2d 737 (2d Cir. 1932) (No. 430)). Later, the brief stated emphatically, " 'He that hath ears to hear, let him hear.' We may without irreverence add to this: 'And if he has not ears to hear what is meant for him to hear, he should provide himself with them.' " *Id.* at 413 (citing Brief of Cargo Owners at 53, The T.J. Hooper v. N. Barge Corp., 60 F.2d 737 (2d Cir. 1932) (No. 430)).

[195] *The T.J. Hooper*, 60 F.2d at 740. The Judge went on to declare the sets necessary: "But here there was no custom at all as to receiving sets; some had them, some did not; the most that can be urged is that they had not yet become general. Certainly in such a case we need not pause; when some have thought a device necessary, at least we may say that they were right, and the others too slack." *Id.* at 740.

[196] 159 F.2d 169 (2d Cir. 1947).

[197] Back then, the Second Circuit's docket was apparently as heavy in sunken ship cases as it now is in drug sentencing appeals, which make for far less colorful fact narratives. The details of the incident were convoluted, but essentially the barge had been tied to several other barges in a small flotilla off the harbor in what Judge Hand called "the North River." *Id.* at 170. Unfortunately, the barges were not adequately tied together to the pier, and they broke away, damaging and sinking the "Anna C." *Id.* at 171. Evidence indicated that the tug boats could have kept the "Anna C." afloat had the owner placed someone on board who could have told them that she was taking on water. *Id.* Judge Hand thus found that the owner could recover for the damages from the ship actually becoming adrift, but not for the sinking damages that could have been averted had a representative been on board to notify the tugs that the boat was leaking. *Id.* at 172 ("[I]f the bargee had been on board, and had done his duty to his employer, he would have

Hand ruled that the owner's duty was a function of the probability that some accident might occur, the seriousness of the potential injury, and the burden of taking adequate precautions to avoid the injury.[198] Judge Hand further articulated the famous "Hand formula" for making this calculation: "[I]f the probability be called P; the injury, L; and the burden, B; liability depends upon whether B is less than L multiplied by P; i.e., whether B less than PL."[199]

This doctrine, which "played so seminal a role in the economic analysis of law,"[200] refines the first principle from *The T.J. Hooper*, the two cases providing an elegant two-part examination. First, lawyers who have access to technologies that will safeguard the privilege should be aware that their failure to keep up with the state of the art may not protect them even if they adhere to a general custom advising them that such safeguards are unnecessary. Second, in the event of mishap, their failure to take proper precautions will be reviewed in light of the severity of the eventual harm, the probability of injury, and the cost of taking more reasonable precautions.

Applied to the inquiry at hand, the test makes crystal-clear that attorneys need be careful in taking advantage of the new Internet-based information technologies. The prevailing consensus that encryption for e-mail is not necessary has evolved without any judicial settlements, relying instead on state boards and an ABA constituted largely of practicing attorneys with every incentive to both sanctify what has become a common practice among attorneys and expand the reaches of the attorney-client privilege (even while courts warn that the privilege is narrowly applied). If an attorney does use these technologies, and does suffer a breach of security resulting in exposure of confidential information, his only argument against waiver is that he understood the medium to be safe. But that custom, like the custom in *The T.J. Hooper* that radios were not obligatory, will not necessarily protect attorneys who have the poor luck to be the first guinea pigs in this par-

---

gone below at once, examined the injury, and called for help from [the tugs]. Moreover, it is clear that these tugs could have kept the barge afloat, until they had safely beached her, and saved her cargo.")

[198] *Carroll Towing*, 159 F.2d at 173.

[199] *Id.*

[200] Posner, *supra* note 11, at 513.

ticular judicial-societal experiment. Unless the attorney can point to some type of precaution, some type of action that he took to protect the privilege other than trusting the inherent chaotic structure of the medium, he is at terrible risk of losing the privilege.

Moreover, in making the initial determination as to whether those precautions are necessary, outside of the reliance on custom, attorneys will likely find that the "Hand Formula" weighs in favor of adopting safety protocols. Unquestionably, the cost of adopting security precautions like encryption is high, not just in financial terms but in the added complexity of using the new technologies. Even now, as encryption programs become cheaper and less complicated, they still add a level of complexity to any transmission. And it may seem that the probability of harm is low, in that interception of electronic transmissions is no trivial endeavor. But encryption is indeed an available technology, and attorneys should consider that those two factors pale in comparison to the extent of the injury that could result from an inadvertent waiver of the attorney-client privilege: harm to the client, harm to the case, or harm to the attorney's ethical standing. Waivers of privilege are not merely damaging, they can be catastrophic. Moreover, even if the attorney defeats an attempt to destroy the evidentiary privilege, the harm to the client through exposure of sensitive material (and the concomitant damage to the attorney-client privilege) cannot be undone. A bell may be un-rung in a court of law, but not in the outside world.

Numerous occasions exist, of course, in which attorneys need not be that scrupulous about using safety mechanisms for Internet communications. Most attorney-client communications are trivial, relating peripherally to the representation but not touching on any sensitive material. But for those occasions when an attorney is transmitting or storing information that she would not want others outside the privilege to see, she should be mindful of Judge Hand's principles on technological integration and think about how she would try to justify precautions against a potential breach in the privilege.

CONCLUSION

Complicated new technologies pose complicated new legal problems, and the Internet is an especially perplexing example. Arguments that lawyers need take no special precautions when using these new technologies fundamentally misunderstand the pace and complexity of technological change, in assuming that the Internet is a safe medium because of its inherently decentralized structure and in presuming that encryption technology will never catch up to become an available option. These arguments also seem to misapprehend the nature of the attorney-client privilege, forgetting how narrow the privilege is supposed to be and how it is an exception to the general rule that information should be admissible.

Mostly, though, it seems self-evident that if lawyers wish to use new technologies, they have an obligation to understand and use them wisely. It is one thing to rely on custom for well-established procedures, such as the document review procedures discussed in most Second Circuit inadvertent waiver cases. It is quite another, though, to rely on custom for the use of modern, dynamic, changeable technologies. If you are going to go out on the cutting edge, be mindful that it can be sharp.