



DETOURS ON THE INFORMATION  
SUPERHIGHWAY:  
*THE EROSION OF EVIDENTIARY PRIVILEGES  
IN CYBERSPACE AND BEYOND*

THOMAS F. O'NEIL III\*

KEVIN P. GALLAGHER\*\*

JONATHON L. NEVETT\*\*\*

MCI Communications Corporation, Washington, D.C.\*\*\*\*

Cite as: 1997 STAN. TECH. L. REV. 3 (1997).

[http://stl.stanford.edu/STLR/Articles/97\\_STLR\\_3/](http://stl.stanford.edu/STLR/Articles/97_STLR_3/)

I. INTRODUCTION

¶1

For over a century, the fundamental technological goal of the telecommunications industry has been to conquer time and distance. During the past several decades, telecommunications media have evolved and transmission methods, rates and volumes have increased with exponential acceleration. Regrettably, however, technological achievement has not come without a price. Almost every new technological development has been accompanied by an increase in the risk that the privacy of the communications will be compromised. As a result, these technological advancements

---

\* Thomas F. O'Neil III is Chief Litigation Counsel to MCI Communications Corporation and its affiliates. A 1982 graduate of the Georgetown University Law Center, Mr. O'Neil clerked for the Honorable Alexander Harvey II, United States District Court for the District of Maryland, and was an Assistant United States Attorney for the District of Maryland from 1986 to 1989. Until December 1995, Mr. O'Neil was a partner of Hogan & Hartson L.L.P., where he represented many individuals and corporations in high-profile administrative, grand jury, and congressional investigations of public corruption, production and distribution of drugs and medical devices, and in particular, health care fraud and abuse.

\*\* Kevin P. Gallagher is an Associate Litigation Counsel to MCI Communications Corporation and its affiliates. Mr. Gallagher graduated from the Georgetown University Law Center in 1985. Before joining MCI, Mr. Gallagher was of counsel at Hogan & Hartson L.L.P.

\*\*\* Jonathon L. Nevett is an Associate Litigation Counsel to MCI Communications Corporation and its affiliates. A 1992 graduate of the Harvard Law School, Mr. Nevett clerked for the Honorable Jay C. Waldman, United States District Court for the Eastern District of Pennsylvania. Following his judicial clerkship, Mr. Nevett was an associate with the Washington, D.C. office of Kirkland & Ellis.

\*\*\*\* The authors thank Legal Assistants William C. Beckwith and Christopher J. Calamari for their assistance in producing the article.

have eroded the sacred protections of attorney communication afforded by various common law evidentiary privileges, thereby shackling counsel seeking to represent effectively individual and corporate clients in today's global marketplace.

¶2 Following this introduction, Part II of this article presents an historical overview of the interaction between technological advances in telecommunications and concerns for privacy, focusing on the advent of the telegraph, the telephone, wireless communications, and computer networks. Part III focuses on the attorney's evidentiary privileges and the impact of technology on the protection of privileged communications. Lastly, Part IV analyzes the interaction between state ethics committee rules and the law regarding these evidentiary privileges.

## II. THE PRIVACY OF TELEPHONY AND TELECOMMUNICATIONS: AN HISTORICAL OVERVIEW

### A. *The Telegraph*

¶3 Virtually from the inception of telegraphy, the practice of electronic eavesdropping, or "wiretapping," advanced in step with communications technology. After [Samuel Morse](#) transmitted the first successful telegram on May 24, 1844, the *New York Tribune* reported that "[t]he miracle of annihilation of space is at length performed."<sup>1</sup> Encroachments upon privacy almost immediately followed suit. The notion of wiretapping is colorfully illustrated by the story of [Anson Stager](#) who, aboard a Midwestern train in 1858, grew impatient when the engine failed.<sup>2</sup> Stager asked the conductor if he would order a replacement engine from the next station if Stager were to telegraph the message for him.<sup>3</sup> When the conductor responded affirmatively, Stager "climbed a telegraph pole and lowered a wire to the ground. He thrust into the ground an iron poker from the coal stove in the coach, and tapped the end of the wire against it to order an engine."<sup>4</sup> To receive the confirming telegraph, Stager "stuck out his tongue, placed the wire upon it and received the electrical impulses."<sup>5</sup>

¶4 The ability to intercept communications made possible by technological innovation had profound economic, political and sociological consequences. George Ellsworth, a Southern telegrapher who served with [General John Morgan](#), a confederate cavalry leader during the Civil War, was renowned for his ability to tap into Union lines.<sup>6</sup> Ellsworth often obtained valuable information from orders he overheard after capturing a telegraph office and "cleverly impersonating the distinctive style of the sending of

---

<sup>1</sup> [GEORGE P. OSLIN](#), THE STORY OF TELECOMMUNICATIONS 33 (1992).

<sup>2</sup> *Id.* at 68.

<sup>3</sup> *Id.*

<sup>4</sup> *Id.*

<sup>5</sup> *Id.*

<sup>6</sup> *Id.* at 124-5.

some Union operator.”<sup>7</sup> Ellsworth would then “send misleading reports and orders, signing the names of Northern generals and causing great confusion.”<sup>8</sup> Interception of telegrams was such a threat that the Union army began using cipher codes to encrypt messages; only generals and the War Department possessed the codes.<sup>9</sup>

¶15 Clandestine surveillance of telegraphy continued apace into the twentieth century. The United States declared war against Germany in World War I after the British deciphered a message from Germany promising Mexico three American states if Mexico joined the war.<sup>10</sup> The [National Security Agency](#) during that period assumed responsibility for cracking codes used by foreign governments.<sup>11</sup> The threat of interception also caused companies such as [Western Union](#) to develop encryption systems during World War II.<sup>12</sup> For example, Western Union’s *Telekrypton* system was used for communication among Allied governments.<sup>13</sup>

### B. The Telephone

¶16 The genesis of the telephone in 1876<sup>14</sup> marked the first time that the human voice could be transmitted over a long-distance. The potential applications and ramifications of this technological breakthrough were staggering and predictably created powerful new incentives for interception. Many of the earliest telephone subscribers owned what is today termed a “party line”; that is, in rural communities several households often shared one telephone line and calls to individual households were distinguished by distinctive ring patterns. The party line enabled neighbors to intercept conversations simply by picking up the telephone. Journalists of the late nineteenth century surreptitiously listened to each other’s telephone discussions in order to “scoop” a story.<sup>15</sup>

¶17 By 1895, New York City police officers routinely conducted wiretaps.<sup>16</sup> “A loose arrangement existed between the New York police and the telephone company whereby the telephone company cooperated with the wiretapping practices of the police department.”<sup>17</sup> After a state legislative committee revealed these practices, a Detective Sergeant testified that the

---

<sup>7</sup> *Id.* at 125.

<sup>8</sup> *Id.* Ellsworth’s conduct is strikingly similar to the modern concept of “spoofing,” whereby an impostor computer intercepts a message and responds as the intended recipient. *See* discussion at Part II(D) *infra*.

<sup>9</sup> *Id.*

<sup>10</sup> *Id.* at 289.

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> *Id.*

<sup>14</sup> On March 7, 1876, [Alexander Graham Bell](#) received a patent for the telephone, called “probably the most valuable patent ever issued.” *Id.* at 219.

<sup>15</sup> RICHARD F. SCHWARTZ & ROBERT E. KNOWLTON, *THE EAVESDROPPERS* 25 (1971).

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

police had monitored confidential conversations of lawyers.<sup>18</sup> The detective elaborated, stating that the objective of monitoring counsel was to ascertain the location of their clients. Significantly, the confidential nature and source of the evidence gathered from such wiretaps was not disclosed to his superiors. While most of the newspaper reports of wiretapping in the early twentieth century related to the interception of stock information, no one was immune from electronic surveillance. In 1916, the Mayor of New York was caught tapping the phones of Catholic priests to gather evidence for a special New York commission investigating charity frauds.<sup>19</sup>

¶8 Tapping a telephone line today is a relatively simple endeavor.<sup>20</sup> In fact, magazines for telephone hackers (“phrackers”)<sup>21</sup> publish lists of locations where handsets similar to those seen on the utility belts of telephone repairmen may be purchased for as little as two hundred dollars.<sup>22</sup> Once armed with a handset, a phracker can connect it to the twisted pairs of copper wire readily available in basements, attics, on telephone poles, or in maintenance tunnels enabling the interception of telephone conversations.<sup>23</sup> Simple recording devices available from retail electronic stores allow the phracker to tape the discussions.<sup>24</sup>

### C. *Wireless Communications*

¶9 While the development of the wireless telephone, or “radiotelephone,” early in this century marked the advent of wireless telephony, only in the past decade has this technology become widely available to the general populace. The harnessing of the radio spectrum for wireless mass communications evolved from cordless telephones to paging systems and cellular telephones.

¶10 Cordless telephones consist of a base transmitter wired to a landline and an electrical source that transmits an AM or FM signal to a hand held “roamphone.”<sup>25</sup> The analog<sup>26</sup> signal is transmitted from the base unit through the telephone network like a regular call. The technology of a cordless telephone parallels that of a standard AM or FM radio. In fact, the radio signals transmitted between the handset and the base unit can be

---

<sup>18</sup> *Id.* at 26.

<sup>19</sup> *Id.*

<sup>20</sup> William Freivogel, *Internet Communications - Part II: A Larger Perspective*, ATT’YS LIABILITY ASSURANCE SOC’Y LOSS PREVENTION J., Jan. 1997, at 2.

<sup>21</sup> See, e.g., *Phrack*, (visited Oct. 1, 1997) <<http://www.fc.net/phrack.html>>.

<sup>22</sup> Freivogel, *supra* note 20, at 2.

<sup>23</sup> *Id.*

<sup>24</sup> E.g., *Radio Shack* sells a microphone/suction cup that attaches to the receiver of a handset and transmits sound to a tape recorder or dictation recorder by wire. Radio Shack, Cat. No. 44-533B.

<sup>25</sup> S. Rep. No. 99-541, at 9 (1986).

<sup>26</sup> “Analog” is a transmission method that uses a continuous electrical signal that varies in amplitude or frequency in response to changes in sound impressed on a transducer in the sending device. HERB KIRCHOFF, *TELECOM LINGO GUIDE* 9 (7th ed. 1994); HARRY NEWTON, *NEWTON’S TELECOM DICTIONARY* 42 (12th ed. 1997).

intercepted by ordinary AM radios, as well as other cordless phones, baby monitors, and other devices. Cellular telephones operate similarly, but use a different portion of the radio spectrum. In 1981, the [Federal Communications Commission](#) approved the use of a specific range of the radio spectrum for cellular communications.<sup>27</sup> Some fifteen years later, over forty-five million Americans use cellular phones.<sup>28</sup>

¶11 Public awareness of wireless communication's exposure to interception has increased with its popularity. As the recent incident involving the Speaker of the United States House of Representatives so clearly illustrated,<sup>29</sup> the fact that mobile base stations transmit and receive signals at a frequency within the FM and VHF range of the radio spectrum<sup>30</sup> makes cellular conversations particularly vulnerable to scanners.<sup>31</sup> Emergent technologies like radio-based paging systems, low-earth orbit ("LEO") satellites, and, in particular, Personal Communication Services ("PCS") have attempted to address certain security issues associated with analog cellular telephones.

¶12 PCS is currently the most advanced cellular technology. A digital cellular<sup>32</sup> service, PCS offers better quality and new combinations of products and capabilities, including number portability.<sup>33</sup> It is estimated that

---

<sup>27</sup> Patricia M. Worthy, *The Impact of New and Emerging Telecommunications Technologies: A Call to the Rescue of the Attorney-Client Privilege*, 39 HOW. L.J. 437, 470 n. 186 (1996); see Christine E. Ene-mark, *Adarand Constructors, Inc. v. Pea: Forcing the Federal Communications Commission into a New Constitutional Regime*, 30 COLUM. J.L. & SOC. PROBS. 215, 218 (1997).

<sup>28</sup> John Markoff, *Code Set Up to Shield Privacy of Cellular Calls Is Breached*, N.Y. TIMES, Mar. 20, 1997, at A1.

<sup>29</sup> On or about December 21, 1996, a conversation between Speaker [Newt Gingrich](#) (R-Ga.), Representative [John Boehner](#) (R-Ohio), and other Republican leaders regarding the [House Ethics Committee investigation](#) of the Speaker was intercepted by a scanner purchased from Radio Shack by a Mr. and Mrs. John Martin. The Martins intercepted the cellular telephone transmissions of a vacationing Representative Boehner, as his car was parked at a Lake City, Florida restaurant. The Martins taped the conversation and turned the tape over to Representative [Karen Thurman](#) (D-Fla.), who released the tape to the media. Mike Williams, *Couple Fined \$1,010 for Taping Gingrich Call*, ATLANTA J.-CONST., Apr. 26, 1997, at A3. The couple violated FCC Prohibition Against Eavesdropping, [47 C.F.R. § 15.9](#) (1996). Section 15.9 provides that

"Except for the operations of law enforcement officers conducted under lawful authority, no person shall use, either directly or indirectly, a device operated pursuant to the provisions of this part for the purpose of overhearing or recording the private conversations of others unless such use is authorized by all of the parties engaging in the conversation." *Id.*

<sup>30</sup> The FCC has allocated channels between 800 MHz and 900 MHz for block assignment in the Cellular Radiotelephone Service, with channels having a bandwidth of 40 KHz. [47 C.F.R. § 22.905](#) (1995).

<sup>31</sup> Individuals who scan the cellular frequencies use either sophisticated devices like those employed by police to monitor 911 calls or easily modify radio scanners to monitor cellular conversations. Fred J. Meyer, *Don't Touch That Dial: Radio Listening Under The Electronic Communications Privacy Act of 1986*, 63 N.Y.U. L. REV. 416, 424 (1988).

<sup>32</sup> "Digital" refers to the use of a binary code, i.e., ones and zeroes, "to represent information. . . . Analog signals—like voice or music—are encoded digitally by sampling the voice or music analog signal many times a second and assigning a number to each sample." NEWTON, *supra* note 26, at 198.

<sup>33</sup> "Number portability" is defined as "the ability of end users to retain their geographic, or non-geographic telephone number when they change" either (1) their service provider; (2) their location; or (3) their service. NEWTON, *supra* note 26, at 457-8.

approximately one million Americans subscribe to a PCS.<sup>34</sup> One of the major selling points of PCS has been the vastly improved security over analog cellular phones. PCS network standards such as [Code Division Multiple Access](#) (“CDMA”) and [Time Division Multiple Access](#) (“TDMA”) were developed for this purpose.<sup>35</sup> However, [recent reports](#) that the encryption codes underlying CDMA and TDMA were cracked by a team of researchers from the [University of California at Berkeley](#) and [Counterpane Systems, Incorporated](#) have proven that claims of complete impenetrability ring hollow.<sup>36</sup> Referring to the work of the researchers who discovered the flaw in the [Cellular Message Encryption Algorithm](#) (“CMEA”) on which CDMA and TDMA are based, the President of the Cellular Telecommunications Industry Association (“CTIA”), Thomas Wheeler, recently stated that the discovery “indicates that a reliance on encryption technology to secure privacy rights is a detrimental reliance.”<sup>37</sup>

#### D. *The Internet and Intranets*

¶13

The age of the Information Superhighway—the Internet—spawned an entire generation of hackers, crackers, sniffers, and spoofers.<sup>38</sup> The development of the personal computer and high-speed modems<sup>39</sup> resulted in the linking of computer networks around the world to form the Internet. Currently, approximately 7.8 million people use the core Internet,<sup>40</sup> 13.5 million use the consumer Internet,<sup>41</sup> and 27.5 million use Internet electronic mail,

---

<sup>34</sup> Markoff, *supra* note 28.

<sup>35</sup> Code Breakers’ Achievement Derided by Industry Experts, *COMM. TODAY*, Mar. 25, 1997, at 8.

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

<sup>38</sup> A “hacker” is “[a] person who ‘hacks’ away at a computer until his program works. . . . The word [hacker] . . . has gone through many meanings. At one state it was a badge of honor conferred on an elite programmer or computer hardware designer. But in [the 1980s the term was associated with trying] to break into computer systems for fun and sport. NEWTON, *supra* note 26, at 307. A “cracker,” on the other hand, is specifically “a ‘hacker’ whose hacks are beyond the bounds of propriety, and usually beyond the law.” The person “‘cracks’ computer and telephone systems by gaining access to passwords, or by ‘cracking’ the copy protection of computer software.” *Id.* at 169. A “sniffer” is a “program that monitors all traffic on a network and reports on problems on the network.” *Id.* at 597. A “spoofers” is someone who “attempt[s] to gain access to an automated information system by posing as an authorized use.” *Id.* at 607. See also [Robert L. Jones](#), *A Lawyer’s Duty with Regard to Internet E-Mail*, (dated August 16, 1995) (visited Oct. 1, 1997) <<http://www.gsu.edu/~lawppw/lawand.papers/bjones.html>>.

<sup>39</sup> The term “modem” is an “[a]cronym for MOdulator/DEModulator.” It “converts digital signals to analog signals and vice-versa [in order to] send data signals (digital) over the telephone network, which is usually analog.” NEWTON, *supra* note 26, at 418.

<sup>40</sup> The “core Internet” consists of interactive services like TELNET remote login, FTP, and World Wide Web hypertext. See [Cyberstats](#), *FAS Cyberstrategy Project* (last modified Feb. 21, 1996) <<http://www.fas.org/cp/cyberstat.html>>.

<sup>41</sup> The “consumer Internet” consists of commercially provided services. *Id.*

much of which is transmitted over analog telephone lines.<sup>42</sup> As Web<sup>43</sup> browsers<sup>44</sup> and service providers have opened the gates to the Information Superhighway, the world has witnessed an explosion of Internet applications and sites. Corporate America is rapidly adding new technologies such as wireless e-mail messaging and Internet videoconferencing to its communications systems. With each new technology comes a vast array of possible applications, both legitimate and nefarious.

¶14 As business and industry rely more heavily on the Internet and intranets,<sup>45</sup> security issues will assume greater importance. Authorized network users account for sixty percent of all breaches of network security.<sup>46</sup> External threats are also substantial, and misconfiguration of firewalls<sup>47</sup> (or other network devices) is probably the biggest chink in the security armor.<sup>48</sup> Moreover, for the Internet to function, network managers and server technicians must vigilantly monitor information, exposing systems to the possibility of inadvertent, as well as intentional interception.

¶15 The techniques used by crackers and spoofers range from the complex to the mundane. A spoofer, for example, may be able to obtain corporate passwords by posing as a network technician and placing a handful of targeted telephone calls to employees.<sup>49</sup> Programs that identify passwords for various types of operating systems are readily obtainable from the Internet through a Web browser word search. Indeed, anyone with knowledge of [UNIX commands](#), [Baudot code](#), [ASCII](#), terminal emulation, port scanning, TCP/IP,<sup>50</sup> or communications settings is well armed to compromise network integrity.<sup>51</sup> Furthermore, the cracker culture tends to lionize and revere the illegal acts of underground stalwarts, such as [Kevin Mitnick](#).<sup>52</sup>

---

<sup>42</sup> *Id.*

<sup>43</sup> The "Web," also known as the "World Wide Web," is a select network of computers on the Internet. NEWTON, *supra* note 26, at 729-30.

<sup>44</sup> A "web browser" is "software" which allows computer users to access documents on the World Wide Web. *Id.* at 718.

<sup>45</sup> "Intranets" are internal corporate computer communications systems based on the Internet Protocol. In essence, an intranet is an Internet-like system available only to persons with access behind the corporate firewall. *Id.* at 346.

<sup>46</sup> [Christopher W. Klaus](#), *Network Security: Anything But Bulletproof* (dated Nov. 21, 1996) (visited Oct. 1, 1997) <<http://www.data.com/tutorials/bulletproof.html>>.

<sup>47</sup> A "firewall" is a combination of computer hardware and software that permits or denies the flow of traffic into or out of a network. NEWTON, *supra* note 26, at 274.

<sup>48</sup> Klaus, *supra* note 46.

<sup>49</sup> Jones, *supra* note 38.

<sup>50</sup> The Internet uses a common protocol called [Transmission Control Protocol/Internet Protocol](#) ("TCP/IP"). TCP/IP has been defined as "a networking protocol that provides communication across interconnected networks, between computers with diverse hardware architectures and various operating systems." NEWTON, *supra* note 26, at 637 (citing definition from Microsoft's Windows for Workgroups Resource Kit). Most intranets use this protocol as well. Firewalls, routers and encryption are terms often used when TCP/IP is discussed. William P. Matthews, *Encoded Confidences: Electronic Mail, the Internet, and the Attorney-Client Privilege*, 45 U. KAN. L. REV. 273, 274 (1996).

<sup>51</sup> HUGO CORNWALL, *THE HACKER'S HANDBOOK* 8-34 (1986).

<sup>52</sup> Kevin Mitnick is considered, among other things, a hacker of telephones and telephone switching systems. *Computer Hacker Awaits Sentencing*, GREENSBORO NEWS & RECORD, Oct. 8, 1996, at B8.

and [Randal Schwartz](#),<sup>53</sup> serving to indoctrinate and motivate successive generations of crackers.

¶16

For many of the reasons outlined above, e-mail messages transmitted over the Internet and intranets are vulnerable to interception. In response to this threat, industry and standards agencies have developed five e-mail encryption protocols, or algorithms that “scramble” transmissions so they are unintelligible if intercepted.<sup>54</sup> These protocols utilize hash codes—a digital fingerprint—to authenticate messages and a system of public and private passwords (or keys) to decrypt messages.<sup>55</sup> However, a major obstacle to network-wide implementation of an encryption program is the general aversion of users to passwords and layers of security, and an equally troublesome consideration is the accessibility of private passwords.<sup>56</sup>

#### E. *The Legal Response*

¶17

The first time the United States Supreme Court authorized the use of wiretap evidence occurred in 1928, when it decided [Olmstead v. United States](#).<sup>57</sup> That case arose out of the routine wiretapping of suspected bootleggers during [Prohibition](#), and the Court narrowly upheld the Ninth Circuit’s ruling that the surveillance did not run afoul of the [Fourth](#) or [Fifth](#) Amendments to the [United States Constitution](#).<sup>58</sup> Congress finally addressed the question of eavesdropping when it enacted Section 605 of the [Communications Act of 1934](#), which severely limited the admissibility of evidence obtained from wiretaps in court proceedings.<sup>59</sup> The original 1934 version of section 605 prohibited the unauthorized interception and divulgence of any communication or the publication of the existence, contents, substance, purport, effect, or meaning of the intercepted communication to any person.<sup>60</sup> Today, section 605, as amended, exempts authorized law enforcement agents from these restrictions.<sup>61</sup> Subsequent related Congressional acts include Title III of the [Omnibus Crime Control and Safe Streets](#)

---

<sup>53</sup> A renowned PERL programmer (much of the Web was constructed with PERL) and author, Randal Schwartz was convicted in 1995 by an Oregon jury for clandestinely obtaining passwords and breaching network firewalls at Intel Corporation. Fiona M. Ortiz, *Computer Expert Convicted in Hacking* THE OREGONIAN, July 26, 1995, at D1.

<sup>54</sup> The five protocols are Secure Multipurpose Internet Mail Extensions (“S/MIME”); Pretty Good Privacy (“PGP”); PGP/MIME; MIME Object Security Services (“MOSS”); and Message Security Protocol (“MSP”). See [Ralph Levien](#), *Protecting Internet E-Mail from Prying Eyes*, (visited Oct. 1, 1997) <[http://www.data.com/Tutorials/Protecting\\_Internet\\_Email.html](http://www.data.com/Tutorials/Protecting_Internet_Email.html)>.

<sup>55</sup> *Id.*

<sup>56</sup> Private passwords must be escrowed with a third party to prevent the loss of access to data if a user is terminated or forgets the password. Matthews, *supra* note 50, at 297.

<sup>57</sup> 277 U.S. 438 (1928).

<sup>58</sup> *Id.*

<sup>59</sup> Pub. L. No. 73-416, 48 Stat. 1103 (codified as amended at 47 U.S.C. § 605 (1988)).

<sup>60</sup> *Id.*

<sup>61</sup> 47 U.S.C. § 605 (1988).

[Act of 1968](#) (the “OCCSSA”),<sup>62</sup> authorizing law enforcement to conduct wiretaps and making it illegal for non-law enforcement agents to eavesdrop on wire communications; the [Electronic Communications Privacy Act of 1986](#) (the “ECPA”),<sup>63</sup> prohibiting the interception and disclosure of any oral, wire or electronic communication by any person, as well as certain wireless communications; and the [Communications Assistance For Law Enforcement Act of 1994](#) (“CALEA”),<sup>64</sup> expanding the protection of wireless communication. Prior to the OCCSSA, there were no laws criminalizing eavesdropping.

¶18

Digital systems are subject to both private and public sector seizure. Because the federal government is concerned about its ability to eavesdrop as new technologies develop, it wishes to hold the keys to decryption. The “[Clipper Chip](#)” debate centers on the government’s desire to escrow keys that can decipher commercial digital mobile telephone conversations. On April 16, 1993, the White House announced the Escrowed Encryption Initiative, a program whereby the Attorney General of the United States requests manufacturers of communications hardware incorporating encryption to install in their products encrypting microcircuits developed by the National Security Agency.<sup>65</sup> The design of the system and the algorithm on which it is based, “[SKIPJACK](#),” are classified.<sup>66</sup> On February 4, 1994, the United States Department of Commerce approved the [Escrowed Encryption Standard](#) (“EES”) as a voluntary Federal Information Processing Standard (“FIPS”).<sup>67</sup> In addition, on February 4, 1994, [Attorney General Janet Reno](#) announced that the [United States Department of Treasury](#) and the [National Institute of Standards and Technology](#) would each retain a component of the 80-bit decryption keys unique to each encryption chip. The components of the key must be recombined in order to decrypt a message.<sup>68</sup> The Attorney General also announced a series of complex and somewhat ambiguous procedures for release of encryption key components pursuant to [Title III](#),<sup>69</sup> State Statutes, or the [Foreign Intelligence Surveillance Act](#) (“FISA”).<sup>70</sup> Hence, the development of technology is not only

---

<sup>62</sup> Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-2520 (1996)) [hereinafter Title III].

<sup>63</sup> Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522, 2703-2711 (1996)).

<sup>64</sup> Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 18 U.S.C. § 2510 (1996)).

<sup>65</sup> [White House Fact Sheet on Clipper](#) (visited Oct. 1, 1997) <[http://www.epic.org/crypto/clipper/white\\_house\\_factsheet.html](http://www.epic.org/crypto/clipper/white_house_factsheet.html)>.

<sup>66</sup> [The Government Solution: The Escrowed Encryption Standard](#) (visited Oct. 1, 1997) <[http://info.acm.org/REPORTS/ACM.CRYPTO\\_STUDY/\\_WEB/chap.7.html](http://info.acm.org/REPORTS/ACM.CRYPTO_STUDY/_WEB/chap.7.html)>.

<sup>67</sup> The program is “voluntary” in that if a Federal Agency decides that telecommunications equipment should encrypt the data it transmits, the telecommunications company can use EES or any other FIPS, although EES is preferred by the government. *See Id.*

<sup>68</sup> Attorney General Makes Key Escrow Encryption Announcements (visited Oct. 1, 1997) [http://www.epic.org/crypto/clipper/reno\\_announcement\\_feb\\_94.html](http://www.epic.org/crypto/clipper/reno_announcement_feb_94.html)>.

<sup>69</sup> Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-2520 (1996)).

<sup>70</sup> 50 U.S.C. §§ 1801-1829 (1994); *see also* [Authorization Procedures for Release of Encryption Key Components in Conjunction with Intercepts Pursuant to Title III, State Statutes, and FISA](#) (visited Oct. 1, 1997) <[http://www.epic.org/crypto/clipper/doj\\_key\\_escrow\\_procedures.html](http://www.epic.org/crypto/clipper/doj_key_escrow_procedures.html)>.

redefining security issues surrounding electronic communications, but also the degree to which government enforcement agencies maintain control over private communications.

### III. PRIVILEGED COMMUNICATIONS IN THE INFORMATION AGE

#### A. Evidentiary Privileges and Waivers

¶19 The rapid evolution of communications technology and the means of intercepting confidential discussions have created significant risks to the time-honored attorney-client privilege,<sup>71</sup> the attorney work product doctrine,<sup>72</sup> and the self-evaluative privilege.<sup>73</sup> While the manner in which lawyers and their clients communicate has evolved over time, the attendant protections have regressed as courts have grappled with the nuances of every technological stride. Consequently, before reaching for the cellular phone or sending an e-mail message, counsel and his or her client must be familiar with the latest developments in this important area.

¶20 The central question raised by the technological revolution is whether use of a certain mode of communication increases appreciably the likelihood that a court will find that an evidentiary privilege has been waived in

---

<sup>71</sup> The oldest and perhaps the most sacrosanct evidentiary shield in our jurisprudential system, the attorney-client privilege is intended to encourage clients to speak candidly with their lawyers. *Coleman v. Am. Broadcasting Co.*, 106 F.R.D. 201, 204 (D.D.C. 1985). It covers communications between a client and counsel (or an agent of counsel) if counsel is acting in a legal capacity; the communication is for the purpose of obtaining legal advice; the communication is understood to be confidential when made; and the communication is kept confidential. *Upjohn v. United States*, 449 U.S. 383, 394-95 (1981). See also *Diversified Indus., Inc. v. Meredith*, 572 F.2d 596, 608-11 (8th Cir. 1977); *United States v. United Shoe Mach. Corp.*, 89 F. Supp. 357, 358-59 (D. Mass. 1950).

<sup>72</sup> The work product doctrine protects the privacy of an attorney's work and the integrity of the adversarial process. *City of Worcester v. HCA Management Co.*, 839 F. Supp. 86, 88 (D. Mass. 1993). Enunciated in [FED. R. CIV. P. 26\(b\)\(3\)](#), the doctrine protects materials and other tangible items prepared by counsel in anticipation of litigation. See *Hickman v. Taylor*, 329 U.S. 495, 511-12 (1947); *In re Sealed Case*, 676 F.2d 793, 809 (D.C. Cir. 1982).

<sup>73</sup> The self-evaluative privilege "prevents the disclosure of confidential critical, evaluative and/or deliberative material whenever the public interest in confidentiality outweighs an individual's need for full discovery." *Wylie v. Mills*, 478 A.2d 1273, 1276 (N.J. Super. Ct. 1984). It is a qualified privilege, which was formulated in *Bredice v. Doctors Hosp., Inc.*, 50 F.R.D. 249 (D.D.C. 1970), *aff'd mem.*, 479 F.2d 920 (D.C. Cir. 1973); see also *Federal Trade Comm'n v. TRW, Inc.*, 628 F.2d 207, 210 (D.C. Cir. 1980). Those seeking to invoke the self-evaluative privilege must establish that the information resulted from a critical self-analysis performed by the party seeking the protection; there is strong public interest in promoting the "free flow" or exchange of the class of information the party is seeking to protect; the "flow" would cease if the class of information were discoverable; and the information was prepared with the expectation that it remain confidential. See *Dowling v. American Haw. Cruises, Inc.*, 971 F.2d 423, 425-26 (9th Cir. 1992); see also Note, *The Privilege of Self-Critical Analysis*, 96 HARV. L. REV. 1083, 1086 (1983).

the case of a non-voluntary disclosure of protected material.<sup>74</sup> Courts generally use one of three analyses to resolve the waiver issue. The first approach is essentially strict liability; any disclosure, even an inadvertent one, waives the privilege.<sup>75</sup> The rationale here, articulated by [Dean John Wigmore](#), is that a bell cannot be unring. In other words, once the confidential communication is disclosed or intercepted by a third party, it is no longer confidential, and the purposes of the privilege no longer can be served.<sup>76</sup>

¶21 At the other end of the spectrum is the so-called intent test.<sup>77</sup> Under this approach, the disclosure of a confidential communication cannot be deemed a waiver absent intent to waive.<sup>78</sup> This theory is grounded on the fundamental notion that a waiver requires the intentional relinquishment of a known right.<sup>79</sup> As one district judge has observed, “[i]f we are serious about the attorney-client privilege and its relation to the client’s welfare, we should require more than . . . negligence by counsel before the client can be deemed to have given up the privilege.”<sup>80</sup>

¶22 Predictably, most courts have adopted a third, more flexible test which assesses the inadvertent disclosure on a case-specific basis, considering primarily “(1) the reasonableness of precautions taken to prevent disclosure; (2) the amount of time taken to remedy the error; (3) the scope of

---

<sup>74</sup> Generally, the waiver analysis differs for each of these three privileges. Disclosure of materials protected under the work product doctrine does not automatically waive the privilege. Unlike a waiver of the attorney-client privilege, a waiver of the work product doctrine occurs only where the materials at issue are disclosed to an adversary, not merely any third party. *See Westinghouse Elec. Corp. v. Philippines*, 951 F.2d 1414, 1428 (3d Cir. 1991); *Hartford Fire Ins. Co. v. Garvey*, 109 F.R.D. 323, 328 (N.D. Cal. 1985).

Because new means of technology are arguably susceptible to interception by an attorney’s adversary, as well as by any third party, the inadvertent disclosure waiver analyses under the attorney-client privilege and the work product doctrine are the same. *See Carter v. Gibbs*, 909 F.2d 1450, 1451 (Fed. Cir. 1990) (stating that criteria for waiver of work product material and attorney-client communications are equivalent under certain circumstances); *Fidelity & Deposit Co. v. McCulloch*, 168 F.R.D. 516, 521 n. 4 (E.D. Pa. 1996) (stating that “[t]he standards governing waiver of the attorney-client and work product privileges through inadvertent disclosure are essentially the same.”); *Hartford Fire Ins. Co.*, 109 F.R.D. at 328 (stating that the difference between waiver of attorney-client and work product privileges disappears in the case of disclosure to adversary).

While the law relating to the waiver of the self-evaluative privilege has yet to crystallize, the analysis would most likely mirror that of the attorney-client privilege and the work product doctrine in the case of inadvertent disclosure. *See In re Wilkie Farr & Gallagher*, No. M8-85(ISM), 1997 WL 118369, at \*2 n.1 (S.D.N.Y. Mar. 14, 1997) (stating that the waiver of the attorney-client privilege applies equally to materials covered by the self-evaluative privilege).

<sup>75</sup> *See, e.g., In re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989). *See also* 8 JOHN H. WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW 2290 (J. T. McNaughton ed., 1961).

<sup>76</sup> *See Underwater Storage Inc.*, 314 F. Supp. 546, 549 (D.D.C. 1970) (stating that “[w]here the policy underlying the rule can no longer be served, it would amount to no more than mechanical obedience to a formula to continue to recognize it.”) (quoting *United States v. Kelsey-Hayes Wheel Co.*, 15 F.R.D. 461, 465 (E.D. Mich. 1954)).

<sup>77</sup> *See, e.g., Mendenhall v. Barber-Greene Co.*, 531 F. Supp. 951, 954 (N.D. Ill. 1982).

<sup>78</sup> *See Georgetown Manor, Inc. v. Ethan Allen, Inc.*, 753 F. Supp. 936, 938 (S.D. Fla. 1991); *Helman v. Murray’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).

<sup>79</sup> *Mendenhall*, 531 F. Supp. at 955.

<sup>80</sup> *Id.*

discovery; (4) the extent of disclosure; and (5) the overriding issue of fairness.”<sup>81</sup> This analysis focuses on the measures taken to preserve the privilege; accordingly, the failure of a lawyer or a client to take reasonable precautions constitutes a waiver, even where the disclosure is inadvertent.<sup>82</sup>

¶23

In applying this multi-pronged formula, courts rely heavily on analogous [Fourth Amendment](#) principles. Typically, the pivotal issue is whether the communication enjoyed a reasonable expectation of privacy under the standard the United States Supreme Court enunciated in *Katz v. United States*,<sup>83</sup> where the Court excluded evidence obtained from an electronic surveillance device placed on a telephone booth as an unconstitutional search and seizure. Interestingly, the *Katz* decision marked the first time that the Supreme Court recognized a reasonable expectation of privacy for telephone conversations. [Fourth Amendment](#) cases, such as *Katz*, however, do not provide sufficient guidance to assure lawyers of the outcome of privilege-waiver cases. The vagaries of the waiver analysis, combined with the explosion of technology, have caused palpable apprehension on the part of clients and lawyers alike as to how and when to communicate safely. In this era of cellular phones, pagers and e-mail, this apprehension can in many circumstances impinge on effective legal representation.<sup>84</sup>

#### B. *The Impact of Technological Advances on Privileged Communications*

¶24

Wireless telephones and e-mail have become essential modes of attorney-client communication. The advent of these technologies has undeniably increased the speed with which counsel and clients communicate. Attendant to the development of these media has been the concern that security and privacy have been sacrificed at the expense of convenience.

##### 1. *Cordless and Cellular Telephones*

¶25

The need for mobile communications drove the development of cordless and cellular telephones. Like their colleagues in various professional arenas, attorneys often need to communicate while outside the office. For example, confidential and time-sensitive information often must be exchanged by way of a cordless telephone from a home or a cellular telephone in an automobile. Today's global economy and legal dilemmas simply do not afford counsel the luxury of returning to the office to communicate privileged information over conventional wireline telephones.

---

<sup>81</sup> [Alldread v. City of Grenada](#), 988 F.2d 1425, 1433 (5th Cir. 1993).

<sup>82</sup> See *Alldread*, 988 F.2d at 1434; *Transamerica Computer v. Int'l Bus. Mach.*, 573 F.2d 646 (9th Cir. 1978); *Bank Brussels Lambert v. Credit Lyonnais*, 160 F.R.D. 437, 443 (S.D.N.Y. 1995); *Fed. Deposit Ins. Corp. v. Marine Midland Realty Credit Corp.*, 138 F.R.D. 479, 482 (E.D. Va. 1991).

<sup>83</sup> [389 U.S. 347](#) (1967).

<sup>84</sup> “The ability of clients to confer confidentially with counsel enhances the caliber of legal representation an attorney can offer a client.” *Helman v. Murray's Steaks, Inc.*, 728 F. Supp. 1099, 1102 (D. Del. 1990).

Schedules require multiple days of travel each week, thereby restricting drastically opportunities to communicate. The advent of telecommuters illustrates another emerging area that requires an updated approach toward the key evidentiary privileges. Attorneys and clients working from home may rely on cordless and cellular telephones as well as e-mail as their primary methods of communication.

¶26 Although cordless and cellular communications have facilitated the attorney's ability to maintain open lines of communication with clients twenty-four hours a day, courts nevertheless have applied legal doctrines to the new technologies with caution. In response to the concern regarding the legal implications of the interception of communications over these media, Congress enacted the [ECPA](#),<sup>85</sup> which prohibits the interception and disclosure of any oral, wire or electronic communications by any person, and the [CALEA](#),<sup>86</sup> which extends the scope of the ECPA to include communications involving cordless telephones.<sup>87</sup> The ECPA directly addresses the issue of privilege in the expanding technological age by stating that "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."<sup>88</sup>

¶27 State and municipal ethics committees, however, have undermined the protection afforded by the ECPA and CALEA to wireless attorney-client communications.<sup>89</sup> These committees have often ignored the ECPA and the CALEA and the privilege protection provided therein for wireless communications, citing the lack of an expectation of privacy as an inherent trait of wireless telephone communication.<sup>90</sup> Ethics panel opinions in Massachusetts, New Hampshire, and New York City have highlighted the malpractice concerns that accompany the use of a cellular or wireless telephone to discuss confidential information. These committees have opined that absent informed consent, attorneys should not discuss confidential information when using cellular or wireless telephones.<sup>91</sup> These ethics opinions place a burden on the attorney when using instruments relied upon every day for the fundamental purpose of attorney-client communication.

---

<sup>85</sup> Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522, 2703-2711 (1996)).

<sup>86</sup> Pub. L. No. 103-414, 108 Stat. 4279 (codified as amended at 18 U.S.C. § 2510 (1996)).

<sup>87</sup> Worthy, *supra* note 30, at 454.

<sup>88</sup> 8 U.S.C. § 2517(4) (1996).

<sup>89</sup> It is unclear whether state courts and ethics committees are bound by the privilege provisions of the ECPA.

<sup>90</sup> See *Edwards v. Bardwell*, 632 F. Supp. 584 (M.D. La. 1986); *People v. Wilson*, 554 N.E.2d 545 (Ill. App. Ct. 1990).

<sup>91</sup> Joan Rogers, *Malpractice Concerns Cloud E-Mail, On-Line Advice*, 12 ABA/BNA LAW. MAN. ON PROF. CONDUCT 59, 61 (1996). See Massachusetts Bar Ass'n Ethics Comm. Op. No. 94-5 (1994) (LEXIS, Ethics Library, ETHOP file); Ass'n of the Bar of the City of New York Comm. on Professional and Judicial Ethics, Formal Op. No. 1994-11 (1994) (1994 WL 780798 (N.Y.C. Assn. B. comm. Prof. Jud. Eth.)); New Hampshire Bar Ass'n, Advisory Op. No. 1991-902/6 (1992).

¶28 The failure of ethics committees to protect fully the privilege of attorney-client communications using cellular or wireless telephones results from a misunderstanding about the vulnerability of communications. All forms of telecommunications are vulnerable to interception by third parties willing to expend the requisite resources; neither counsel nor client should effectively be denied access to these emerging technologies for fear of waiving an evidentiary privilege.

## 2. E-Mail

¶29 E-mail has become an indispensable resource in the attorney's arsenal; vital information can be disseminated rapidly to many recipients and accessed from computers in the office or on the road. Like the wired telephone call, all e-mail communications travel along lines over the telecommunications infrastructure. There are, however, subtle differences in the paths e-mail messages travel from author to recipient. Methods for transmission vary according to the network being used and this distinction has led to a fission in the privilege analysis when pertaining to e-mail communication.

¶30 Two methods of e-mail transmission are relatively free from concern. The first requires the establishment of direct connections with clients, thereby eliminating the threat that a message is transmitted along multiple Internet servers and the concomitant threat of interception at each station along the way. The second type of secure e-mail transmission involves messages traveling over proprietary networks such as [MCI Mail](#) or [America Online](#). When attorney and client are both subscribers to the same commercial e-mail service provider, the message crosses a single network protected by firewalls and other security measures. The limited case law to date suggests that a proprietary network that is secure and includes reasonable precautions provides an expectation of privacy.<sup>92</sup> Of course, satisfying this standard requires potentially significant expenditures.

¶31 A third method for transmission involving e-mail communication between attorney and client over the Internet creates the greatest concern among legal pundits over a waiver of privilege. The reason for this angst is the circuitous route Internet e-mail messages sometimes take after the author presses the send button. Unlike its direct network transmission counterparts, e-mail messages traveling over the Internet do not always follow the same path and can be routed through a series of servers.<sup>93</sup> Some members of the legal community have interpreted the exposure to multiple networks as a sign that a privileged attorney-client communication is put in jeopardy at each station. A greater understanding of how e-mail messages are transmitted is necessary, however, before concluding that In-

---

<sup>92</sup> See, e.g., *United States v. Maxwell*, 42 M.J. 568, 576 (1995) (finding that America Online subscribing plaintiff had an "objective expectation of privacy with regard to messages he transmitted electronically to other subscribers of the service who . . . had individually assigned passwords"), *rev'd on other grounds*, 45 M.J. 406 (C.A.A.F. 1996).

<sup>93</sup> Sheryl Canter, *Internet E-Mail Encryption*, PC MAGAZINE, Apr. 8, 1997, at 243.

Internet e-mail communications lack the expectation of privacy and precautionary measures capable of preserving the attorney-client privilege.

¶32

An Internet e-mail message is divided into packets as it travels across different servers before ultimately being reassembled at its destination.<sup>94</sup> The routing computers involved handle hundreds of thousands of e-mail messages daily from a variety of authors and entities with no intermediate computer handling every piece.<sup>95</sup> Thus, for interception of the message to occur during transmission, a potential cracker would need to collect fragments from multiple computers, making it considerably more difficult to intercept than a traditional wired telephone call. The nature of e-mail transmission exposes the flaws in attempts to compare Internet e-mail messages to their hard copy paper counterparts. The frequently invoked metaphor comparing an e-mail message traveling across the Internet absent encryption to the postcard sent via the [United States Postal Service](#) is a failed attempt to put privileged attorney-client communication over the Internet in layman's terms. The postcard example oversimplifies the burdens involved in intercepting e-mail messages and fails to appreciate the dynamics of transmission.

¶33

In the absence of guidance from the courts, however, some legal ethics committees have exhibited a similar misunderstanding of e-mail transmission over the Internet. While advising on malpractice issues, the Iowa Supreme Court Board of Professional Ethics and Conduct adopted a myopic approach when stating that "sensitive material" sent across the Internet by attorneys must be encrypted.<sup>96</sup> Absent encryption, the attorney must receive the client's written acknowledgment of the risks such communication poses to the expectation of privacy.<sup>97</sup> This opinion failed to undertake an analysis of the technology involved with Internet e-mail. The [South Carolina Ethics Advisory Committee](#) approached the issue of on-line communications with little technological analysis as well. The Committee stated that "the 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."<sup>98</sup> By limiting its language to such vagaries, the Bar not only casts a doubt on the expectation of privilege regarding attorney-client e-mail communications traveling over the Internet, it also opens direct attorney-client network connections and proprietary networks to suspicion. These two opinions also fail to take into account the protection of the ECPA and CALEA.

¶34

Recently, the Illinois State Bar Committee on Professional Ethics, however, stated that attorneys and their clients may use unencrypted e-mail

---

<sup>94</sup> Freivogel, *supra* note 20, at 3.

<sup>95</sup> William Freivogel, *Communicating With or About Clients on the Internet: Legal, Ethical, and Liability Concerns*, ATT'YS LIABILITY ASSURANCE SOC'Y LOSS PREVENTION J., Jan. 1996, at 18.

<sup>96</sup> Iowa Supreme Court Board of Professional Ethics and Conduct, Op. No. 96-01 (Aug. 29, 1996).

<sup>97</sup> *Id.*

<sup>98</sup> [South Carolina State Bar Ass'n Ethics Advisory Comm.](#), Advisory Op. No. 94-27 (Jan. 1995).

to communicate without fear of violating Rule 1.6(a) of the Rules of Professional Conduct.<sup>99</sup> In a well-reasoned opinion, the committee found that e-mail messages should enjoy an expectation of privacy because intercepting an e-mail message is “no less difficult than intercepting an ordinary telephone call,” and intercepting an e-mail message would be illegal under the ECPA.<sup>100</sup>

¶35 Rather than adopting the poorly-reasoned and short-sighted approach articulated by the Iowa and South Carolina ethics opinions described above, when faced with the issue of Internet-related communication, courts and ethics committees must analyze the transmission methods and utility of the relevant technologies. Society will be ill-served if adjudicating bodies simply eschew the dynamics of e-mail transmission and err on the side of greatest caution. Such an approach would pass greater cost and burden to the attorney and client and prevent them from exchanging key information over the Internet.

¶36 To evaluate the impact of emerging technologies on the expectation of privacy required by the attorney-client privilege, courts should adapt their analyses to modern technological realities. Traditional approaches to measuring the expectation of privacy in cordless, cellular and e-mail communication often ignore the nature of today's evolving marketplace and display a limited understanding of how the technology works. Justice Brandeis' dissent in *Olmstead* offers guidance for the future: “Time works changes, brings into existence new conditions and purposes. Therefore a principle to be vital must be capable of wider applications than the mischief which gave it birth.”<sup>101</sup>

#### IV. GUARDING PRIVILEGES IN THE NEXT MILLENNIUM

¶37 The technological mode of communication is clearly irrelevant in cases involving voluntary disclosures of privileged information. More pressing for courts and legislators, however, are claims of involuntary disclosures through so-called high-tech channels. Telecommunications breakthroughs continue to reduce the impediments of time and distance in our society. Unfortunately, unless tribunals and ethics committees become more progressive or take a realistic view in analyzing inadvertent waivers, counsel and clients will be deprived of the benefits of ever-improving technologies.

¶38 History demonstrates the unlikelihood of developing forms of communication that cannot be intercepted. [Anson Stager](#) tapped into telegraph wires nearly 150 years ago; today, researchers have cracked the purportedly unbreakable codes used with PCS; tomorrow, future technologies likely will prove equally vulnerable. The traditional rule of waiver of

---

<sup>99</sup> Illinois State Bar Ass'n Comm. on Professional Ethics, Op. 96-10, (May 16, 1997).

<sup>100</sup> *Id.*

<sup>101</sup> *Olmstead v. United States*, 277 U.S. 438, 472-73 (1928).

privilege upon any disclosure<sup>102</sup> or a poorly informed application of the reasonable precautions standard,<sup>103</sup> will discourage counsel and their clients from using emerging communications technologies. While some commentators might consider this chilling effect a laudable outcome,<sup>104</sup> in reality, these standards in the Information Age promote wastes of time and money, and thus less effective legal representation.<sup>105</sup> The purpose of the attorney-client privilege is to encourage free and open communication between lawyers and their clients. This objective is thwarted, however, by these roadblocks into cyberspace. As the rest of modern society shares information at light speed, an attorney is severely hindered when he or she cannot utilize the same technology, either because it is too prone to interception or because the cost of safeguarding it is prohibitive.

¶39

The evolutionary gap between telephony and evidentiary privilege law is highly illustrative. It was not until 1967 that the Supreme Court presumptively held in *Katz*<sup>106</sup> that counsel and clients enjoyed a reasonable expectation of privacy with their telephone conversations. Before then, they risked waiving their privilege if they did not communicate by mail or in-person. The new methods of communications today present similar risks and difficulties; in this era of globalization, counsel must consult the laws of the more than fifty-one jurisdictions to determine if it is reasonable to use a given technology.

¶40

Perhaps the most effective way to protect attorney-client communications in the modern era is to expand federal and enact state legislation that defines confidential communications to include those between attorneys

---

<sup>102</sup> Professors McCormick and Weinstein recognized that in Wigmore's time it might have been realistic for clients to guard against intercepted communications, but that modern technology made it virtually impossible to do so. See CHARLES MCCORMICK, HANDBOOK OF THE LAW OF EVIDENCE § 75 (2d ed. 1972); 2 JACK B. WEINSTEIN & MARGARET A. BERGER, WEINSTEIN'S EVIDENCE § 503(b)[02], at 503-52 (1982).

<sup>103</sup> Thus, under the reasonable precautions test, inadvertent disclosures do not result in *per se* waivers of privilege. Nevertheless, the cost of meeting this test is high; for example, the cost of developing coded signals to protect communications is significant. "Still, experts point out that it probably won't be long before devices that can make sense of encrypted and digitized signals will be on the shelves at Radio Shack and other stores." William G. Flanagan & David Stix, *Telephone Voyeurs*, FORBES, Sept. 30, 1991, at 172. Instead, under this test "courts would be forced to confront and resolve the issues of confidentiality based on the complexities of an ever-changing telecommunications environment." Worthy, *supra* note 27, at 463 (1996).

<sup>104</sup> According to Wigmore, "a privileged person would seldom be found to waive, if his intention not to abandon could alone control the situation." WIGMORE, *supra* note 75, at 2327. The D.C. Circuit, which has consistently applied the traditional rule, expressed a similar view when it rejected a company's contention that its inadvertent disclosure of a privileged document to a government auditor resulted from a bureaucratic error, stating that it "will grant no greater protection to those who assert the privilege than their own precautions warrant." *In re Sealed Case*, 877 F.2d 976, 980 (D.C. Cir. 1989).

<sup>105</sup> See, e.g., Anne G. Bruckner-Harvey, *Inadvertent Disclosure in the Age of Fax Machines: Is the Cat Really Out of the Bag?*, 46 BAYLOR L. REV. 385, 389 (1994) (stating that extraordinary measures taken to ensure against inadvertent disclosures translate "into wasted time and energy on behalf of the attorney and added expenses to the client's costs").

<sup>106</sup> *Katz v. United States*, 389 U.S. 347, 359 (1967).

and their clients through advanced technology. An individual can reasonably expect that an e-mail transmission will be private if interception is illegal. By way of example, in 1994, the California legislature amended the [California Evidence Code](#) in order to capture new wireless communication technologies within the concept of privileged communications. The statute effectively accomplishes this goal by defining as a “confidential communication between client and lawyer”.

[I]nformation transmitted between a client and his or her lawyer in the course of that relationship and in confidence by a means which, so far as the client is aware, discloses the information to no third persons other than those who are present to further the interest of the client in the consultation or those to whom disclosure is reasonably necessary for the transmission of the information or the accomplishment of the purpose for which the lawyer is consulted, and includes a legal opinion formed and the advice given by the lawyer in the course of that relationship. A communication between a client and his or her lawyer is not deemed lacking in confidentiality solely because the communication is transmitted by facsimile, cellular telephone, or other electronic means between the client and his or her lawyer.<sup>107</sup>

¶41 This legislation is a useful model because it is broad enough to encompass new and emerging technologies and to remove the need for judicial evaluation of these technologies. Most importantly, it provides the protection necessary to allow lawyers and their clients to freely and efficiently use new technologies without risk of waiver.

¶42 In this era of constant technological change, the adoption of such legislation is vital to the continued integrity of the attorney-client relationship as many in the legal profession embrace these new forms of communication. Courts, legislatures, and bar committees must address these modern technological issues intelligently, for distrust and a lack of understanding of the emerging technology will only result in material encroachments on these long-standing and compelling evidentiary privileges.

---

<sup>107</sup> CAL. EVID. CODE § 952 (West 1994).