Cybersex and Divorce: Interception of and Access to E-mail and Other Electronic Communications in the Marital Home

by
L. Kathryn Hedrick* & Mark Gruber**

I. Introduction

Opportunity and easy access to relationships via the Internet is attacking the sanctity and monogamy of marriage. Chat rooms and personal ads abound. Internet romance is easy to find and simple to maintain. One of the beauties of cyber-chat is that one can be whomever they wish; an 80-year-old can pretend to be 20 and vice-versa. It feels anonymous and safe because the other person in the chat room or at the other end of the message cannot see or touch the person with whom they are communicating, freeing up any inhibitions they might normally have with someone who is physically present. This perceived anonymity causes the messages or cyber-conversations to be more blunt and direct; the language used may be harsher and more crude than that used in conversation or postal mail.1 A spouse may participate in these types of cyber-affairs because they feel they can fulfill their needs without actually consummating a relationship. This is a misconception about affairs – the assumption that if the participants do not have physical sex, they are not having an affair.

Man has always communicated, from early times of sounds and gestures to paper mail, the telephone, and electronic commu-

---

* Kay Hedrick graduated from the University of Missouri-Kansas City in May 2001. She will be employed of Counsel for the Regina Keelan Bass Family Law Firm in Kansas City, Missouri.

** Mark Gruber practices in Hopatcong, New Jersey.

The desire for privacy has increased as society’s various means of communication have evolved. “The protection of mail has often been said to be of national concern.” Statutory protection of mailed material from obstruction and delay continues until the mail is physically delivered to the person to whom it is directed. In this modern computer age, spouses are increasingly obtaining “proof” of the other spouse’s infidelity from reading electronic mail (e-mail), retrieving pager messages, wiretapping the home telephone, eavesdropping on cellular or cordless phones, or retrieving records from Internet conversations in chat rooms or private cybersex chat rooms. Improper retrieval of electronic communication may constitute a violation of the Electronic Communications Privacy Act of 1986 ("ECPA"). If the retrieved messages were stored on a home computer to which both spouses have equal access there is most likely no violation. However, if the e-mail is retrieved through accessing an online account, such as America Online or Hotmail, or hacking into a password protected file on the shared computer, the spouse surreptitiously accessing the account or file is most likely subject to criminal and civil penalties.

II. Expectation of Privacy

If “Congress does not act to protect the privacy of our citizens, we may see the gradual erosion of a precious right. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances.” Privacy is eroding, but not gradually. A computer is obsolete almost while it is carried out of the store. Technological advances, though important to society, are quickly surpassing statutory protection of privacy. As predicted more than a hundred years ago, “[n]umerous mechanical devices threaten to make good the prediction that ‘what is whispered in the closet shall be proclaimed from the

---

4 See United States v. Johnson, 620 F.2d 413 (4th Cir. 1980).
housetops.’” Privacy is the “right to be let alone,” it is the principle that protects personal writings and any other production of the intellect or emotions.

The legislative history of Title III to the Omnibus Crime Control and Safe Streets Act of 1968 (“Title III”) indicates that a primary purpose of its passage was a concern for privacy interests. In addition, as noted by the Sixth Circuit, the purpose of Title III “was to sharply curtail electronic surveillance and to authorize it only under strict judicial supervision and authorization.” The history of the ECPA also emphasizes the importance of individual privacy as the “primary reason for bringing email, voice-mail, and other forms of communications under the umbrella of Title III.” In support of protecting electronic communications, the Senate Report also notes that one’s

---

9 See Warren, supra note 7, at 213.
13 Thomas R. Greenberg, E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute, 44 AM. U. L. REV. 219, 252 (1994). “The intent of Congress to take account of privacy concerns is further evidenced by incorporation into the ECPA the Office of Technology Assessment’s most rigorous recommendations respecting electronic communications. In its study, the OTA suggested three options for congressional consideration regarding electronic communications, such as e-mail, those three options, ranging from protecting such communications at all phases of transmission and storage, to taking no action at all.” Id. at 252, n. 206, citing Office of Technology Assessment, Federal Government Information Technology: Electronic Surveillance and Civil Liberties 18, 38 (1985)(noting that Title III was first major congressional action concerning surveillance and was drafted to conform with Katz v. United States, 389 U.S. 347 (1967)). Congress adopted the more stringent of the OTA-proffered options. See generally Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2521, 2701-2710, 3121-3126 (1988 & Supp. v 1993)).
interest in the privacy of correspondence does not change based on the form of the correspondence.\textsuperscript{14}

Although Congress was concerned with the invasion of privacy, establishing both civil and criminal penalties for electronic surveillance, it is clear from case law that the ECPA does not apply to workplace invasions.\textsuperscript{15} Specifically, an employer may intercept, access, read, and share an employee’s e-mail with others, because the employee has no expectation of privacy in the workplace.\textsuperscript{16} In \textit{Smyth v. Pillsbury Co.},\textsuperscript{17} the court found that no reasonable expectation of privacy exists in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system.\textsuperscript{18} Once e-mail is sent over an e-mail system that is utilized by the entire company, any reasonable expectation of privacy is lost.\textsuperscript{19} The \textit{Smyth} court found no privacy interest in workplace e-mail communications.\textsuperscript{20} “The company’s interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have.”\textsuperscript{21}

In line with the Restatement (Second) of Torts,\textsuperscript{22} the Supreme Court of Idaho indicated that liability exists for the invasion of privacy when one intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another.\textsuperscript{23} The intrusion could occur without any physical invasion such as eaves-
dropping by means of wiretapping. However, it should be noted that in *Wesley College v. Pitts*, the federal district court in Delaware found that “Congress had in mind more surreptitious threats to privacy than simply looking over one’s shoulder at a computer screen when it passed the ECPA.” There must be something in the nature of prying to be an intrusion and the matters looked into must be truly private.

In a Tennessee case, a wife’s telephone conversation was overheard and taped by her husband. The court found the recordings inadmissible because there was no interception or invasion of privacy. The wife was in the garage speaking on the telephone in a normal tone of voice. Her husband, standing outside an open window, could overhear the wife’s portion of the conversation as well as record it. The court found that “a conversation carried on in a tone of voice audible to a person outside the enclosure is not private.” The court allowed the husband’s testimony regarding what he heard, admitting the transcription of the conversation into evidence. The court held the transcription to be “entirely what [the husband had] heard naturally and could have related if his memory had been as perfect as the recording.”

E-mail messages are typically presumed to be private, entitling users to protection from prying eyes; however, some courts have held that there may be a reduced expectation of privacy, if

---

24 See id.
26 Id. at 384, citing *United States v. Meriwether*, 917 F.2d 955, 960 (6th Cir. 1990) (finding that no “electronic, mechanical or other device” was used to acquire pager messages when simply pressing a digital display button and visually observing telephone numbers). See generally *United States v. McLeod*, 493 F.2d 1186, 1188 (7th Cir. 1974) (holding no interception when government agent stood four feet from defendant and overheard conversations involving illicit gambling activities because agent did not use any “electronic, mechanical or other device” in obtaining evidence).
29 See id.
30 See id.
31 Id., citing *U.S. v. Llanes*, 398 F.2d 880 (2nd Cir. 1968).
32 *Mimms*, 780 S.W.2d at 743.
any at all. This limited expectation of privacy in e-mail cannot be enhanced by an employer’s promises to the contrary and it applies to World Wide Web chat rooms as well.

It is clear that ECPA protections may not extend to the workplace because if an expectation of privacy exists at all, it is limited. However, the expectation of privacy and, therefore, application of the ECPA, is less certain in the marital home. It may be implied from case law, however, that if a spouse takes the necessary steps to keep a conversation private, either on a telephone or in person, electronic communication, voicemail, or data or electronic communication stored on a computer, there could be an expectation of privacy and, therefore a violation of the ECPA. One way a spouse may keep the protected communications private is by closing the door and window to the garage while speaking on the telephone or by password protecting any sensitive files on the computer as well as on the individual’s e-mail account with their online or internet service provider.

III. The Wiretap Act and Stored Communications Act of the ECPA

The primary purpose of these Acts was “to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.” The Wiretap Act of the ECPA amended Title III in 1986 by adding “electronic communication” to both the definition of

---

33 See United States v. Maxwell, 45 M.J. 406, 417-19 (C.A.A.F. 1996) (holding reduced or no expectation of privacy depending upon medium of electronic communication used); Smyth, 914 F. Supp. at 98 & 101 (finding no reasonable expectation of privacy in employer-provided e-mail).
36 See supra note 15 & note 33.
41 “[E]lectronic communication’ means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole
the wiretap offense\textsuperscript{42} and the definition of “intercept”\textsuperscript{43} extending the protection of Title III against unauthorized “interception” to “electronic communications.”\textsuperscript{44} Endeavoring to intercept and procuring someone to intercept is also prohibited.\textsuperscript{45} The Stored Communications Act, enacted through the ECPA in 1986, protects against unauthorized “access” to “electronic communication while it is in electronic storage.”\textsuperscript{46}

\textbf{A. Electronic Communication}

The Internet has definitely changed the way society communicates. E-mail essentially has replaced traditional letters and even telephone calls as the primary choice for communication.\textsuperscript{47} E-mail messages are sent out globally on a daily basis.\textsuperscript{48} It is the “most rapidly adopted form of communication ever known”\textsuperscript{49} going from obscurity to mainstream dominance in less than two decades.\textsuperscript{50}

or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include — (A) any wire or oral communication; (B) any communication made through a tone-only paging device; (C) any communication from a tracking device (as defined in section 3117 of this title); or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.” 18 U.S.C. § 2510 (12)(A)-(D) (1996).


\textsuperscript{43} “‘Intercept’ means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device.” 18 U.S.C. § 2510(4) (1996).


\textsuperscript{45} See id. See also White v. Weiss, 535 F.2d 1067 (8th Cir. 1976) (conduct of a private detective who personally instructed and supervised an individual in the installation and connection of wiretapping equipment for purpose of intercepting telephone communications fell within interception language of the statute).

\textsuperscript{46} See 18 U.S.C. § 2701(a) (1996). “(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication.” 18 U.S.C. § 2510(17) (1996).


\textsuperscript{48} See generally id.

\textsuperscript{49} Brain, \textit{supra} note 47.

\textsuperscript{50} See id.
The Internet is an “external, public electronic communication structure that connects organizations and individuals throughout the world.”51 It allows users to communicate by routing data between computers.52 The World Wide Web runs on the Internet, “enabling users to send and receive textual, graphical, video, and audio materials in real time by use of interconnected data files, or ‘hyperlinks.’”53

In recent years, the world has experienced rapid growth of both Online Service Providers (“OSPs”) and Internet Service Providers (“ISPs”).54 American Online (“AOL”) is a type of OSP, a “private commercial communication network within which subscribers can correspond via email among themselves, participate in chat rooms, and access other subscriber-only content.”55 In addition, OSPs also frequently offer Internet access.56 ISPs provide access to the Internet, the World Wide Web, and allow users to send and receive Internet e-mail, but do not offer the private services of the OSPs.57

1. **E-Mail**

E-mail is one of the most common uses of the Internet.58 “Transmission of e-mail from the sender to the recipient through an electronic communication system (“system”) is indirect.”59 Once a message is sent it is immediately stored in “temporary or intermediate storage.”60 In addition, the system automatically

53 Id.
54 Decoste, supra note 51, at 81.
55 Id.
56 Id.
57 See generally id.
58 Id., citing Kershenbaum, supra note 52, at 24.
60 Id.
stores a copy of the e-mail for back-up protection, in the event the system crashes before transmission is complete. On route from sender to recipient, a message passes through both intermediate and back-up protection storage.

Transmission is considered complete when the recipient logs on to the system provider and retrieves, or downloads, the message from intermediate storage. Once the intended recipient retrieves the message, it is copied to a third type of storage on the system, or “post-transmission storage.” A message may remain in post-transmission storage for an indefinite amount of time.

Falsely reassured by critical misconceptions as to the deletion and privacy of e-mail, and “lured by the casual nature and ease of use of e-mail, users can become complacent and imprudent about the contents of their communications.” As one commentator noted, “unlike paper memorandums [sic], whose corporeal existence makes people think twice about committing questionable thoughts to paper, the transitory nature of e-mail makes it a perfect example of ‘out of sight, out of mind.’”

2. Instant Messaging, Bulletin Boards, and Chat Rooms

Instant Messaging (“IM”) allows a user to maintain a list of people they wish to interact with online. A message can be sent instantly to anyone from the “buddy list” maintained on the user’s computer. As long as both users are online at the time the message is sent, the two parties can communicate. Creating a
message opens up a small window where the user and friend can type messages to each other in “real time.”71

Most of the popular IM programs provide a variety of features:

- Instant messages: send real time notes back and forth with other users online
- Chat: create a custom chat room to use with other users
- Web links: share links to favorite Web sites
- Images: look at and share images with other users on each other’s computers
- Sounds: play sounds for other users
- Files: share files by sending them directly to other users
- Talk: use the Internet instead of a phone to speak with other users
- Streaming content: real-time or near real-time stock quotes and news72

Before the heightened popularity of the Internet, the use of bulletin boards (“BB”) and OSPs were prevalent.73 A BB is similar to an isolated Website that can only be reached using special communications software and a modem.74 Once connected to the BB, the user must use a series of menus to navigate through the contents of the BB, and to reach other BBs, the user must disconnect and dial into the other one.75

Major OSPs, such as AOL, CompuServe, and Prodigy, are the primary providers of online communication.76 Probably one of the biggest attractions of OSPs is the community that it builds.77 AOL, considered the pioneer of the online community, provides its users with the ability to talk in real-time while online using IMs and chat rooms.78 The chat room, typically specified

---

72 See Brain, supra note 47.
73 See id.
74 See id.
75 See id.
76 See Brain, supra note 47.
77 See id.
78 See id.
by subject, is an online “room” segregated from the rest of the OSP service.\textsuperscript{79} A user can enter the room and participate with a group of subscribers in a “conversation.”\textsuperscript{80} To enter the “room,” users first enter a “lobby” where they can view a list of the screen names of other users in the room at that time.\textsuperscript{81} While in the lobby a user may also see a copy of the conversation as it is then taking place.\textsuperscript{82} The user has the choice of joining the conversation or navigating to a specific interest by clicking on a symbol known as an “icon.”\textsuperscript{83} Connection to an icon will move the user into a more specific “public room.”\textsuperscript{84} As the user enters the room, all other users in the room immediately see the new participant’s screen name.\textsuperscript{85} AOL monitors and records all public chats that take place on their system.\textsuperscript{86} Individuals “chatting” in the public area can leave the area and enter a “private room.”\textsuperscript{87} AOL does not maintain nor monitor the private chat room conversations, but does provide software to users to enable them to record the messages.\textsuperscript{88}

Users of IM have no expectation of privacy.\textsuperscript{89} Although a user may be protected from interception during transmission under the Wiretap Act, the user would not be protected under the Stored Communications Act. Messages and connection information are temporarily stored on servers controlled by the provider of the IM utility and they are immediately deleted upon completion of the communication.\textsuperscript{90}

3. Webpages

The process of communication through a website is similar to the transmission of e-mail.\textsuperscript{91} As noted by the Ninth Circuit:

\textsuperscript{79} See id.
\textsuperscript{80} See Maxwell, 45 M.J. 406.
\textsuperscript{81} See id.
\textsuperscript{82} See id.
\textsuperscript{83} See id.
\textsuperscript{84} See Maxwell, 45 M.J. 406.
\textsuperscript{85} See id.
\textsuperscript{86} See id.
\textsuperscript{87} See id.
\textsuperscript{88} See Maxwell, 45 M.J. 406.
\textsuperscript{89} See generally Brain, supra note 47.
\textsuperscript{90} See id.
\textsuperscript{91} See Konop v. Hawaiian Airlines, 236 F.3d 1035, 1043 (9th Cir. 2001).
12 Journal of the American Academy of Matrimonial Lawyers

‘There is ordinarily a period of latency between the initial transmission of information for storage on a web server, and the acquisition of that information by its recipients’ . . . In other words, after the sender or owner of the website loads the communication onto the website, the information is transmitted to the web server where it is stored temporarily until an authorized recipient downloads the information from the server onto his personal hard drive. Transmission between the owner of the website and each individual authorized recipient is not complete until the recipient accesses the website and downloads the information from the web server onto his personal hard drive.\(^92\)

Interception of website communication occurs if the communication is acquired by a third party while in the course of transmission, before it is downloaded by the recipient.\(^93\) In *Konop v. Hawaiian Airlines*, when the Vice President of Hawaiian logged on using the name of an authorized recipient and downloaded the information from the website onto his own hard drive, he acquired the information before the authorized recipient retrieved it.\(^94\) The court concluded “the contents of secure websites are ‘electronic communications’ in intermediate storage that are protected from unauthorized interception under the Wiretap Act.”\(^95\)

B. Interception and Access of Electronic Communication

1. Interception, 18 U.S.C. § 2511

Prior to the 1986 ECPA Amendment, Title III was held not applicable to the interception of communications between two computers via telephone lines.\(^96\) As amended, however, Title III now prohibits any “interception” of communications, including electronic communications such as e-mail, unless one of the specifically enumerated exceptions applies.\(^97\) The time of occurrence of the interception, before, during, or after transmission, is central to the Act’s application, therefore, a thorough understanding of the meaning of the word “intercept” as it applies to electronic communication is key to understanding and applying

\(^92\) *Fraser*, 135 F. Supp. 2d at 637, quoting *Konop*, 256 F.3d at 1043.

\(^93\) See *Konop*, 236 F.3d. at 1043.

\(^94\) See *id.* at 1048.

\(^95\) *Id.*

\(^96\) See United States v. Seidlitz, 589 F.2d 152 (4th Cir. 1978).

the Act.\footnote{See generally Fraser, 135 F. Supp. 623; Konop, 236 F.3d. 1035.} Since the passage of Title III, there has been much talk about when an interception occurs. As indicated by the following cases, with a more thorough understanding of what e-mail is and how it is transmitted comes a better understanding of when interception can or cannot occur.

In \textit{United States v. Turk},\footnote{526 F.2d 654 (5th Cir. en banc 1976).} the Fifth Circuit held that the word “intercept” “require[s] participation by the one charged . . . in the \textit{contemporaneous} acquisition of the communication through the use of the device.”\footnote{Id. at 658 (emphasis added).} It is important to note, however, that the \textit{Turk} court acknowledged that “[n]o explicit limitation of coverage to contemporaneous ‘acquisitions’ appears in the Act.”\footnote{Id.} In \textit{Steve Jackson Games, Inc. v. United States Secret Service},\footnote{36 F.3d 457 (5th Cir. 1994).} the Fifth Circuit affirmed its decision in \textit{Turk}, holding that e-mail cannot be “intercepted” in violation of Title III when the acquisition of the contents of electronic communications was not contemporaneous with the transmission of the communications.\footnote{See id. at 463 (holding that “the ECPA legislative history’s explanation of the prohibitions regarding disclosure also persuades us of the soundness of Turk’s interpretation of ‘intercept’ and our understanding of the distinctions Congress intended to draw between communications being transmitted and communications in electronic storage.”).} Three years following \textit{Steve Jackson Games}, the United States District Court of Massachusetts chimed in, agreeing with the Fifth Circuit that “it is apparent that “intercept” requires the contemporaneous acquisition of the information . . . only [] interception . . . \textit{while in transmission}, like a wiretap on a telephone in use, can amount to a violation of Section 2511.”\footnote{United States v. Moriarity, 962 F. Supp. 217, 220-21 (D. Mass. 1997) (emphasis in original).}

In \textit{United States v. Smith},\footnote{155 F.3d 1051 (1998).} however, the Ninth Circuit rebuked the previous courts for looking beyond the statutory definition of “intercept,”\footnote{See \textit{id}. at 1057 (emphasis added)— (finding that “although the government’s proposed definition of ‘intercept’ might comport with the term’s ordinary meaning—‘to take, seize or stop by the way or before arrival at the destined place,’ \textit{See, e.g., Webster’s Third New International Dictionary} 1176} but only as it applied to wire
communications. The court drew a distinction between wire and electronic communications, stating the distinction between the two is “critical, because unlike the definition of ‘wire communication,’ the definition of ‘electronic communication’ does not specifically include stored information.” The court felt that it is natural to except “non-contemporaneous retrievals” from the scope of the Wiretap Act in those cases concerning electronic communications, because the “‘narrow’ definition of ‘intercept’ fits like a glove.” The court also noted that “Congress’ use of the word ‘transfer’ in the definition of ‘electronic communication,’ and its omission . . . of the phrase ‘any electronic storage of such communication’ (part of the definition of ‘wire communication’) reflects that Congress did not intend for ‘intercept’ to apply to ‘electronic communications’ when . . . in ‘electronic storage.’”

(1986)—in this case, ordinary meaning does not control. When [ ] the meaning of a word is clearly explained in a statute, courts are not at liberty to look beyond the statutory definition.” Id.). See also Colautti v. Franklin, 439 U.S. 379 (1979) (“As a rule, ‘[a] definition which declares what a term ‘means’ . . . excludes any meaning that is not stated.’; cf. Perrin v. United States, 444 U.S. 37 (1979) (emphasis added) (“A fundamental canon of statutory construction is that, unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning.”)

107 See generally Smith, 155 F.3d at 1056-59.
109 Id. at 1057.
110 Id., citing Steve Jackson Games, 36 F.3d at 461-62; accord Wesley College, 974 F. Supp. at 386; Bohach, 932 F. Supp. at 1235-36; United States v. Reyes, 922 F. Supp. 818, 836 & n.19 (S.D.N.Y. 1996). “The only cases involving wire communications that have adopted the narrow definition of ‘interception’ have done so with little analysis and with seeming unawareness of § 2510(1)’s express inclusion of stored information within the meaning of ‘wire communication.’ See Moriarity, 962 F. Supp. 217; Payne v. Norwest Corp., 911 F. Supp. 1299 (D. Mont. 1995), aff’d in part and rev’d in part, 113 F.3d 1079 (9th Cir. 1997). Indeed, the Moriarity court cited electronic-communication cases in support of its decision. See Moriarity, 962 F. Supp 217 at 220-21. Similarly, although the Turk case—in which the narrow definition of “intercept” first surfaced—involved wire communications, its interpretation of “intercept” is no longer of any real persuasive force because when Turk was decided in 1976, the statutory definition of “wire communication” did not yet include stored information. Congress’s amendment of § 2510(1) to include stored information occurred ten years later, in 1986. See Electronic Communications Privacy Act, Pub.L. No. 99-508, 100 Stat. 1848 (1986). Consequently, to the extent that Turk stands for a definition of “intercept” that necessarily entails contemporaneity, it...
In wire communications, the Ninth Circuit rejected the term ‘intercept’ as implying contemporaneous acquisition because “messages in electronic storage cannot . . . be acquired contemporaneously . . . such an interpretation, [ ] flies in the face of ‘the cardinal rule of statutory interpretation that no provision [of a statute] should be construed to be entirely redundant’111 . . . ‘[i]t is our duty ‘to give effect . . . to every clause and word of a statute.’”112

In Konop v. Hawaiian Airlines,113 Konop had created a secure website which was only accessible through application to Konop for a password in exchange for a promise of confidentiality.114 Konop’s intent was to prevent access to management or union representatives.115 However, a vice-president surreptitiously obtained access by masquerading as another user.116 The Ninth Circuit again considered the issue of interception of communications, specifically whether an electronic bulletin board and website, which are stored electronic communications, are protected from interception under the Wiretap Act of Title III.117 Overturning its position in Smith, the Ninth Circuit held that acquisition of an electronic communication does not need to be contemporaneous with transmission.118

Further explaining the process of transmission, the court found that electronic communication cannot be successfully completed without being stored.119 Therefore, it was not necessary

111 Id. at 1058, citing Kungys v. United States, 485 U.S. 759, 778 (1988). See also Colautti, 439 U.S. at 392 (“[It is an] elementary canon of statutory construction that a statute should be interpreted so as not to render one part inoperative.”).
113 Konop, 236 F.3d 1035.
114 See id.
115 See id.
116 See id.
117 See Konop, 235 F.3d 1035.
118 Id. at 1044.
119 See id. at 1045, citing Tatsuya Akamine, Proposal for a Fair Statutory Interpretation: E-Mail Stored in a Service Provider Computer is Subject to an Interception Under the Federal Wiretap Act, 7 J.L. & Pol’y 519, 561 (1999) (“‘Electronic storage’ is a part of the entire communication process, and thus,
for Congress to explicitly include the concept of storage in its definition of electronic communication. It made no more sense to the court that a “private message expressed in a digitized voice recording stored in a voice mailbox should be protected from interception, but the same words expressed in an e-mail stored in an electronic post office pending delivery should not.”

The court found it equally senseless that Konop’s messages would have been protected had he recorded and delivered them through a secure voice bulletin board accessible by telephone, but “not when he set them down in electronic text and delivered them through a secure web server accessible by a personal computer.” The court held electronic communications to be protected interception when stored to the same extent as when they are in transit.

In the most recent decision regarding interception of electronic communication, the United States District Court for the Eastern District of Pennsylvania further analyzed the word “interception” finding that acquisition must occur “before arrival.” Interception occurs when the transmission is interrupted. For example, after being sent by the sender but before being received by the intended recipient the message is acquired by a third party. When, at what point in time, the message is acquired determines whether interception has oc-

---

120 See Konop, 236 F.2d 1035.
121 Id. at 1046.
122 Id.
123 See id.
124 Fraser, 135 F. Supp. 2d. at 634 (“The common meaning of ‘intercept’ is ‘to stop, seize, or interrupt in progress or course before arrival.’ WEBSTER’S NINTH NEW COLLEGIATE DICTIONARY 630. With respect to communication, the ‘progress or course’ is the transmission of a message from the sender to the recipient.”).
125 Id. at 634.
126 Id.
Vol. 17, 2001  Cybersex and Divorce  17

curred. The Wiretap Act provides protection for private communication only during the course of transmission.

The meaning of “interception” does not change when the communication is indirect, passing through storage in the course of transmission from sender to recipient. In an e-mail communication system, as in a voice-mail communication system, a message passes through intermediate storage in the course of transmission. In both systems, a message may also be saved in storage after transmission is complete. Retrieval of a message from storage while it is in the course of transmission is an “interception” under the Wiretap Act; however retrieval of a message from storage after transmission is complete is not an “interception” under the Act. The only relevant difference between a voice-mail system and an e-mail system is that e-mail is stored in two different types of storage during the course of transmission –

127 “[I]f the recipient of a letter sent by U.S. Mail opens and reads the letter, and a third party subsequently retrieves the opened letter from the desk of the recipient, there is no “interception.” In contrast, if a third party removes the letter from the recipient’s mailbox before the recipient has retrieved and read the letter, there is an ‘interception.”’ Id.

128 “Other courts have agreed that “interception” can only occur during the transmission process.” Id. citing, e.g., Meriwether, 917 F.2d at 960 (“Congress contemplated dealing only with “transmissions” which were unlawfully intercepted”); Steve Jackson Games, 36 F.3d at 463 n.8; Reyes, 922 F. Supp. at 836 (“the acquisition of the data [must] be simultaneous with the original transmission of the data”).

129 Fraser, 135 F. Supp. 2d at 635 (e.g., “recording a message into the recipient’s voice-mail mailbox sends voice-mail communication. The message remains in storage in the recipient’s mailbox until the recipient retrieves it from his or her personal mailbox by calling the voice-mail system. After listening to the message, the recipient may either delete it from the mailbox or save it for some period of time. If a third party obtains access to the recipient’s personal mailbox and retrieves a saved message after the recipient has heard the message, there is no interception. The third party’s acquisition of the message from storage occurred after the message had been transmitted from the sender to the recipient. On the other hand, if a third party obtains access to the recipient’s mailbox and retrieves a message before it has been heard by the recipient, there is interception.”). See also Smith, 155 F.3d 1051 (interception occurred when voicemail message retrieved from recipient’s personal mailbox before it had been received by the recipient and forwarded it to her own personal mailbox).

130 See Fraser, 135 F. Supp. 2d 623.

131 See id.

132 See id.
intermediate storage and back-up protection storage. Retrieval of an e-mail message from either intermediate or back-up protection storage is interception; retrieval of an e-mail message from post-transmission storage, where the message remains after transmission is complete, is not interception.


“Access” to an electronic communication in storage is a lesser-included offense of an “interception.”’ Interception and ‘access’ are not ... temporally different.’ The terms are conceptually different, “[t]he word ‘intercept’ entails actually acquiring the contents of a communication, whereas the word “access” merely involves being in position to acquire the contents of a communication.”

An “access” could be a violation simply by making unauthorized use of a password and roaming around in a user’s e-mail or voicemail system. If an e-mail is never read, printed, or downloaded, if the voicemail is not listened to or recorded, or if some other type of “intercepting” of the contents of a communication never takes place, the entry access itself is still a violation of the Stored Communications Act. If the user making the unauthorized access to the system retrieves and/or records a message, however, that user crosses the line between the Stored Communications Act and the Wiretap Act and violate the latter’s prohibition on “interception.”

The Stored Communications Act protects messages that are temporarily stored in intermediate storage, after the sender sends the message but before the intended recipient retrieves it. Communications stored in back-up protection storage.

---

133 See supra notes 60 - 61.
135 See Smith, 155 F.3d at 1058.
136 Id.
137 See id.
138 Id. (emphasis in original). See also Fraser, 135 F. Supp. 2d 623; Konop, 235 F.3d 1035.
139 See 155 F.3d at 1058.
140 See id.
141 See Fraser, 135 F. Supp. 2d 623.
143 See Fraser, 135 F. Supp. 2d 623.
are also protected. The Stored Communications Act does not cover retrieval of a message from post-transmission storage.\textsuperscript{144}

C. Exceptions to Interception and Access

The Wiretap Act prohibits the interception and disclosure of wire, oral, or electronic communications.\textsuperscript{145} The Stored Communications Act prohibits access to stored wire and electronic communications.\textsuperscript{146} The Acts specifically enumerate exceptions to their prohibitions, such as communications which are “readily accessible,”\textsuperscript{147} have been consented to,\textsuperscript{148} or communications to which the party intercepting is actually a participant in the communication.\textsuperscript{149} Various other statutory exceptions also exist for operators at a switchboard, operators of citizen band radios, amateurs, general mobile radio services, and marine aeronautical services.\textsuperscript{150} In addition to the specifically enumerated exceptions, a few courts have applied common law exceptions such as implied consent, vicarious consent, the interspousal immunity doctrine, and intercpections occurring in the marital home.

1. Consent

Consent of a party to the communication can circumvent the application of the Wiretap Act and Stored Communications Act. Consent implies the voluntary agreement to an interception or access to the communication. In Florida, however, the state statute affords greater privacy protection than Title III’s requirement of prior consent of one of the parties to the communication.\textsuperscript{151} The Florida statute requires the consent of all

\textsuperscript{144} See id.
\textsuperscript{147} See 18 U.S.C. § 2511(2)(g)(i) (1996). See also Konop, 235 F.3d 1035 ("It shall not be unlawful . . . for any person . . . to intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.").
\textsuperscript{149} See id.
parties to the communication, not just one.\textsuperscript{152} In addition, a Florida court has found that federal law does not preempt state law when it is offering greater privacy protection.\textsuperscript{153}

No definition of “parties to the communication,” is provided in either the statute or the current case law, but Webster’s Dictionary defines “party” as “a person or group participating in an action or affair.”\textsuperscript{154} “[P]arties to the communication’ might also be construed to include not just the actual authorized recipients of a communication, but also its intended recipients.”\textsuperscript{155} This definition is consistent with portions of the Wiretap Act that permit service providers to divulge contents of communications “with the lawful consent of the originator or any addressee or intended recipient of such communication.”\textsuperscript{156}

In \textit{Konop}, where Hawaiian’s Vice-President, Davis, posed as a Hawaiian pilot, Wong, to gain access to Konop’s website and BBs, the court found that just because Wong was eligible to gain access to the website he was not made a “party” to its contents.\textsuperscript{157} However, Davis later received consent to view the site from another Hawaiian pilot, Gardner.\textsuperscript{158} Gardner, however, did not give Davis the “prior consent,”\textsuperscript{159} that could excuse Davis’ earlier acts of interception using the log-in account Davis created for Wong.\textsuperscript{160}
Vol. 17, 2001  

Cybersex and Divorce  

21

a. Implied Consent

“Consent may be actual or implied for purposes of [the] consent exception to Title III.”  

Implication can be inferred from the surrounding circumstances, which includes the knowledge that an interception may take place.  

In a Washington case, a father waived any statutory privacy right when he left messages on an answering machine. The father made disparaging remarks about the mother in messages he left for the parties’ son. The court held that a party consents to the recording of a communication when the other party announces, in a reasonably effective manner, that a recording is taking place. Since the only function of an answering machine is to record messages, no reasonable expectation of privacy was found in a message left on such a machine.  

It should be noted, however, that although consent to interception may be implied, it should not be done so casually, but the “surrounding circumstances must convincingly show that the party knew about and consented to interception in spite of lack of formal notice or deficient formal notice, in determining whether intercepted telephone conversations are admissible.”  

b. Vicarious Consent

In order for a guardian to consent on behalf of minor children, the guardian must have an “objectively reasonable good faith belief” that interception or access is necessary to act in best interest of the children; vicarious consent is permissible, it is a

165 See id.
166 See id.
167 See id.
168 See United States v. Lanoue, 71 F.3d 966 (1st Cir. 1995), appeal after new trial 137 F.3d 656 (1st Cir. 1998).
defense to a claim under the federal wiretapping statutes.\textsuperscript{169} An Alabama appellate court took the \textit{Thompson} decision further by holding that a parent may vicariously consent on behalf of a minor child, but the parent must have a reasonable good faith basis that the minor child is being abused, threatened or intimidated.\textsuperscript{170}

In \textit{State v. Diaz},\textsuperscript{171} a babysitter was indicted for aggravated assault and endangering the welfare of a minor.\textsuperscript{172} The child’s parents hired a private company to install video and audio surveillance equipment after they had noticed bruises on their child.\textsuperscript{173} The court held that the New Jersey wiretap statute did not apply because parents can vicariously consent on behalf of their children to the monitoring of caregivers.\textsuperscript{174} Both the federal and state statutes provide an exception for consent.\textsuperscript{175} In addition, \textit{Cacciarelli v. Boniface}\textsuperscript{176} held that a minor child may vicariously consent for one parent to intercept communications between a minor child and the other parent.\textsuperscript{177}

2. \textit{The Interspousal Immunity Doctrine and Interceptions in the Marital Home}

The federal wiretapping statutes have no interspousal immunity exception.\textsuperscript{178} “The plain language and legislative history of Title III evince \textit{no Congressional intent} to exempt domestic relations from its scope.”\textsuperscript{179}

\textsuperscript{169} See Thompson v. Dulaney, 838 F. Supp. 1535 (D. Utah 1993). See also Campbell v. Price, 2 F. Supp. 2d 1186 (E.D. Ark. 1998) (custodial parent’s good faith concern for minor child’s best interests may, without liability under the Federal Wiretapping Statute, empower the parent to intercept the child’s conversations with her non-custodial parent.).


\textsuperscript{172} See id.

\textsuperscript{173} See id.

\textsuperscript{174} See id.


\textsuperscript{177} See id.


\textsuperscript{179} Campbell, 2 F. Supp. 2d 1186 (emphasis added).
Historically courts have upheld the interspousal immunity doctrine in favor of domestic tranquility. This common-law doctrine was based on the legal fiction of marital identity, that in the eyes of the law the husband and wife were one person, the husband. Therefore, it was impossible to maintain a tort action between husband and wife. Interestingly enough, however, husbands and wives were always regarded as separate individuals in criminal law.

One of the primary purposes for the passage of Title III was to combat crime; it is a criminal statute with additional civil consequences. As further noted by the Sixth Circuit, the interspousal immunity doctrine should not bar a criminal prosecution, because “[e]ven in states which recognize interspousal immunity, that immunity does not apply to criminal prosecutions.”

Courts have long been divided on the federal level regarding interspousal immunity. A minority of courts has created a marital home exception and applied interspousal immunity, while a majority of courts have held that no such exception exists. One leading case, and probably the most discussed case, applying the marital home exception is Simpson v. Simpson. The husband in Simpson, suspecting his wife of infidelity, attached a tape recording device to the home telephone line to record his wife’s conversations.

---

181 See Jones, 542 F.2d 661.
182 See id.
183 See id.
185 Jones, 542 F.2d at 672.
188 See Simpson, 490 F.2d 803.
conversations with third parties.\textsuperscript{189} The court created an exception, denying the wife civil recovery despite the fact that the statute itself made no such exception. Though the doctrine does have its limited followers, state and federal courts alike have continually rejected the \textit{Simpson} decision.\textsuperscript{190}

The early federal cases of \textit{Anonymous v. Anonymous}\textsuperscript{191} and \textit{London v. London}\textsuperscript{192} reached similar conclusions to that of \textit{Simpson}. These courts held that acts taking place in the family home, involving family members, were little different than the taping of and listening to a conversation on an extension phone.

Highly critical of \textit{Simpson}, the Sixth Circuit Court of Appeals held that there was no marital home immunity.\textsuperscript{193} The \textit{Simpson} court stated that without “marital home” immunity, the federal statute might conflict with state statutes, which grant interspousal immunity from court claims. \textit{Jones} found, however, that the statute made no such provisions, nor indicated any such intent.\textsuperscript{194}

The Fourth Circuit in \textit{Pritchard v. Pritchard},\textsuperscript{195} following the reasoning in \textit{Jones}, stated that the statute clearly made no “marital home” exception.\textsuperscript{196} The court held that a husband who, while the parties were married, wiretapped the family phone and recorded his wife’s conversations with third parties was clearly liable under the statute.\textsuperscript{197} The \textit{Pritchard} case also discussed the legislative history of the federal statute and found that the history indicated Congress was aware of the extent of wiretapping in family situations and that it was the clear intent of Congress to prohibit such wiretapping.\textsuperscript{198}

In \textit{Kratz v. Kratz},\textsuperscript{199} a husband hired a private detective to wiretap the family telephone. The court, contrary to the \textit{Simpson} holding, found that the statute was a clear prohibition of such

\begin{footnotes}
\item[189] See id.
\item[190] See supra note 187.
\item[191] See Anonymous, 558 F.2d 677.
\item[193] See Jones, 542 F.2d 661.
\item[194] See id.
\item[195] See Pritchard, 732 F.2d 372.
\item[196] See id.
\item[197] See id.
\item[198] See id.
\item[199] See Kratz, 477 F. Supp. 463.
\end{footnotes}
conduct and that the wife had a right to privacy, even in the marital home.\footnote{See id.}

In an interesting California case, a husband secretly recorded conversations between his wife and another man.\footnote{See Otto, 831 P.2d 1178.} To the husband’s shock, the taped conversations revealed a plot to murder him; he was eventually found murdered in his home.\footnote{See id.}

Upon discovery of the tapes, the police focused their investigation on the wife and her lover, who were eventually convicted of the murder.\footnote{See id.} The Attorney General’s Office attempted to apply an “implied interspousal or wiretap exception” to admit the tapes into evidence.\footnote{See id. This exception, which is recognized in a minority of states, does not prohibit a family member from tapping the family telephone.\footnote{See Otto, 831 P.2d 1178.} The court looked to the language of the statute and noted that the “interspousal wiretap exception” was not specifically enumerated and, therefore, did not exist.\footnote{See id. The court, analyzing the legislative history, which indicated Congress was aware of the problem of interspousal surveillance, found that Congress could have specifically enumerated interspousal immunity as an exception had it so desired.\footnote{See id. Further, the court found the language of Title III to be clear, as is the legislative history and the holdings of a majority of courts: the penalties and prohibitions of 18 U.S.C. § 2511 apply to interspousal wiretapping.\footnote{See id.}

In Texas, an appellate court did not recognize Simpson, noting that the exception was not found in the Act itself.\footnote{See Turner, 765 S.W.2d at 470.} The suit was brought by a third party against a husband, which especially troubled the court because of the issue of privacy for the third party, not just the wife.\footnote{See id. The court held the transcripts of the wiretap could be used as evidence, specifically stating that no express exception exists in the federal wiretap statute for intercept-
tions of conversations between a spouse and a third party which took place prior to consent of one of the parties to the interception.\textsuperscript{211} The court refused to create such an exception even though the wiretap device was in the marital residence.\textsuperscript{212}

Louisiana is in the minority, recognizing the marital home exception. A Louisiana court of appeals found that a taped conversation between a wife and the private investigator she hired was not interception.\textsuperscript{213} Following \textit{Simpson}, the court held that although a wiretap occurred, it was done in the course of a marital matter and did not rise to the level of a violation of Title III.\textsuperscript{214}

Although \textit{Simpson} has not been overruled, it has been soundly criticized for creating a marital home exception despite the legislative history and the language of the federal act. The \textit{Simpson} court likened the marital home exception to interspousal immunity, which is based on maintaining marital harmony. However, it is not the place of the judiciary to concern themselves with preserving domestic tranquility and marital harmony. If spouse lacks trust and communication in their marriage leading them to surreptitiously tape the private conversations or access the private e-mail of their betrothed; it is the conduct of the taping spouse threatening the tranquility of that marriage. It is correct and logical that a majority of courts have moved away from the \textit{Simpson} decision and found no marital home or interspousal immunity exception in the Wiretap Act.

\textbf{IV. Penalties and Exclusion}

The contrasting penalty schemes further complicate the interpretation of the Act. The Stored Communications Act allows for civil damages under section 2707 or criminal prosecution under section 2701(b), which provides for incarceration up to two years.\textsuperscript{215} The Wiretap Act, however, involving the actual interception of the communication, allows for civil damages under section 2520 or criminal prosecution under section 2511, provid-

\textsuperscript{211} See id.
\textsuperscript{212} See id.
\textsuperscript{213} Robinson, 499 So.2d 152.
\textsuperscript{214} See id.
\textsuperscript{215} See Smith, 155 F.3d at 1058-59.
ing for incarceration up to five years.\textsuperscript{216} This contrast is further evidence that “accessing” is a lesser-included offense of “interception.”\textsuperscript{217} Finally, it should be noted that no exclusion remedy exists for violations of the Stored Communications Act.\textsuperscript{218} Evidently, merely accessing a communications facility does not necessarily produce the contents of communication in need of suppression; therefore, an exclusion provision in the Stored Communications Act is unnecessary.\textsuperscript{219} The actual interception of communication, however could yield sensitive information leading to suppressible evidence and, pursuant to section 2515, the contents of any such communication obtained in violation of the Wiretap Act may not be introduced in official proceedings.\textsuperscript{220}

V. Conclusion

The law in this area is convoluted and complex. It is clear from the legislative history, as well as current case law, that any interception or access of electronic communications prior to its delivery to the intended recipient or authorized user, absent one of the specifically enumerated exceptions or application of current applicable common law exceptions, is a violation of Title III and its inclusive Acts. What is unclear, however, is when “receipt” actually takes place. ‘Delivery,’ according to the Missouri Court of Appeals, is the actual delivery into the manual possession of the person to whom the mail is addressed.\textsuperscript{221} However, the Fraser court indicated in dicta that the mail must be opened \textit{and read} before receipt is complete.\textsuperscript{222} If reading the mail does indeed prove to be the catalyst for receipt of mailed material, it would naturally follow that downloading e-mail onto the intended recipient’s computer would not be enough to complete the transmission and, therefore, any interception post-download and prior to reading would be a violation of Title III.

\begin{footnotes}
\footnotetext[216]{See id.}
\footnotetext[217]{See id.}
\footnotetext[218]{See id.}
\footnotetext[219]{See Smith, 155 F.3d at 1058-59.}
\footnotetext[220]{See id.}
\footnotetext[221]{United States v. Maxwell, 137 F. Supp. 298, 303 (Mo. Ct. App. 1955), aff’d 235 F.2d 930 (8th Cir. 1956), cert. denied, 352 U.S. 943 (1956).}
\footnotetext[222]{See Fraser, 135 F. Supp. 2d 623 (indicating when a letter is opened \textit{and read} it is received by the intended recipient (emphasis added)).}
\end{footnotes}