WHO LET THE KATZ OUT? HOW THE ECPA AND SCA FAIL TO APPLY TO MODERN DIGITAL COMMUNICATIONS AND HOW RETURNING TO THE PRINCIPLES IN *KATZ V. UNITED STATES* WILL FIX IT

Nicholas Matlach[†]

I. INTRODUCTION

When Alexander Bell demonstrated a phone call to the astonished judges at the Centennial Exposition in Philadelphia, it launched, as Lord Kelvin put it, "[T]he most wonderful thing I have seen in America."[1] From the phone call's humble beginnings as a tinker project by an eccentric scientist to voice enabled website applications, phone communications have created a revolution of interconnectivity.[2] However, criminal use of modern communications methods[3] have forced law enforcement to continuously seek ways to thwart illegal activities through wiretaps and other means.[4]

For example, Voice over Internet Protocol ("VoIP") technology allows criminals to mislead investigators by changing their caller identification infor-

[†] J.D. Candidate, May 2010, The Catholic University of America, Columbus School of Law. The author would like to thank Alejandro Hopkins for his expert advice on the technical aspects of this Note and his parents for their unending love, support, and encouragement.

[1] HERBERT N. CASSON, THE HISTORY OF THE TELEPHONE 35–40 (2nd ed. 1910). *See also* LEWIS COE, THE TELEPHONE AND ITS SEVERAL INVENTORS: A HISTORY 1 (1995) (calling the patent for Bell's device, "the most valuable patent ever issued.").

[2] *See* Jim Landers, *Believer in Broadband: FCC's Powell Presses for Big Leap for U.S.*, DALLAS MORNING NEWS, Sept. 29, 2002, at 1H.

[3] *See* BRENT E. TURVEY, CRIMINAL PROFILING: AN INTRODUCTION TO BEHAVIORAL EVIDENCE ANALYSIS 672 (2008).

[4] *See* Dean Takahashi, *Wiretapping Could Stifle VOIP Technology*, SAN JOSE MERCURY NEWS, Feb. 5, 2007, at 1E. *Black's Law Dictionary* defines wiretapping as "Electronic or mechanical eavesdropping, usu. done by law-enforcement officers under court order, to listen to private conversations." BLACK'S LAW DICTIONARY 1631 (8th ed. 2004).

mation,[5] and because of VoIP's decentralized nature,[6] advanced encryption methods have defeated many wiretaps.[7] Additionally, unclear laws and regulations frustrate law enforcement in their efforts to listen in on criminals' conversations.[8] Because modern communications provide criminals much greater flexibility in their ability to conspire, Congress and the states should amend the wiretap laws to allow law enforcement greater flexibility in wiretapping these new technologies.[9]

As modern communication technologies become ubiquitous, the need for comprehensive wiretap legislation becomes more pronounced.[10] However, the benefits of wiretapping to law enforcement must always be weighed against the Fourth Amendment's protection of legitimate privacy interests. At its core, the Fourth Amendment limits the federal government's ability to intrude into people's lives.[11] It protects the people from "the general warrants and warrantless searches that had so alienated the colonists and had helped speed the movement for independence."[12] However, the Constitution provides little guidance on how the Fourth Amendment is to be applied; as scholars have noted, "[n]o provision of the U.S. Constitution has been more difficult to interpret or more controversial in its application . . . ."[13] When dealing with modern communications mediums, which were unthinkable at the writing of the Fourth Amendment, this difficulty amplifies.

Designing a law to ensure the rapid growth and expansion of technology, while protecting Americans' essential liberties, is exceptionally challenging. Only by returning to the fundamentals will this feat be achieved. The current artificial distinctions between wire, oral, and stored communications in the

---

[5] Jonathan E. Meer, *Is the Federal Government Making VoIP Safer?*, 25 COMM. L. 9 (2007).

[6] *See* discussion *infra* Part II.B.iv.

[7] *See, e.g.*, David Wiley, *Italy Police Warn of Skype Threat*, BBC NEWS, Feb. 14, 2009, http://news.bbc.co.uk/2/hi/7890443.stm.

[8] *Bugging the Cloud: Internet Wiretapping*, THE ECONOMIST, Mar. 8, 2008, at Technology Quarterly 28, 30 [hereinafter *Bugging the Cloud*].

[9] *See* Michael Cooper, *Spitzer Wants Wiretap Law to Include New Technologies*, N.Y. TIMES, Apr. 14, 2004, at B5.

[10] Editorial, *Dial-Up Law in a Broadband World*, N.Y. TIMES, Apr. 8, 2010, at A26 (explaining how a "surprising coalition of major technology companies and civil liberties advocates" are pushing for a long overdue upgrade to ECPA).

[11] *See* U.S. CONST. amend. IV. The Fourth Amendment was applied to the states with the adoption of the Fourteenth Amendment. U.S. CONST. amend. XIV § 1; *see also* Mapp v. Ohio, 367 U.S. 643, 655 (1961) (holding that the federal exclusionary rule under the Fourth Amendment applies to the states).

[12] Chimel v. California, 395 U.S. 752, 761 (1969).

[13] OTIS H. STEPHENS & RICHARD A. GLENN, UNREASONABLE SEARCHES AND SEIZURES: RIGHTS AND LIBERTIES UNDER THE LAW 1 (2006).

law[14] will continue to produce inconsistent results when applied to modern communications mediums.[15] The laws must be overhauled to protect legitimate expectations of privacy while allowing law enforcement to conduct lawful wiretaps.

At this point, an important distinction must be made. Electronic interception—wiretapping—involves a tap *between* the two points of communication,[16] while electronic eavesdropping involves a listening device on one end of the communication.[17] For example, a microphone placed in the room of someone having a conversation—even if that device is sensitive enough to hear conversation being broadcast into that room—is an electronic eavesdropping device.[18] However, if that same device acts as a physical splice in the electrical current—even if it only receives one side of the communication—then it is an electronic interception.[19] There is overlap between the two subjects, but the focus of this Note will be on *electronic interception.*

Part II will discuss the evolution of wiretapping law through Supreme Court decisions, legislative enactments, and a brief description of modern communications technologies. Part III analyzes the definitions and scope of the Electronic Communications Privacy Act ("ECPA") and the Stored Communications Act ("SCA").[20] Part IV applies the ECPA and SCA to modern communications technology, illustrating the artificiality of the current statutory scheme. Finally, Part V calls for legislation reform by returning to the principles of *Katz v. United States* and creating three separate categories of communications—public, quasi-public, and private—that protects the reasonable expectations of privacy inherent within the design and use of the different communications technology.

---

[14] *See* 18 U.S.C. § 2510 (1), (2), (17) (2006).

[15] CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 1:12, at 1-21–1-23 (3rd ed. 2008).

[16] *See* 18 U.S.C. § 2510(4)–(5) (2006). *See also* JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE § 1:2, at 1–3 (2009) ("'Wiretapping,' as the name itself suggests, refers to the interception of wire (i.e., telephone) communications.").

[17] CARR & BELLIA, *supra* note 16, at § 1.2, at 1-3.

[18] *See* H. Lee Van Boven, *Electronic Surveillance in California: A Study in State Legislative Control*, 57 CAL. L. REV. 1182, 1183 n.6 (1969).

[19] *See* CARR & BELLIA, *supra* note 16, at § 1.2, at 1-3.

[20] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C. § 2510 (2006)). The SCA was enacted as part of, and contained within, the ECPA. Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 375 (2009).

II. BACKGROUND

A. The History of Wiretapping and Electronic Privacy

The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[21]

In 1925, the Supreme Court held the Fourth Amendment must "be construed in the light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens."[22] The grammatical structure of the first clause of the Amendment does not absolutely shield an individual's person, house, or papers from the government's investigatory purposes.[23] Instead, the Supreme Court has held that it gives rise to a reasonable expectation of privacy.[24] As Justice Harlan explained, a reasonable expectation of privacy is a twofold test: "[F]irst that a person have exhibited an actual (subjective) expectation of privacy, and, second that the expectation be one that society is prepared to recognize as 'reasonable.'"[25] This shifting boundary of reasonability requires regular reexamination by the courts of the boundaries of privacy that society is prepared to accept as reasonable.[26]

The second clause of the Fourth Amendment limits the granting of warrants to when a law enforcement agency provides a sworn statement that demonstrates probable cause and sufficient specificity[27] to a neutral magistrate.[28] The determination of probable cause is a low bar, but it must rise above a police officer's mere hunch or whim.[29] By requiring specificity of the items and plac-

---

21 U.S. CONST. amend. IV.

22 Carroll v. United States, 267 U.S. 132, 149 (1925).

23 THOMAS K. CLANCY, THE FOURTH AMENDMENT: ITS HISTORY AND INTERPRETATION § 1.2.1.2 (2008).

24 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1 (2009).

25 *Katz*, 389 U.S. at 361.

26 *See, e.g.*, Steven Penney, *Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach*, 97 J. CRIM. L. & CRIMINOLOGY 477, 481–491 (2007).

27 U.S. CONST. amend. IV.

28 *See* Steagald v. United States, 451 U.S. 204, 212 (1981) ("The purpose of a warrant is to allow a neutral judicial officer to assess whether the police have probable cause to make an arrest or conduct a search.").

29 *See* Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (stating that the standards of probable cause "seek to safeguard citizens from rash and unreasonable interferences with privacy and from unfounded charges of crime.").

es to be searched and seized,[30] this requirement helps ensure that the warrant can only be used to obtain evidence relating to a particular crime or crimes.[31]

However, the Amendment itself does not provide a remedy for overreaching government intrusions or defective warrants. Instead, the judicially-created exclusionary rule provides a remedy[32] that restricts the government's ability to introduce evidence seized through an unlawful search or defective warrant against the individual.[33] The primary purpose of this rule is "to deter law enforcement officials from conducting unlawful searches and seizures by depriving them of the incentive to do so."[34]

Applying the Fourth Amendment principles to the wiretapping of evolving communications technologies can be difficult.[35] The Supreme Court examined this issue for one of the first times in the 1927 case *Olmstead v. United States*.[36] Taking place fifty years after the invention of the telephone, *Olmstead* involved a criminal conspiracy to import liquor, during the era of prohibition, to the United States through Vancouver, British Columbia.[37] Bureau of Prohibition agents installed wiretaps in the phone lines leading the conspirators' homes and monitored their communications for months.[38] The wiretaps revealed that twelve primary investors and at least fifty other individuals had conspired to import contraband liquor with gross sales, in 1920s figures, in excess of two million dollars.[39]

A five-to-four majority of the Court refused to stretch "[t]he language of the [Fourth] amendment . . . to include telephone wires, reaching to the whole world from the defendant's house or office."[40] Further, the Court recognized that "search and seizure" does not forbid "hearing or sight."[41] Finally, the Court explained that Congress was the appropriate branch to adopt a policy to ex-

---

30 Marron v. United States, 275 U.S. 192, 196 (1927) ("[T]he requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another").

31 *See, e.g.*, Stanford v. Texas, 379 U.S. 476, 485–86 (1965) (providing that a warrant's vague and overbroad description of "literary material" relating to the Communist Party of Texas was "constitutionally intolerable").

32 CLANCY, *supra* note 23, at § 13.1 (609-10).

33 *E.g.*, Mapp v. Ohio, 367 U.S. 643, 655 (1961) (holding that the exclusionary rule applies to the states as well as the federal government); Wong Sun v. United States, 371 U.S. 471, 484–85 (1963).

34 FISHMAN & MCKENNA, *supra* note 15, at § 1:2, 1-6.

35 *See Bugging The Cloud*, *supra* note 8, at 28.

36 Olmstead v. United States, 277 U.S. 438 (1928).

37 *Id.* at 456, 465.

38 *Id.* at 456–57.

39 *Id.* at 456.

40 *Id.* at 465.

41 *Id.*

clude evidence obtained through wiretaps.[42]

Congress adopted this exclusionary policy when it enacted The Communications Act of 1934 ("Communications Act").[43] This Act created the Federal Communications Commission ("FCC" or "Commission") to, among other things, regulate common carriers,[44] such as telephone companies, and also prohibited the unauthorized interception or divulgence of the content of any communication transmitted by wire without the sender's consent.[45] Three years later, the Supreme Court held in *Nardone v. United States* that the language prohibited the use of intercepted communications by law enforcement agents in federal court.[46]

However, *Nardone* did not dissuade determined police officers from using wiretaps to investigate cases, nor did it discourage creative prosecutors from seeking ways to admit the evidence.[47] Two years after *Nardone*, the Court provided additional guidance and limits for wiretapping in *Weiss v. United States*.[48] In *Weiss*, eight men conspired using the postal system in an attempt to collect false disability and accident claims from insurance companies.[49] A few months before the indictment, law enforcement officers intercepted, recorded, and produced stenographic transcripts of every phone call to and from Weiss'

---

[42] *Id.* at 465–66. A decade before *Olmstead,* Congress passed a temporary World War I statute that prohibited and criminalized the tapping of telephone or telegraph lines taken over by the government. *See* Act of Oct. 29, 1918, § 1, 40 Stat. 1017, 1017–18. After the war, Congress allowed this statute to expire, and thus, no federal anti-wiretapping laws existed when Olmstead's phones were tapped. *See* Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553, 583 (2007).

[43] Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1103–04 (1934).

[44] *Id.* at 1070.

> "[C]ommon carrier" or "carrier" means any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy, except where reference is made to common carriers not subject to this chapter; but a person engaged in radio broadcasting shall not, insofar as such person is so engaged, be deemed a common carrier.

47 U.S.C. § 153(10) (2006).

[45] Communications Act of 1934, Pub. L. No. 73-416, § 605, 48 Stat. 1103–04 (1934). ("[N]o person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted communication to any person . . . .").

[46] Nardone v. United States, 302 U.S. 379, 381–83 (1937).

[47] *See, e.g.*, Sablowsky v. United States, 101 F.2d 183, 185 (3d Cir. 1938) (reversing the conviction of the appellants based on evidence of over 1,500 intercepted phone calls introduced at trial); Diamond v. United States, 108 F.2d 859, 860 (6th Cir. 1938) (holding that the federal government was incorrect in asserting that since "only four or five" of the 150 intercepted calls were interstate, the Communications Act prohibition on interception did not apply).

[48] Weiss v. United States, 308 U.S. 321 (1939).

[49] *Id.* at 324.

office.[50] As a result of the wiretap, seventy-six conversations were admitted into evidence against the defendants.[51] Three of the defendants pled guilty and agreed to testify for the government.[52] At trial, the remaining defendants were found guilty.[53]

On appeal, the defendants argued that section 605 of the Communications Act barred the admission of the phone calls into evidence.[54] The government urged the Court to hold that section 605 did not apply to intrastate communications, and that, even if it did, the divulgence of the messages was within the consent requirement since the defendants helped to correct the transcripts and testified to their content.[55]

After examining the language, structure, and legislative history of section 605, the court rejected the government's argument that section 605 did not apply to intrastate communications.[56] It concluded that the "the broad and inclusive language of the second clause of the section is not to be limited by construction so as to exclude intrastate communications from the protection against interception and divulgence."[57] The Court also rejected the government's consent argument because "[t]he Act contemplates voluntary consent and not enforced agreement to publication."[58] Because the defendants only learned about the wiretaps after they were indicted, the Court held their consent was involuntarily made.[59] *Weiss* provided two principles that have permeated subsequent wiretapping policy: the federal government has jurisdiction over wiretapping,[60] and consent must be given voluntarily prior to the wiretapping for the evidence to be admissible.[61]

The Supreme Court resolved the question of whether only one or both parties need to provide consent in *Rathbun v. United States*.[62] In *Rathbun*, a law enforcement officer received prior consent from one party to a telephone conversation, but not the other party, to listen in to a telephone conversation in

---

50 *Id.* at 325.

51 *Id.*

52 *Id* at 324. One defendant even assisted prosecutors in correcting the accuracy of the stenographic transcript prior to trial. *Id.*

53 *Id.*

54 *Id.* at 326.

55 *Id.* at 326–27.

56 *Id.* at 328–29.

57 *Id.* at 329. The Court noted the petitioner's argument that section 605 did not seek to exclude intrastate calls from protection because a person wiretapping a telephone line cannot distinguish between intrastate and interstate communications. *Id.* at 328.

58 *Weiss*, 308 U.S. at 330.

59 *Id.*

60 *See* FISHMAN & MCKENNA, *supra* note 15, § 4:14, 4-22.

61 *Id.* at § 5:1–2, 5-7; *Weiss*, 308 U.S. at 330.

62 Rathbun v. United States, 355 U.S. 107 (1957).

which the defendant threatened the life of another.[63] The defendant argued that section 605 required the consent of both parties to divulge the contents of those communications.[64] The Supreme Court disagreed, holding that "[e]ach party to a telephone conversation takes the risk that the other party may have an extension telephone and may allow another to overhear the conversation."[65] The concept of one-party consent is critical to understanding what expectation of privacy an individual may have when having a conversation using any communications medium; a person always assumes the risk that the other person may be a government agent or working with the government.[66]

Congress replaced the Communications Act's one-sentence provision in section 605 with a comprehensive federal wiretapping statute when it passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[67] The statute prohibited the interception of oral and wire communications without a warrant.[68]

In 1986, Congress updated the federal wiretapping laws to include electronic communications and stored communications with the passage of the ECPA and the SCA.[69] In 1994, Congress passed the Communications Assistance for Law Enforcement Act ("CALEA") to keep federal wiretapping statutes current with rapidly changing communications technology.[70] The primary goal of CALEA

---

63 *Rathbun*, 355 U.S. at 108.

64 *Id.* at 108–11.

65 *Id.* at 111. Congress incorporated this holding into the federal wiretapping statutes: "It shall not be unlawful . . . for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(c) (2006). *See also* FISHMAN & MCKENNA, *supra* note 15, § 5:12 at 5-29 (noting that some states have stricter standards than federal laws on when law enforcement officers can listen in on such conversations).

66 Hoffa v. United States, 385 U.S. 293, 303 (1966).

67 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 212 (1968) (codified as amended at 18 U.S.C. §§ 2510-2521 (2006)).

68 18 U.S.C. § 2511(1)–(2). However, it also created a specific exemption for the president to make warrantless wiretaps within his constitutional authority for foreign intelligence gathering and "to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government." § 2511(3). In 1972, the Supreme Court held that the president does not have the constitutional authority to perform warrantless domestic wiretaps under the "clear and present danger" test, United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 321–22 (1972), but the decision left open the question of whether the same rule applied to foreign wiretaps. *Id.* at 321–22.

69 Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986). *See infra* Part III and accompanying text.

70 Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. § 1001-10 (2006)) and in scattered sections of 18 U.S.C.). *See* Susan Landau, *National Security on the Line*, 4 J. TELECOMM. & HIGH TECH. L.

was to preserve the ability of law enforcement officers to receive wiretapped communications from surveillance targets in light of evolving communications technologies.[71] Congress paid for the modifications and expansions necessary for common carriers to provide these wiretaps.[72] CALEA defined a telecommunications carrier as a "person or entity engaged in the transmission or switching of wire or electronic communications as a common carrier for hire."[73] Examples of telecommunications carriers in the committee report included:

> local exchange carriers, interexchange carriers, competitive access providers (CAPs), cellular carriers, providers of personal communications services (PCS), satellite-based service providers, cable operators and electric or other utilities that provide telecommunications services for hire to the public, and any other common carrier that offers wire or wireless service for hire to the public.[74]

CALEA also intended to exclude information services,[75] described as "electronic mail [and] on-line services providers, such as Compuserve, Prodigy, [and] America-On-line . . ." from the definition of a telecommunications carrier.[76] Finally, CALEA gave the FCC the authority to designate any service provider as a telecommunications carrier if the Commission determined it was in the public interest.[77]

B. Modern Communication Mediums

1. The Traditional Wiretap of an Analog Communication

The basic premise of Bell's telephone still exists today: two wires, one for transmission and one for reception, run from a source to its destination in an

---

409, 410 (2006) ("As telecommunications technology changed, law enforcement sought to keep the law current, and . . . [CALEA was] passed. In requiring that digitally-switched telephone networks be designed in accordance with federally-specified wiretapping standards, CALEA substantively changed the way telecommunications equipment was developed and deployed.").

[71] H.R. REP. NO. 103-827, at 9–10 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3492–93.

[72] FED. BUREAU OF INVESTIGATION & U.S. DEP'T OF JUSTICE, COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT: SECOND ANN. REP. TO CONGRESS 2 (1996) (providing that Congress authorized $500 million to telecommunications carriers for fiscal years 1995 through 1998 to pay for "all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services . . . to establish the capabilities necessary to comply with [sections of] CALEA.").

[73] 47 U.S.C. § 1001(8).

[74] H.R. REP. NO. 103-827, at 20 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3500.

[75] *See* 47 U.S.C. § 1001(8)(C).

[76] H.R. REP. NO. 103-827, at 20 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3500.

[77] 47 U.S.C. § 1001(8)(B)(ii).

unbroken link.[78] The transmission wire transfers the electrical signal created by the pressure of the voice against the microphone to the speaker, which converts the electrical impulses back into sound.[79] Therefore, in order to have a two-way communication, one wire connects each microphone to the opposite speaker.[80]

This basic premise is an oversimplification of the modern Public Switched Telephone Network ("PSTN"), which uses "circuit-switched" systems to transmit from source to destination.[81] The main advantage of the PSTN is the ability to connect a subscriber to any phone in the world on the network.[82] This is possible with the use of centralized hubs,[83] which automatically transfer the electrical current of calls to other hubs and switches until it reaches the destination.[84] Under CALEA, once law enforcement officials obtain a wiretap order from a judge allowing them to monitor a telephone call, the PSTN can be used to relay the call to the surveillance target, as well as to the government agent.[85]

2. The Modern Wiretap of a Digital Communication

Modern communications use a global interconnected web of digital networks called the Internet.[86] The Internet functions like a courier: small segments of code, called packets, travel between computers.[87] All packets contain a small piece of code that references a protocol.[88] These protocols are standards

---

78 *See* LAWRENCE HARTE, TELECOM BASICS 116–17 (3rd ed. 2004).

79 *See id.* at 116.

80 *Id.* at 116–17.

81 *See* OLIVER C. IBE, CONVERGED NETWORK ARCHITECTURES: DELIVERING VOICE AND DATA OVER IP, ATM, AND FRAME RELAY 12 (2002). PSTN networks typically follow a five-class hierarchy. A class five hub would be in a local office in a section of a city or town while a class one regional hub connects to an international gateway for long distance calling. A phone call to a neighbor uses the class five hub. However, if someone were to place a call to someone in another region the call would climb up the hierarchy to an idle class one regional center. *See id.*

82 *See id.*

83 *See* HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 568 (25th ed. 2009) (defining a hub as "[t]he point on a network where circuits are connected.").

84 *See* Ibe, *supra* note 81, at 12.

85 *See* Timothy Singleton, *Big Brother Hears You, But Can He Understand What He Hears? The Problematic Application of CALEA to VoIP Communications in the Age of Encryption*, 15 TULSA J. COMP. & INT'L L. 283, 297–98 (2008).

86 *See* TIM BERNERS-LEE & MARK FISCHETTI, WEAVING THE WEB: THE ORIGINAL DESIGN AND ULTIMATE DESTINY OF THE WORLD WIDE WEB BY ITS INVENTOR 6 (1999).

87 *See* JAMES GILLIES & ROBERT CAILLIAU, HOW THE WEB WAS BORN: THE STORY OF THE WORLD WIDE WEB 4–6 (2000).

88 *See* Keith E. Witek, *Software Patent Infringement on the Internet and on Modern Computer Systems — Who is Liable for Damages?*, 14 SANTA CLARA COMPUTER & HIGH TECH. L.J. 303, 346 (1998).

set by the Internet Engineering Task Force ("IETF").[89] For example, a protocol is like the information contained on a standard envelope containing the source, destination, and routing information.[90] There is great flexibility on what a protocol may contain, but the IETF has established international standards that allow computers throughout the world to interpret a data packet's header information.[91]

A digital wiretap uses a program called a network analyzer to copy some or all of the packets from a given computer or network.[92] The network analyzer can be configured to look for certain protocols and will make copies of the data packets as the tapped computer receives them.[93] These copies are sent back to the tapper's computer for recompilation and analysis.[94] For example, to wiretap e-mail communications, a sophisticated network analyzer will read the header information on all of the packets, and those that reference one of the many types of common e-mail transport protocols will be copied, while others are discarded.[95]

The FBI's former network analyzer, Carnivore, allowed it to capture as detailed or narrow of a field of information as necessary from those users' com-

---

[89] Internet Engineering Task Force, Mission Statement, http://www.ietf.org/about/mission.html (last visited Jan. 9, 2010). The IETF seeks to "make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet." *Id.* It is important to that although the IETF "makes standards that are often adopted by Internet users . . . it does not control, or even patrol, the Internet. Paul Hoffman & Susan Harris, *The Tao IETF: A Novice's Guide to the Internet Engineering Task Force*, Sept. 2006, http://www.ietf.org/rfc/rfc4677.txt (last visited Jan. 9, 2010).

[90] *See* GILLIES & CALLIAU, *supra* note 87, at 4–5.

[91] *See* Internet Engineering Task Force, The IETF Standards Process, http://www.ietf.org/about/standards-process.html (last visited Feb. 19, 2010). Protocols are key to modern communication privacy because every destination and sub-destination reads the protocol for routing, tracking, and filtering purposes. The information contained within this header is dependent on the content, transmission method, and other factors that allow then network to properly route the information between two computers and traverse firewalls. BEHROUZ A. FOROUZAN, TCP/IP PROTOCOL SUITE §§ 11.1–6, 12.1–11 (2006). A firewall may be either a hardware or software component that works like a gatekeeper by analyzing the header information and deciding to accept or reject the packet. *Id.* at § 28.7. It is through these properly configured firewalls that users maintain their privacy from unwanted communications by hackers and wiretappers.

[92] *See* ALFRED BASTA & WOLF HALTON, COMPUTER SECURITY AND PENETRATION TESTING 69–80 (2008); *see also* Xiaomin Huang et al., *Computer Crime*, 44 AM. CRIM. L. REV. 285, 289 n.20 (2007).

[93] *See* BASTA & HALTON, *supra* note 92, at 69–80.

[94] *See id.*

[95] *See* Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 77 (2003) (describing the FBI's use of "packet sniffers," or network analyzers, in wiretapping e-mail communications).

puters under surveillance.[96] Carnivore would capture all information flowing from the user's computer to the user's Internet service provider ("ISP") and then filter out information that was not included in the warrant.[97] This information was stored and transmitted to an FBI computer and then examined by federal agents.[98] The National Security Agency ("NSA") uses a more expansive system, a highly classified network analyzer called Echelon.[99] This system involves a tap at communications portals, including international telecommunications satellites ("Intellisats"), "undersea cables, land-based microwave networks, and regional telecommunications satellites."[100] Echelon splits the information collected into encrypted and unencrypted streams.[101] The encrypted streams are then decrypted and join the unencrypted streams at a supercomputer, which analyzes the communications key words or phrases and alerts NSA operators to any potentially dangerous content.[102]

3. Merging the Phone Company with the Internet

In 1995, software developers created Voice over Internet Protocol ("VoIP") to transmit phone calls digitally over the Internet.[103] Using high-speed Internet access, a VoIP user can communicate across the office or across the world without incurring long distance or per-minute usage charges.[104] The technology can be either hardware or software interfaces that converts phone conversations into data packets, which are then transmitted through the Internet.[105]

The difference between the VoIP and the PSTN networks is similar to the difference between trains and cars. In a traditional PSTN system, a physical wire connects two points for the duration of the phone call.[106] This method is like a long train moving between two points and occupying the entire length of the track for the duration of the trip. VoIP communication takes that same length of train and splits it into millions of tiny cars that travel on a massive

---

[96] PRESTON GRALLA, HOW THE INTERNET WORKS 373 (8th ed. 2007) (noting that while the FBI has discontinued Carnivore, the agency still uses similar technology).

[97] *Id.*

[98] *See id.*

[99] *Id.*

[100] *See id.* at 374–75.

[101] *Id.* at 375.

[102] *Id.*

[103] *See* Amy L. Leisinger, Note, *If it Looks Like a Duck: The Need for Regulatory Parity in VoIP Telephony*, 45 WASHBURN L.J. 585, 587–89 (2006).

[104] *See* DAVID GREENBLATT, THE CALL HEARD 'ROUND THE WORLD: VOICE OVER INTERNET PROTOCOL AND THE QUEST FOR CONVERGENCE 61–63 (2003).

[105] JAMES E. GASKIN, TALK IS CHEAP: SWITCHING TO INTERNET TELEPHONES 11–14 (2005).

[106] *See* Harte, *supra* note 78, at 116.

interconnected web of highways. The cars all know where they are going, and in what order they need to arrive, but take the quickest—not necessarily the most direct—path. While traveling, other packets (i.e., e-mail messages, Web sites, downloads, streaming radio) can merge into and out of the data string creating a continuous transmission scalable up to the width and number of the highways—bandwidth.[107]

Traditional VoIP providers have a central server that facilitates phone calls.[108] When a VoIP-enabled telephone is used to dial a phone number, the central server will interpret the dialed digits like the way physical switches would in the traditional PSTN.[109] The central server then redirects the call through the Internet to either another subscriber's VoIP phone or to a local switching station for a phone connected to the PSTN.[110] Once the call is redirected, the individual VoIP software communicates directly without interfacing the central server.[111] If the connection is to a non-VoIP telephone number, then a central server will facilitate the VoIP call and convert it into an analog call that interfaces with the PSTN.[112] While many traditional VoIP providers claim to be "a revolutionary breakthrough in the history of human communications," they are actually "only an improvement . . . in the technical world."[113]

4. Decentralized Digital Communications with Skype

One new revolutionary communication technology, Skype, is unique because it uses a modified version of a peer-to-peer (P2P) network,[114] called Kazaa.[115] P2P networks were most famously used by Napster and Grokster to share music files that violated copyright laws.[116] Skype uses two different types

---

[107] *See* Marc Elzweig, *D, None of the Above: On the FCC Approach to VoIP Regulation*, 2008 U. CHI. LEGAL. F. 489, 494–96 (2008).

[108] *See* GASKIN, *supra* note 105, at 25.

[109] *See id.*

[110] *See id.* at 24, 29.

[111] *See* GRALLA, *supra* note 96, at 121–23.

[112] *Id.* at 123.

[113] GASKIN, *supra* note 105, at 25.

[114] *See* HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 847 (25th ed. 2009) (defining a peer-to-peer network as a network "in which every node has equal access to the network and can send and receive data at any time without having to wait for permission from a control mode.").

[115] ANDREW SHEPPARD, SKYPE HACKS: TIPS & TOOLS FOR CHEAP, FUN, INNOVATIVE PHONE SERVICE 1 (2006) ("Using P2P technology means that Skype runs on a mesh of interconnected PCs spread across the global Internet . . . .").

[116] *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1101 (9th Cir. 2001); MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 921–22 (2005).

of computers: nodes and super nodes.[117] A node is a computer on a network that is running the Skype software, and a super node is a node that is "nominated . . . to take on some of the administrative and coordinating activities of [the] network."[118]

The Skype network exists by and for the users and is free of charge for all of the users on the network.[119] Unlike a PSTN, which works on a five-layer hub-and-spoke network,[120] Skype uses a three-layer Web structure.[121] The first layer is all of the nodes that talk to the super nodes in the second layer, which handle "some of the administrative and coordinating activities of its P2P network."[122] The individual nodes then can directly communicate with other nodes independent of the super-nodes.[123] The third layer functions like a traditional VoIP provider: a central server that completes the connection between the Skype user and the PSTN.[124]

Skype differs from most forms of modern communication in a critical way: voice communications over Skype are decentralized.[125] In a PSTN, if a hub is inoperable, all dependant spokes also become inoperable unless supported by a

---

[117] SHEPPARD, *supra* note 115, at 2.

[118] *Id.* Skype has not released the software rules that designate how a computer becomes a super node, but Skype's Web site explains the advantage of this type of super node network structure over more traditional P2P technology introduced by Kazaa:

> P2P network technologies used by file-sharing applications would be almost suitable for decentralizing [Skype], but those networks are fragmented in nature – a search does not reach all nodes in the network. Clearly, in order to deliver high quality telephony with the lowest possible costs, a third generation of P2P technology ("3G P2P"), or Global Index (GI) was a necessary development and represents yet another paradigm shift in the notion of scalable networks. The Global Index technology is a multi-tiered network where supernodes communicate in such a way that every node in the network has full knowledge of all available users and resources with minimal latency.

Skype, P2P Telephony Explained — For Geeks Only, http://www.skype.com/help/guides/p2pexplained/ (last visited Jan. 8, 2010) [P2P Telephony Explained].

[119] *See* SHEPPARD, *supra* note 115, at 3.

[120] IBE, *supra* note 81, at 12–13. Traditional PSTN networks typically follow a five-class geographic hierarchy. A class five hub connects the individual phones to a local office. Following predetermined routing procedures, this local office will either connect a phone call to another phone connected to that local office, or pass the call to regional and long distance hubs in the hierarchy. Eventually, the call will be passed back to a local office that will complete the circuit to the call recipient. *Id.*

[121] *Cf.* SHEPPARD, *supra* note 115, at 2–3.

[122] *Id.*

[123] *Id.* at 3.

[124] *See* GRALLA, *supra* note 96, at 122–23.

[125] *See* SHEPPARD, *supra* note 115, at 2, 4; *see also* Samuel Korpi, Internet Telephony – Security Issues in Skype § 1.3 (Spring 2006) (unpublished dissertation, Helsinki University of Technology), *available at* http://www.tml.tkk.fi/Publications/C/21/Korpi_ready.pdf.

direct link to another hub.[126] In Skype's network, the destruction of any single super node results in the promotion of the computer with the next highest available bandwidth to replace it.[127] For this reason, the software is self-sustaining as long as it is being used.

The popularity of Skype is widespread. In 2009, Skype earned $551 million in revenue and boasted 405 million registered users.[128] Many products have helped to bridge the gap between a traditional phone and the computer-based Skype software, while some manufactures have even created Internet phones that integrate directly with the Skype network without the need for a computer.[129] Also, many smart phones[130] have the ability to use Skype software to make phone calls,[131] and Verizon Wireless is the first cell phone carrier to fully support Skype calls on most of their new smart phones.[132] The popularity of Skype will continue to push new technologies to expand the usefulness of Skype style services into completely integrated Web-based applications.[133] In

---

[126] *See* IBE, *supra* note 81, at 12–13 (2002). Due to the sophistication of the modern PSTN network, it would take more than one of the higher class hubs (one through four) to bring down the entire network. *Id.*

[127] *See* IAN J. TAYLOR & ANDREW HARRISON, FROM P2P AND GRIDS TO SERVICES ON THE WEB § 11.2.3, at 208 (2nd. ed. 2009).

[128] Gabriel Madway, *Skype Founders Sue eBay, Investors*, REUTERS, Sept. 17, 2009, http://www.reuters.com/article/idustre58f5xc20090917. Skype earns revenue by charging by the minute for phone calls between software and PSTN phones or cell phones. Press Release, Skype, Skype Available on Apple App Store (March 31, 2009), http://about.skype.com/2009/03/skype_available_on_apple_app_s.html.

[129] *See, e.g.*, Posting of Peter Rojas, *The Skype Phones of CES*, to ENGADGET, http://www.engadget.com /2007/01/12/ the-skype-phones-of-ces/ (Jan. 12, 2007, 8:52 EST); Press Release, Belkin, Make Free Unlimited Skype™ Calls Without a Computer with Belkin's New Desktop Internet Phone for Skype (Jan. 7, 2008), http://www.belkin.com/pressroom/releases/uploads/01_07_08DesktopInternetPhoneSkype.html.

[130] PEI ZHENG & LIONEL M. NI, SMART PHONE & NEXT GENERATION MOBILE COMPUTING § 1.1.1.3 at 4–5 (2006) (stating that a smart phone is a cell phone that, in addition to making voice calls, can "facilitate data access and processing with significant computing power . . . . [A] smart phone usually provides personal information management (PIM) applications and some wireless communications capability. Roughly speaking, a smart phone is like a small, networked computer in the form of a cell phone.").

[131] *See, e.g.*, Press Release, Skype, Skype Coming to BlackBerry Smartphones in May (Mar. 31, 2009), http://about.skype.com/2009/03/skype_coming_to_blackberry_sma.html (last visited Nov. 6, 2009); Posting of Jessica Dolcourt, *Skype for iPhone: It's Official*, to CNET.COM, http://reviews.cnet.com/8301-12261_7-10206786-51.html (Mar. 29, 2009, 00:27 EST).

[132] *See* Press Release, Verizon Wireless, Skype Mobile For Verizon Wireless Available Thursday: Companies Deliver Expansive Global Calling Community and Free Skype-to-Skype Calls on the Most Reliable Wireless Network in the United States (Mar. 23, 2010), *available at* http://news.vzw.com/news/2010/03/pr2010-03-23a.html.

[133] *See, e.g.*, Mark Gibbs, *Ribbit Offers an Open Alternative to Skype*, NETWORK WORLD, Dec. 19, 2007, *available at*

short, Skype is becoming less like a computer phenomenon for geeks and more like the telephone sitting on the nightstand.

5. Taking Digital Communications to the Next Level with Instant Messaging

Instant messaging ("IM") began on isolated university networks and was designed to transmit an instantaneous message to another computer on the network.[134] The first successful introduction of IM technology was a program called ICQ, an acronym for "I seek you," that focused on creating peer-to-peer communities.[135] As the Internet grew into community-based networks, IM technology was offered as a feature of certain subscription services.[136] A new generation of instant messaging applications has evolved to not only transmit text, but also images, documents, voice, and even video.[137]

Americans are also increasingly using IM services with devices other than a personal computer. A recent study by the Pew Internet & American Life Project found that seventy percent of Internet users fifty years or younger use more than one device to access the Internet.[138] Through these devices, users increasingly access social networking Web sites ("SNWs") to send text messages or IMs. The Pew study found that fifty-eight percent of teenage users of SNWs send text messages or IMs through these sites.[139] In short, IM has become "part of the fabric of our daily lives . . . ."[140]

IM services thrive on the size of their membership. The more people use a specific platform for instant messaging, the more likely they will recruit others to join that platform.[141] IM applications are often free to download and use after a user registers some basic information.[142] Typically, this information is not

---

http://www.networkworld.com/newsletters/web/2007/1217web2.html.

[134] JOHN W. RITTINGHOUSE & JAMES F. RANSOME, IM INSTANT MESSAGING SECURITY § 1.3.1, at 3 (2005).

[135] *Id.* at 3–4.

[136] *Id.* at 4.

[137] *Id.* at § 2.2, at 40. *See* John N. Titley, Comment, *Real-Time Confusion: Classifying Instant Messages Under Section 5 of the Securities Act of 1933*, 56 CASE W. RES. L. REV. 1177, 1180–81 (2006).

[138] AMANDA LENHART ET AL., PEW INTERNET & AMERICAN LIFE PROJECT, SOCIAL MEDIA & MOBILE INTERNET USE AMONG TEENS AND YOUNG ADULTS 14 (2010), http://pewinternet.org/~/media//Files/Reports/2010/PIP_Social_Media_and_Young_Adults_Report.pdf.

[139] *Id.* at 20.

[140] RITTINGHOUSE & RANSOME, *supra* note 134, at § 1.3, at 8.

[141] *See* Matthew A. Goldberg, *Message in a Bottleneck: The Need for FCC-Mandated Interoperability Among Instant Messaging Providers*, 9 MARQ. INTELL. PROP. L. REV. 133, 136–37 (2005).

[142] RITTINGHOUSE & RANSOME, *supra* note 134, at § 2.1.1, at 33–34. One of the reasons

verified, allowing for relatively anonymous communication. After registering, the user will connect to the IM chat server and begin using the service.[143]

A user is then able to initiate individual or group chats.[144] Other members of the community may initiate a chat with the user in separate dialog boxes that display that communication.[145] The user can have multiple individual or group chats simultaneously.[146] While some users may think that their chats are only visible to them and the party they are communicating with, most IM communications are transmitted and stored on the IM provider's central server.[147]

Another prominent IM service is Google Talk, which uses an open source protocol called XMPP for its Web-based IM application.[148] This open source protocol functions using the server-client model with encryption built around a streaming core.[149] Compare this structure to a public water utility where water is retrieved from an aquifer by a central pumping station, treated and purified, and then forwarded to its destination inside pipes designed to protect the water from contamination. In this context, the IM chat server is the central pumping station and the aquifer is an IM user registered with the network. The server logs and retransmits the message to the destination inside encrypted streams.[150]

In addition to personal use, businesses utilize IM services, employing in-house and customer service-based IM applications for employees and clients.[151]

---

for the success of IM is the fact that it is a "client-driven" communications service in that "[a]ny user can download a client, configure a user account, and be up and running in minutes." *Id.* at § 7.1, at 196. This is contrasted with e-mail, which requires a server configuration before an individual can receive communications. *Id.*

[143] *See id.* at § 2.1, at 33–36.

[144] *See* 7 Things You Should Know About Instant Messaging, EDUCAUSE LEARNING INITIATIVE (EDUCAUSE, Boulder, CO), Nov. 2005, http://net.educause.edu/ir/library/pdf/ELI7008.pdf.

[145] *See id.*

[146] *See* GRALLA, *supra* note 96, at 113.

[147] *See, e.g.*, AOL, AIM Privacy Policy, http://www.aim.com/tos/privacy_policy.adp (last visited Feb. 19, 2010) (AOL Instant Messenger reports that it will display the contents of a user's IMs and personally identifiable information in response to:

> legal process (for example, a court order, search warrant or subpoena), or in other circumstances in which AOL has a good faith belief that AIM or AOL are being used for unlawful purposes. AOL may also access or disclose your AIM information when necessary to protect the rights or property of AIM or AOL, or in special cases such as a threat to your safety or that of others.

Id.

[148] *See* Google, Google Talk for Developers, http://code.google.com/apis/talk/open_communications.html (last visited Feb. 8, 2010).

[149] XMPP, Summary of XMPP, http://xmpp.org/about/summary.shtml (last visited Feb. 8, 2010).

[150] XMPP, Extensible Messaging and Presence Protocol (XMPP): Core, XML Streams, http://xmpp.org/rfcs/rfc3920.html#streams (last visited Feb. 26, 2010).

[151] *See* RITTINGHOUSE & RANSOME, *supra* note 134, at § 7.1, at 195–99 (noting that ad-

6. Creating New Forms of Digital Communications with Social Networking Web Sites

SNWs are "virtual communities on the Internet" where people are provided a forum for communication to share backgrounds, interests, and hobbies.[152] Beginning in 1997, SixDegrees.com developed the first Web site that today would be recognized as a SNW.[153] The site provided the ability to construct a user profile, develop a "friends" list, and explore other users' friends lists to make more connections.[154] With the Internet boom in the late 1990s, SixDegrees.com grew to several million people but failed to develop a sustainable business model.[155] The service was before its time but not by far. Between 1997 and 2001, many Web sites attempted to tap the SNW market, all offering different interfaces and features, but none found the right mix of features, membership, and profitability until Facebook.[156]

Today, Facebook is one of the most popular SNWs, especially among younger people.[157] Facebook launched in 2004 and was originally only available to students at Harvard University before later expanding to other universities, high schools, corporate entities, and eventually to the public at large.[158] In early 2008, within five years of its launch, Facebook reached 150 million users, and now has over 400 million users.[159] By July 2009, Facebook was the

---

vantages include "phone cost savings," "back-channel communications" during conference calls, immediate communications in no talk environments, emergency communications, team bonding, "find-me-wherever-I-am service" to transmit messages from a IM application to a mobile IM application seamlessly, "expertise on demand," and self service "person-to-machine queries").

[152] Ian Byrnside, *Six Clicks of Separation: The Legal Ramifications of Employers Using Social Networking Sites to Research Applicants*, 10 VAND. J. ENT. & TECH. L. 445, 453–54 (2008).

[153] Danah M. Boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, J. COMPUTER-MEDIATED COMM. 210, 214 (2007), http://jcmc.indiana.edu/vol13/ issue1/boyd.ellison.html.

[154] *Id.*

[155] *Id.*

[156] *See id.* (discussing SNWs that were not successful); *see* Posting of Nisan Gabbay, *Facebook Case Study: Offline Behavior Drives Online Usage*, to Startup Review, http://www.startup-review.com/blog/facebook-case-study-offline-behavior-drives-online-usage.php (Nov. 5, 2006) (describing why Facebook's model succeeded); Posting of MG Siegler, *Facebook Crosses 300 Million Users. Oh Yeah, And They Just Went Cash Positive*, to TechCrunch, http://techcrunch.com/2009/09/15/facebook-crosses-300-million-users-oh-yeah-and-their-cash-flow-just-went-positive/ (Sept. 15, 2009).

[157] *See* Quantcast, Facbook.com-Quantcast Audience Profile, http://www.quantcast.com/facebook.com (last visited Apr. 16, 2010) (providing that approximately 125 million people in the United States accessed Facebook in February 2010).

[158] Boyd & Ellison, *supra* note 153, at 218.

[159] Facebook, Facebook – Statistics, http://www.facebook.com/press/info.php?statistics

fourth most-trafficked Web site in the United States.[160]

Facebook's broad appeal derives from the site allowing users to easily share information about themselves to a customizable audience. Users can create and share their own profiles with their personal information, such as their photos, activities, interests, music, television shows, movies, books, and quotations.[161] This allows users to keep up with old friends and even find new friends with common interests.

SNWs like Facebook have shifted from the "foggy vision of geeks" to the baby boom generation with incredible speed.[162] With the influx of multigenerational adopters of Facebook and other SNWs, business have sought to tap the opportunity to establish or expand brand recognition and online sales.[163] For example, Grapekillers, a group of Washington state wineries, created a Facebook page and quickly had 1,500 fans.[164] From Facebook advertising alone, Grapekillers can pack their showroom for a weekend release of a new bottle of wine.[165] In short, SNWs are a powerful communication tool.

7. Voice Communications 3.0

IMs are a great communications tool for two or three individuals, but group chats quickly become overbearing. Because of the delay in the conversation, participants do not know when to type and when to read. The result is a continuous stream of delayed text responses on multiple subjects with no clear purpose or direction. Group chatting in this environment is often confusing and unproductive and has not been adopted as a serious or legitimate form of communication. However, one startup company has a new way to chat that could change that.

TinyChat is a free text, video, audio, and desktop conferencing site where users do not need to sign up for an account, download any software, or have

---

(last visited March 26, 2010).

[160] David Sarno, *Facebook Reports Milestones in Cash Flow, Users*, L.A. TIMES, Sept. 16, 2009, at B4.

[161] *See* Helen W. Gunnarsson, *Law and Technology: Twitter and LinkedIn and Facebook, Oh My!*, 97 ILL. B.J. 288, 290 (2009).

[162] *See* Kevin Patrick Allen, *Ecommerce Know-How: Four Keys to Twitter, Facebook Success*, PRACTICAL ECOMMERCE, Nov. 9, 2009, http://www.practicalecommerce.com/ articles/1358-Ecommerce-Know-How-Four-Keys-to-Twitter-Facebook-Success (last visited March 25, 2010).

[163] *Id.*

[164] *Id.*

[165] *Id. See also* Christopher J. Bucholtz, *Social CRM: Size Matters*, ECOMMERCE TIMES, Nov. 3, 2009, http://www.ecommercetimes.com/rsstory/68537.html (stating that small businesses may be best able to utilize social networking sites).

any technical skill in order to use the site.[166] TinyChat has received critical acclaim for its "dead-simple service" with uses ranging from "offering a simple way to chat with your less-than-tech-savvy friends, to skirting corporate firewalls that block typical instant message protocols."[167] A user can start a new chat room by adding a forward slash and a unique name to the end of the TinyChat URL: typing the address http://tinychat.com/newchatroom will create a chat room called "newchatroom." which can then be shared with whoever the room creator chooses.[168] When a user first accesses the TinyChat Web site, they are prompted to create a unique username.[169] This nickname identifies the individual's contributions to the chat room but does not necessarily identify the individual. After creating their nickname, the user can see up to 12 simultaneous audio-video Webcam streams and over 100 chat participants' text messages.[170]

While the true value of the TinyChat system lies in the need for reliable, easy, and cheap video conferencing, the applicability of the technology underlying the service has broad application across industries. The future of voice communications will continue to shake off the requirements for computers, personally identifying registrations and platform specific protocols in favor of universally available, cross platform, and very simple Web and phone applications.[171]

8. The Next Generation's Phone Call

The next generation will likely have a completely different conception of what it means to make a phone call, and of the underlying technology that makes the phone call possible. Ribbit, which claims to be "Silicon Valley's

---

[166] *See* Posting of Ben Par, *Forget Skype: TinyChat Launches Dead-Simple Video Chat*, to Mashable, http://mashable.com/2009/09/30/tinychat-p2p (Sept. 30, 2009); *see generally* TinyChat, http://www.tinychat.com (last visited Nov. 6, 2009). Tinychat does allow the room creator the option of requiring authentication with a Twitter or Facebook account. *Id.*

[167] Scott Gilbertson, *TinyChat: Disposable, Web-Based Chat Anyone Can Use*, WIRED, Feb. 19, 2009, http://www.wired.com/epicenter/2009/02/tinychat-dispos. *See also* Leena Rao, *Virtual Chat Room TinyChat Adds Video Conferencing and Screen Sharing*, TECHCRUNCH, May 27, 2009, http://www.techcrunch.com/2009/05/27/virtual-chat-room-tinychat-adds-video-conferencing-and-screen-sharing/ (last visited Feb. 8, 2010) ("The video conferencing feature is very easy to use and the quality of the video isn't terrible.").

[168] *See* Leena Rao, *Virtual Chat Room TinyChat Adds Video Conferencing and Screen Sharing*, TECHCRUNCH, May 27, 2009, http://www.techcrunch.com/2009/05/27/virtual-chat-room-tinychat-adds-video-conferencing-and-screen-sharing.

[169] *See* Tinychat, http://www.tinychat.com (last visited Nov. 6, 2009).

[170] Posting of admin, *Tinychat V2 is Live!*, to Tiny Chat Blog, http://tinychatblog.com/tinychat-v2-is-live/ (May 27, 2009).

[171] *See* RITTINGHOUSE & RANSOME, *supra* NOTE 134, § 8.1 at 209–10, § 8.5 at 214–15.

First Phone Company," is taking the next step in voice communications away from the traditional PSTN model.[172] The company has created a free development platform that allows two-way voice integration for any Web site without the need to install additional software.[173] With this new technology, the future of voice communications is limited only by the imagination of Web developers.[174]

Ribbit recently sponsored a development challenge that gave application developers free reign with the development platform to create their most innovative work.[175] Out of 150 applications developed by 500 programmers in thirty countries,[176] the winning five applications show the power of the new platform for voice on the Internet. The application that won the grand prize—called Lucid Viewer—integrated the Ribbit voice module with mapping and street view capabilities to produce "a new mapping and communication experience."[177] With Lucid Viewer, a user will be able to virtually walk down a street and call, using their computer's microphone and headset, or send a text message to an individual merchant's telephone number by clicking on a button that hovers over a picture of the merchant's storefront.[178] Other applications include Ribbit's self-developed Salesforce application, which creates text transcripts of voicemails and can even be used to log and process customers' voice messages.[179] With technology like Ribbit's employed through the Internet, the difference between a phone call and electronic communications virtually disappears.

---

[172] Ribbit Corporation, http://www.ribbit.com (last visited Nov. 6, 2009).

[173] *See* Press Release, Ribbit, Silicon Valley's "First Phone Company" Triples the Size of its Developer Community (Dec. 21, 2007), http://www.ribbit.com/news/releases/122107.php.

[174] In 2008, British Telecommunications purchased Ribbit's voice service for $105 million. Press Release, Ribbit, BT Acquires Ribbit (Dec. 21, 2007), http://www.ribbit.com/news/releases/072908.php. Ted Griggs, Chief Executive of Ribbit, noted the significance of the acquisition:

> The communications industry is entering a new phase. Closed networks are becoming open platforms and developers are now driving innovation. By adding Ribbit's capability to the power of BT's global 21CN platform, we will now be able to give the development community the tools they need to innovate on a global scale.

Id.

[175] Camille Ricketts, *Ribbit Announces Winners of its "Killer" Mobile Apps Competition*, VENTUREBEAT, Mar. 31, 2009, http://venturebeat.com/2009/03/31/ribbit-announces-winners-of-its-killer-mobile-apps-contest/.

[176] *Id.*

[177] *Id.*

[178] *Id.*

[179] *See* Ribbit for Salesforce – What is It?, http://www.ribbit.com/crm/salesforce/what-is-it.php (last visited March 17, 2010).

III. THE STRUCTURE OF FEDERAL WIRETAPPING LAWS

A. Electronic Communications Privacy Act

With the ECPA, Congress sought to provide more stringent protections to the contents of modern electronic communications from unauthorized and unwarranted interception.[180] The ECPA expanded the reach of the federal wiretap provisions under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to include new forms of electronic communications technology.[181] The ECPA wanted a sufficiently wide net to allow courts to protect private conversations from the piercing eyes of their government, the pilfering tendencies of corporate competitors,[182] and the idle temptations of the technically savvy. However, courts have found that the Fourth Amendment provides little privacy protection to technological information exposed to the public.[183]

The ECPA's operating prohibition reads: "any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be [criminally] punished . . . or shall be subject to [civil] suit."[184] A criminal punishment may include fines or up to five years imprisonment.[185] Civil penalties may include injunctive or declaratory relief, and damages of at least $10,000.[186] The statute explicitly exempts from this prohibition individuals who perform maintenance or quality control checks on the service or are acting under the color of law with prior authorization.[187]

In order for law enforcement to obtain a wiretap, they must apply for an ex parte order from a judge within the jurisdiction where the wiretap will be per-

---

180 S. REP. NO. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.

181 *See id.* at 1–3.

182 *See id.*

183 *See, e.g.*, Freedman v. Am. Online, 412 F. Supp. 2d 174, 181 (D. Conn. 2005) ("[F]or purposes of the Fourth Amendment, a subscriber does not maintain a reasonable expectation of privacy with respect to his subscriber information."); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)

> [E]-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.

Id.; United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers . . . [but not] in transmissions over the Internet or e-mail that have already arrived at the recipient.").

184 18 U.S.C. § 2511(1) (2006).

185 § 2511(4)(a).

186 § 2520(a)–(c).

187 § 2511(2).

formed.[188] The order will only be authorized if there is probable cause to believe that "an individual is committing, has committed, or is about to commit a particular offense," and that "particular communications concerning that offense will be obtained through such interception."[189] There must also be probable cause for the "belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased, listed in the name of, or commonly used" by the target of the wiretap.[190] Finally, there must be a showing that "normal investigative procedures" are ineffective or "reasonably appear to be unlikely to succeed if tried or to be too dangerous."[191] Even though the probable cause for a wiretap order is the same as for a warrant for a physical search, the additional requirements of this statute prohibits law enforcement from using wiretaps in the early stages of an investigation and make it one of the hardest types of warrants to obtain.[192] Much of this difficulty is attributable to the ECPA's complex definitions.[193]

1. Wire Communication

Virtually all communication today traverses a wire at some point.[194] *Webster's Dictionary* defines "wire" as a thin metal thread or slender rod for conducting electrical current.[195] In non-technical language, this definition would include every communication that traveled through electrical circuitry.

---

188 § 2518. The wiretap order must be obtained by a judge with jurisdiction over the "place where a communication is initially obtained regardless of where the communication is ultimately heard." United States v. Nelson, 837 F.2d 1519, 1526–27 (11th Cir. 1988).

189 § 2518(3)(a)–(b).

190 § 2518(3)(d).

191 § 2518(3)(c).

192 *See* United States v. Sorapuru, 902 F. Supp. 1322, 1327 (D. Colo. 1995) (explaining that the purpose of the additional requirements "is to ensure that wiretaps are not routinely employed as the first step in criminal investigation.").

193 *See* James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, in 2 Ninth Annual Institute on Privacy and Security Law 543, 547, 560–61 (2008) (arguing that the ECPA is outdated and that the complex language of the Act must be updated in response to technological changes).

194 *See* Mark C. Del Bianco, *Voices Past: The Present and Future of VoIP Regulation*, 14 COMMLAW CONSPECTUS 365, 368 (2006).

195 RANDOM HOUSE WEBSTER'S UNABRIDGED DICTIONARY 2180–81 (2d ed. 2001).

However, the ECPA defines wire communications differently:

> any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce.[196]

The definition contains three components. First, it must be an "aural transfer," meaning there must be an audible voice.[197] *Webster's Dictionary* defines "aural" as "of or pertaining to the ear or to the sense of hearing";[198] however, at least one court has included an electronic recording device capturing a conversation within the definition of "aural acquisition."[199] The transmission of the aural communication does not have to be from a live human speaker as long as a human voice is a part of the communication.[200]

The second section of this definition requires the transmission to be by "aid of wire, cable, or other like connection" at any point.[201] Congress intended this section to include wireless communications from cell phones, satellites, and fiber optic cables.[202] From cell phone circuitry to the electronic switches used to link the cell phone towers to the PSTN, all communications contain a metal wire, satellite, or fiber optic cable at some point between transmission and reception.[203]

The final section of the wire communication definition limits the protection to communications that are furnished or operated by a person who is "engaged in providing or operating such facilities" for local, domestic, or international communications or for communications that affect interstate or foreign com-

---

196 18 U.S.C. § 2510(1) (2006).

197 § 2510(18). The human voice in this concept must be pure, unadulterated human voice at some point between transmission and reception. Some transmissions may be mixed between electronic and aural communications, such as a live video transmission through closed circuit television. Congress intended to include these mixed communications within the meaning of aural if the transmission contains the human voice at some point between transmission and reception. *See* S. REP. NO. 99-541, at 16 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3570.

198 RANDOM HOUSE WEBSTER'S UNABRIDGED DICTIONARY 137 (2d ed. 2001).

199 United States v. Turk, 526 F.2d 654, 657–58 (5th Cir. 1976).

200 *Id.* at 658.

201 18 U.S.C. § 2510(1) (2006).

202 S. REP. NO. 99-541, at 12 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3566 ("[A] wire communication encompasses the whole of a voice telephone transmission even if part of the transmission is carried by fiber optic cable or by radio-as in the case of cellular telephones and long distance satellite or microwave facilities.").

203 *See id. See also* Shubert v. Metrophone, Inc., 898 F.2d 401, 404 (3rd Cir. 1990) (noting that "the intention of Congress to include [cellular] communications within the Privacy Act's protection is apparent from the legislative history . . . .").

merce.[204] The definition remains vague regarding what qualifies as a facility. In some instances, software installed on two computers may be the "facility" for communication.[205] ECPA replaced the "common carrier" language in this section of the definition presumably to expand its reach,[206] but courts are still trying to define the length of that reach.[207]

2. Oral Communication

The ECPA also distinguishes "aural communications" from "oral communications,"[208] which includes "any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception under circumstances justifying such expectation," and explicitly excludes electronic communications.[209] Literally, oral communication is the source of aural communications.[210] However, the purpose of the separate class of communications is to protect against electronic eavesdropping.[211] Congress intended to protect conversations from interception through better-than-normal hearing assistance devices—such as parabolic microphones or remote listening devices—that are not carried through an electronic medium.[212]

3. Electronic Communications

The ECPA's primary purpose was to extend the protections of wire and oral communications to a new category of electronic communications.[213] Congress defined "electronic communication" broadly to include "any transfer of signs,

---

[204] § 2510(1).

[205] *See, e.g.*, SHEPPARD, *supra* note 115, at 1 (discussing the use of Skype in making two-way phone calls over the Internet).

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

[207] *See generally* Timothy J. Miano, *Formalist Statutory Construction and the Doctrine of Fair Warning: An Examination of United States v. Councilman*, 14 GEO. MASON L. REV. 513 (2007) (providing an in-depth look at some of the shortcomings of federal wiretap laws as they apply to technology that was not envisioned during the passage of federal wiretap statutes, and how different circuits have interpreted the statutes).

[208] *See* § 2510(2).

[209] § 2510(2).

[210] WEBSTER'S ENCYCLOPEDIC UNABRIDGED DICTIONARY OF THE ENGLISH LANGUAGE 1361 (1996) (defining oral as "uttered by mouth; spoken.").

[211] *See* S. REP. NO. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567.

[212] *See id.* ("In essence, an oral communication is one carried by sound waves, not by an electronic medium."). *See also* Robert A. Pikowsky, *The Need for Revisions to the Law of Wiretapping and Interception of Email*, 10 MICH. TELECOMM. & TECH. L. REV. 1, 41 (2003).

[213] *Id.* at 1.

signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system."[214] The definition explicitly excludes oral and wire communications, which excludes those communications containing voice.[215] This definition, therefore, includes all electronic communications not transmitted by sound waves, radio waves, or containing the human voice.[216]

4. Intercept

The ECPA prohibits the interception of wire or electronic communications.[217] The Act defines interception as "aural or other acquisition of the *contents* of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[218] The ECPA defines "electronic, mechanical, or other device" as "any device or apparatus which can be used to intercept a wire, oral, or electronic communication other than any telephone or telegraph instrument, equipment or facility, or any component thereof" used by a subscriber, communication service, or law enforcement officer.[219]

Traditionally, storage of electronic communications includes temporary storage while in transmission by a service provider, but does not include, however, long-term storage of communication after transmission has occurred.[220] The ECPA defines storage as "(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 commu-

---

[214] 18 U.S.C. § 2510(12).

[215] § 2510(12) (listing three other exceptions: "(B) any communication made through a tone-only paging device; (C) any communication from a tracking device...; or (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.").

[216] S. REP. NO. 99-541, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568.

> As a general rule, a communication is an electronic communication protected by the federal wiretap law if it is not carried by sound waves and cannot fairly be characterized as containing the human voice. Communications consisting solely of data, for example, and all communications transmitted only by radio are electronic communications. This term also includes electronic mail, digitized transmissions, and video teleconferences.

Id.

[217] 18 U.S.C. § 2511(1)(a) (providing a prohibition against any person who "intentionally *intercepts*, endeavors to *intercept*, or procures any other person to *intercept* or endeavor to *intercept*, any wire, oral, or electronic communication.") (emphasis added).

[218] § 2510(4) (emphasis added).

[219] § 2510(5).

[220] Computer Crime & Intellectual Prop. Section, U.S. Dep't of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 123 (3d ed. 2009), *available at* http://www.cybercrime.gov/ssmanual/index.html.

nication service for purposes of backup protection of such communication."[221] Since electronic transmissions occur within milliseconds, determining the difference between the transmission and the temporary or permanent storage of electronic communications is challenging.[222] However, the current trend is to require that the intercepting acquisition be contemporaneous with the transmission.[223]

5. Commerce Clause Limitation

The Commerce Clause limits the scope of the ECPA.[224] Congress has used an activity's impact on interstate commerce as the basis to enact many statutes across a range of issues.[225] Traditionally, the Supreme Court has interpreted "interstate commerce" to include the greatest possible reach of the Commerce Clause.[226] However, the amount of influence a technology must exert on interstate commerce to qualify is not apparent.

Wickard v. Filburn provides the controlling test: if an activity "exerts a substantial economic effect on interstate commerce," regardless of whether or not it is considered to be commerce, it is within the purview of the Commerce Clause and Congress's regulatory arm.[227] *Perez v. United States* further expanded the reach of the Commerce Clause, stating "where the class of *activities* is regulated and that class is within the reach of federal power, the courts

---

221 § 2510(17).

222 *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 n.6 (9th Cir. 2002); Bohach v. City of Reno, 932 F.Supp. 1232, 1236 (D. Nev. 1996). *See also* Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 383–87 (2009).

223 *See* United States v. Councilman, 418 F.3d 67, 79 (1st Cir. 2005) (noting that e-mail messages, stipulated as electronic communications within the scope of the Wiretap Act, are included within the definition of 'intercept' even though they may be stored in temporary memory while in transition to a final destination); *Konop*, 302 F.3d at 878 (finding that due to Congress' amendment of the Wiretap Act, a Web site can only be "intercepted" during transmission, not when it is in electronic storage).

224 *Compare* § 2510(1), (12), *with* U.S. CONST. art. 1, § 8, cl. 3.

225 *See, e.g.*, 8 U.S.C. § 1375a(b)(5)(B) (regulating international marriage brokers); 15 U.S.C. § 1644(a) (penalizing the fraudulent use of credit cards); 18 U.S.C. § 38 (penalizing fraud involving aircraft or space vehicle parts).

226 *See* Scarborough v. United States, 431 U.S. 563, 577–78 (1963); Citizens Bank v. Alafabco, Inc., 539 U.S. 52, 56 (2003) (per curiam).

227 Wickard v. Filburn, 317 U.S. 111, 125 (1942). *Wickard* involved a wheat farmer who exceeded the Secretary of Agriculture's limitations in growing wheat on his farm for his personal consumption. *Id.* at 115. Even though the crops were being grown only for the farmer's personal consumption, the Court held that it had a substantial enough impact on interstate commerce to bring it within Congress' authority to regulate. *Id.* at 125.

have no power 'to exercise, as trivial, individual instances' of the class."[228]

However, the Supreme Court drew the line in *Lopez v. United States* when it held the Gun-Free School Zones Act unconstitutional because the law–which prohibited bringing guns onto school campuses–was not sufficiently related to interstate commerce—and thus outside of Congressional authority under the Commerce Clause.[229]

B. Stored Communications Privacy Act

Congress also sought to protect stored communications with the inclusion of the Stored Communications Act ("SCA").[230] The SCA prohibits the unauthorized access to an electronic communications service or facility "and thereby obtain[ing], alter[ing], or prevent[ing] authorized access to a wire or electronic communication while it is in electronic storage . . . ."[231] Electronic storage is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission" and any backup of those communications by the service provider.[232] The Fifth Circuit analyzed the interrelationship of the ECPA and the SCA and concluded:

> Congress' use of the word "transfer" in the definition of "electronic communication", and its omission in that definition 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 those communications are in "electronic storage."[233]

From this complicated interrelation, a working definition of stored communications is revealed. When a communication is in transmission between the source and the destination, the ECPA governs.[234] However, when a communication reaches its destination, the SCA governs.[235] For example, an e-mail is in

---

[228] Perez v. United States, 402 U.S. 146, 154 (1971) (quoting Maryland v. Wirtz, 392 U.S. 183 (1968)).

[229] Lopez v. United States, 514 U.S. 549, 561 (1995).

[230] Pub. L. No. 99-508, tit. II, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–2712 (2006)).

[231] § 2701(a).

[232] § 2510(17).

[233] Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461–62 (5th Cir. 1994).

[234] *See* United States v. Rodriguez, 968 F.2d 130, 136 (2d Cir. 1992) ("[W]hen the contents of a wire communication are captured or redirected in any way, an interception occurs at that time.").

[235] *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1072–73 (9th Cir. 2004).

> The [Stored Communications] Act reflects Congress's judgment that users have a legitimate interest in the confidentiality of communications in electronic storage at a communications facility. Just as trespass protects those who rent space from a commercial storage facility to hold sensitive documents . . . the Act protects users whose electronic communications are in electronic storage with an ISP or other electronic

storage when it is in the drafts folder of the sender's mailbox. The message is in transmission from the moment that the sender presses "send" until the moment the e-mail is opened. If the email service stores a copy of the message in the "Sent Items" folder, then that copy remains in storage while the transmitted copy is in transmission for 180 days. Before 180 days have passed, the SCA requires a warrant to be issued to allow government access to the electronic communication.[236] After 180 days have passed, the SCA allows "law enforcement to obtain documents in storage . . . with just a subpoena or court order," which requires "a showing of less than probable cause."[237] Determining whether an e-mail is in transmission or in storage is critical for a law enforcement officer seeking to wiretap the communication under an ECPA heightened requirements for a warrant or a court order under the SCA. This determination is also one of the most arbitrary of federal wiretapping laws.

IV. ANALYSIS

In order to discuss how the federal wiretapping statutes apply to the ECPA and SCA interception of modern communications technologies, it must be assumed that it is technically possible to intercept and decrypt the contents of the different communications technologies. Some of the technologies include advanced encryption algorithms and open source coding to prevent clandestine attempts to integrate back doors by government and civilian interceptors.[238] These developments have made it increasingly difficult to execute an instantaneous wiretap on some communications services.[239] However, since interception technology grows at the speed of communication innovation, eventually every communications technology will spawn its own interception technology. If this assumption is incorrect, then the applicability of the ECPA and SCA to this technology is merely academic.

---

communications facility.

Id.

[236] 18 U.S.C. § 2703(a) (2006).

[237] Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 382–93 (2009); § 2703(b).

[238] *See, e.g.*, SHEPPARD, *supra* note 115, at 3.

[239] Andy Greenberg, *Wiretapping's Fuzzy Future*, FORBES.COM, May 15, 2008, http://www.forbes.com/2008/05/15/wiretapping-voip-lichtblau-tech-security08-cx_ag_0515wiretap.html.

A. Traditional VoIP

Traditional VoIP easily falls within the first two sections of the definition of wire communications. It is limited and dedicated to transmitting the human voice from a source to a destination making it an aural transmission.[240] Even if a computer recording initiates a communication, such as commonly done by telemarketers or political campaigns, the human voice is still heard by the recipient, which thus qualifies it as an aural transfer. Furthermore, wires are used at some point between the transmission and destination during this communication.[241]

VoIP must still satisfy the remaining prong outlined by the statute: the wire aiding the communication must be provided by a facility that ordinarily operates facilities for communication for interstate or foreign commerce.[242] Since VoIP works in conjunction with an Internet connection, it uses an ISP's wires and facilities to supply the communication.[243] However, not all VoIP providers also function simultaneously as ISPs.[244] For those companies that do provide ISP and VoIP services, the communication is likely to fall within the definition of a wire communication.[245]

Whether non-ISP based VoIP providers fall under the federal wiretapping statutes may depend upon their effect on interstate or foreign commerce. To assert that such VoIP providers should be included under the wiretapping statutes would require looking at the market and the number of VoIP providers in the aggregate to show the number of users, as well as the monthly rate, to show a substantial impact on traditional PSTN providers.[246] However, the FCC has excluded VoIP from state regulation as common carriers[247] and has declined to

---

[240] S. REP. NO. 99-541, at 12 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3566 (defining "wire communication" as "includ[ing] existing telephone service, and digitized communications to the extent that they contain the human voice at the point of origin.").

[241] *See* S. REP. NO. 99-541, at 12 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3566; *see also* 18 U.S.C. § 2510(1).

[242] *See* § 2510(1); *see also* discussion *supra* Part III.A.i.

[243] *See* GRALLA, *supra* note 96, at 121–23.

[244] *Cf.* H. Russell Frisby, Jr. & David A. Irwin, *The First Great Telecom Debate of the 21st Century*, 15 COMMLAW CONSPECTUS 373, 393 (2007).

[245] *See* S. REP. NO. 99-541, at 12, *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3566 ("Wire communication encompasses the whole of a voice telephone transmission even if part of the transmission is carried by fiber optic cable or by radio, as in the case of cellular telephones and long distance satellite or microwave facilities.").

[246] *Cf.* Wickard v. Filburn, 317 U.S. 111, 128 (1972) (holding that the production of a product, when viewed in the aggregate, can have a significant impact on market policies). Under the *Wickard* principle, VoIP providers should be viewed in the aggregate to determine their impact on interstate commerce.

[247] *See In re* Vonage Holdings Corporation Petition for Declaratory Ruling Concerning an Order of the Minnesota Public Utilities Commission, *Memorandum Opinion and Order*,

classify VoIP as subject to its Title II regulations.[248] With the rapid changes and myriad of options in modern communications, it may be impossible to ever accurately determine the impact of any one technology on interstate commerce.

B. Instant Messaging

Analyzing IM in the context of federal wiretapping laws requires two different categories of messaging: standard and enhanced. Standard IM services include the original text-based communications.[249] Enhanced IM services include the ability to transmit voice and video along with text-based communications.[250]

1. Standard Messaging

By excluding voice from the standard messaging category of IM applications, standard IM services are excluded from the wire communications definition because they are not an aural communication.[251] However, text-based IM is closely related to one of the listed examples, "writing," in the electronic communication definition, and would likely fit within the first part of the definition.[252]

However, courts have held that the use of chat rooms open to the general public offer users no reasonable expectation of privacy and therefore do not need any warrant at all to intercept.[253] For example, in *United States v. Maxwell*, the court held that "[m]essages sent to the public at large in the 'chat room' or e-mail that is 'forwarded' from correspondent to correspondent lose any semblance of privacy."[254]

However, many instant messaging applications involve private communications that are easily distinguished from the "public at large" approach because they are only between two individuals.[255] For example, in *United States v.*

---

19 F.C.C.R. 22,404, ¶ 1 (Nov. 9, 2004).

[248] *See* Kevin Ryan, Comment, *Communications Regulation—Ripe for Reform*, 17 COMMLAW CONSPECTUS 771, 791 (2009).

[249] James B. Speta, *A Common Carrier Approach to Internet Interconnection*, 54 FED. COMM. L.J. 225, 238 (2002).

[250] *Id.* at 237–38.

[251] *See* 18 U.S.C. § 2510(1), (18) (2006).

[252] § 2510(12).

[253] *See* United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996); United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997).

[254] *Maxwell*, 45 M.J. at 419.

[255] *See* MICHAEL MILLER, ABSOLUTE BEGINNER'S GUIDE TO COMPUTER BASICS 268–72 (2d ed. 2004); *see also Maxwell* 45 M.J. at 418–19 (distinguishing the expectation of pri-

Meek, the court analyzed the expectation of privacy between two people in an online chat, and found it to be similar to a phone call in that "either party . . . has the power to surrender each other's privacy interest to a third party."[256] Commentators have suggested that courts that reject an individual having a reasonable expectation of privacy in private chat rooms have failed to uphold the protections that Katz provides. Aya Gruber has noted that:

> [T]hese courts deem private chat rooms unprotected simply because there is a potential that an anonymous conversant may breach confidences. This paves the way for holding that private chat room or instant message conversations may be monitored by the police, even when none of the participants has consented to interception.[257]

If a court holds that an individual has a reasonable expectation of privacy in a private IM conversation, the question then becomes whether IM falls under the long arm of the Commerce Clause. IM is an invention of and for the Internet.[258] IM services cannot fairly be included in the same class of activities as e-mail because the purpose of IM is for instantaneous communication, [259] while the purpose of e-mail is to have a letter-based conversation.[260] Similarly, IMs cannot fairly be included within a class of phone calls because the technology has the inherent ability to carry on multiple conversations with groups and individuals independently and simultaneously.[261] Furthermore, IM services are typically offered at no cost to users.[262] Defined in its broadest context, IM is part of a class of communications activities that exist on the Internet. In the narrowest context, IM is its own separate and distinct technology.

With the vast amount of communications that traverse the Internet, it would be overly inclusive to categorize all of those communications as part of the same class of activities for commerce clause purposes. A law enforcement of-

---

vacy that is lacking in e-mail exchanges due to the ability of the e-mail to be stored, with the expectation of privacy that can be found in IMs or other 'real time' transmissions, due to the inherent nature of those communications to be "lost forever").

256 United States v. Meek, 366 F.3d 705, 711 (9th Cir. 2004). *See also* Paul Ham, *Warrantless Search and Seizure of E-Mail and Methods of Panoptical Prophylaxis*, 2008 B.C. INTELL. PROP. & TECH. F. 090801, at *9–10 (2008), *available at* http://bciptf.org/index.php?option=com_content&task=view&id=42&Itemid=30 (comparing IM communications to private e-mails, and likely having a similar expectation of privacy).

257 Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What Katz is Made Of?*, 41 U.C. DAVIS L. REV. 781, 815 (2008).

258 *See* RITTINGHOUSE & RANSOME, *supra* note 134, § 1.3.1, at 3–4 (2005).

259 *See* MILLER, *supra* note 255, at 267 (2d ed. 2004) ("Instant messaging is the ideal medium for very short, very immediate messages.").

260 *Id.* at 259 ("An email message is like a regular letter, except that it's composed electronically and delivered almost immediately via the Internet.").

261 *See, e.g.*, PETER SAINT-ANDRE, ET AL., XMPP: THE DEFINITIVE GUIDE 77–81 (2009); *but see supra* text accompanying note 292.

262 *See, e.g.*, Meebo, Meebo Products, http://www.meebo.com/products/ (last visited March 16, 2010).

ficer should not have to get an ECPA search warrant to view a Web site that is available to anyone with a Web browser. Nor should a private chat be subject to fewer protections than a phone call merely because the words are written. Similarly, by signaling out each technology as a separate class, the impact of any individual technology on interstate commerce will result in arbitrary distinctions based on the popularity of the technology at a given time. Modern communications must be regulated based upon the privacy of the communication transmitted and not the popularity of the medium used to transmit that communication.

If a court holds that an individual does not have a reasonable expectation of privacy in a private IM conversation, then the existence of encryption in these technologies may play a determinative factor. While some IM services include encryption, the existence and effectiveness of this encryption is not controlling when determining whether a wiretap is illegal.[263] In 1990, the United States Court of Appeals for the Third Circuit held that the Wiretap Act did not expressly require wireless carriers to provide encryption for cellular transmissions,[264] because Congress changed the "required *mens rea*" for a violation of the statute from "willful to intentional."[265]

However, much has changed in communications from the 1990s until today. Encryption has vastly improved and is included seamlessly and cheaply on many different communications technologies.[266] Since this is a relatively untested area of the law, a court may one day hold that an encrypted communication should be treated differently from an unencrypted communication.

2. Enhanced IM

The vast expansion of IM capabilities has created a new class of technologies that separates itself from its ancestors. As in the water utility analogy discussed earlier, when only text is flowing through the pipes, it is a more straightforward analysis for interception. However, when these pipes have the ability to include voice, images, documents, pictures, and video, the complex-

---

[263] *Cf.* Shubert v. Metrophone, Inc., 898 F.2d 401, 405–06 (3rd Cir. 1990) (finding that "Congress could not have intended that the transmission of a cellular signal to an intended recipient be considered an intentional divulgence based merely on the circumstance that technology exists which could make interception more difficult or not possible.").

[264] *Id.* at 405.

[265] *Id.* at 405–06 ("Under the Privacy Act . . . it is unlawful for the communications provider to 'intentionally divulge the contents' of a communication . . . we cannot equate transmission to divulgence even though the transmission may be readily intercepted.").

[266] *See* Mark Mayne, *Encryption - Past, Present and Future*, SECURE COMPUTING MAGAZINE, Sept. 9, 2009, at 32.

ity for interception magnifies.

For example, Google Talk, Google's enhanced IM program, separates VoIP and text packets into separate protocols for network efficiency.[267] Essentially, Google Talk creates two different pipes; one pipe falls under the standard IM analysis, while the other falls under the traditional VoIP analysis. Because Google Talk uses a server-based routing of VoIP calls,[268] it is therefore closely analogous to the traditional VoIP configuration, with the exception that Google's service is free. Configuring a network analyzer to only look for one type of IM protocol might narrowly fit within the definitions of ECPA but there are dozens of different types of IM services using many different IM technologies. The Fourth Amendment's particularity requirement would result in law enforcement officers, attorneys, and magistrates becoming experts in telecommunications to determine which content stream to tap for which technology.

3. Chat on Demand Web Sites

The analysis of enhanced IM also applies to modern chat Web sites, with one large exception: chats are exposed and thus, the user may not have a reasonable expectation of privacy.[269] Without purchasing an encryption and password protection packet, nothing prevents an unwanted user from stumbling upon the chat room and reading or listening to the conversation.[270] Daniel Blake, TinyChat.com's co-founder, has stated that chats held on the Web site are private because "only those who know the link can enter [the] video chat room."[271] While this may provide some level of security in a practical sense,

---

[267] *See* Summary of XMPP, http://xmpp.org/about/summary.shtml (last visited Oct. 8, 2008); Google, Google Talk for Developers, http://code.google.com/apis/talk/open_communications.html (last visited Jan. 23, 2010) (providing that Google Talk uses the standard XMPP protocol for authentication, presence, and messaging).

[268] *See* Google, Google Talk for Developers, http://code.google.com/apis/talk/open_communications.html (last visited Jan. 23, 2010).

[269] *See* United States v. Charbonneau, 979 F.Supp. 1177, 1185 (S.D. Ohio 1997) (holding that there was not a "reasonable expectation of privacy in the chat rooms"). *See also* Reno v. American Civil Liberties Union, 521 U.S. 844, 870 (1997) (noting that "through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox").

[270] *See* Posting of Robin Wauters, *TinyChat Makes Creating Disposable Chat Rooms a Breeze*, to Mashable, http://techcrunch.com/2009/02/18/tinychat-makes-creating-disposable-chat-rooms-a-breeze/ (Feb. 18, 2009).

[271] Max Zeledon, *Growing Pains for Online Video Chat*, BUSINESS WEEK ONLINE, May 8, 2009, http://www.businessweek.com/technology/content/may2009/tc2009056_365774.htm.

whether this provides a level of privacy under the wiretapping laws remains to be seen.

C. Decentralized VoIP

Like unencrypted IM communications, decentralized VoIP communications such as those provided by Skype may reduce the reasonable expectation of privacy below the threshold of the federal wiretap laws. Because all communications pass from one computer to the next, the packets are "exposed" to the public, even if only in a fragmented form.[272] Decentralized VoIP moves much like an armored battalion through a city. Instead of the protection existing all around the communication stream, like the pipe in a water system, in decentralized VoIP, the packets include encryption like the armor on a tank.[273] The entire battalion does not take one path through the city, but distributes itself through the various streets and reassembles at the other end in the same formation it started. Similarly, Skype encrypted packets take the quickest path through the fastest super nodes coming together at the other end.[274] During the time the packets are flowing through the P2P network, they are exposed to the public with only their encryption armor for protection.

Cracking the high levels of encryption is exceptionally difficult for even the most powerful supercomputers.[275] Additionally, since only part of any commu-

---

[272] *See* P2P Telephony Explained, *supra* note 118 (noting that Skype encrypts the packets for privacy protection because all Skype calls are publicly routed through "the public Internet").

[273] Data encryption algorithms encode readable information into unreasonable information. An algorithm is defined as a "mathematical formula for an operation, such as computing the check digits on packets of data that travel via packet switched networks." HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 115 (25th ed. 2009). An encryption is defined as "the transformation of data into a form unreadable by anyone without a secret decryption key. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended." *Id.* at 434.

[274] *See* SHEPPARD, *supra* note 115, at 2–3 (2006).

[275] *See* Cracking Encryption Algorithms, MyCrypto.net, http://www.mycrypto.net/encryption/encryption_crack.html (last visited Nov. 6, 2009). MyCrytpo.net theorizes it would take a retail CPU that could process one billion keys per second and include one million of these processors in a supercomputer. With 100 of these supercomputers working in a network with peak performance and no downtime it would take twenty thousand years to process all of the possible key combinations. Even factoring a doubling of technological growth every eighteen months the possibility that a single phone conversation could be cracked in a person's lifetime is literally impossible without a revolutionary new invention. *Id.*

However, a large supercomputer may not be necessary to break encryption. In 1997, a software company accepted a ten thousand dollar challenge to break a specific kind of sixty-four bit encryption. Using distributed network computing, in which a large group of computers' idle processing power is pooled into a network supercomputer, it took three hundred

nication will flow through a user's computer and the technology allows a large number of clients and simultaneous phone calls, an interceptor, even if he were able to overcome the encryption, would only get a small piece of the content.[276] However, since the network operates on a mostly open source P2P network, with pieces of the source code freely available to the public, creative software engineers may be able to trick the network into diverting all communications from a particular individual through a single, or group of, computers, and thereby compile all of the packets of a conversation.[277]

Traditionally, most communications worked along a steady stream of data flowing from source to destination and a wiretap intercepted the communications by tapping into and diverting that stream to a third party.[278] However, by decentralizing the communications, anyone in the decentralized VoIP network could have part of that data stream flow directly through their computer making them at least a subdestination in route to the final destination.[279] Whether the compilation and de-encryption of packets sent through a public environment is the same as an interception of communications is an open question for the courts.

D. The Next Generation of Phone Calls

The next generation of digital communications will stretch the definition of aural acquisition. Programs like Ribbit can transform voice data into textual transcripts of the message.[280] This one-way communication is partially aural because a modulated voice synthesis prompts the human voice message.[281] The transcribed message remains a "stored" communication because it resides in the user's mailbox,[282] but once the message is read on a cell phone, it is consid-

---

thousand computers four years to find the key. *See* Andy Patrizio, *Codebusters Crack Encryption Key*, WIRED, Oct. 7, 2002, http://www.wired.com/science/discoveries/news/2002/10/55584.With the explosion of peer-to-peer networks and the rapid growth of processing power in home PCs in the past decade, the computing power necessary to break this encryption may reside within the same networks that are carrying phone calls.

[276] *Cf.* SHEPPARD, *supra* note 115, at 1–2.

[277] *Cf. id.* at 170–73.

[278] *See* People v. Chavez, 44 Cal. App. 4th 1144, 1149–50 (1996) (distinguishing electronic interception or wiretapping usually involves the connection to the wires, while electronic eavesdropping, or bugging, involves all other forms of electronic surveillance).

[279] *See* SHEPPARD, *supra* note 115, at 2–3.

[280] Ribbit, Ribbit for Salesforce – How it Works, http://www.ribbit.com/crm/salesforce/how-it-works.php (last visited Feb. 10, 2010).

[281] *See* S. REP. NO. 99-541, at 16 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3570 (providing that aural means the unadulterated human voice).

[282] *See* 18 U.S.C. § 2701(a) (prohibiting unauthorized access to communications stored

ered to be an electronic transmission. With technology like this, the line between stored and transmitted communications is exceptionally unclear.

If the program accepts voice prompts to navigate a Web site or database, then the communication qualifies as a wire communication because it contains voice transmitted over a wire.[283] However, the difference is that this communication is between an individual and a computer,[284] which is not the type of communication that Congress sought to protect with the ECPA.[285] If the same interaction happened with a keyboard and mouse it would not qualify as a wire communication because it would lack the human voice to make it an aural communication. Because of the particularity requirement in the Fourth Amendment, it is vital for law enforcement officers and magistrates to know which provision of the wiretapping statute is being used when issuing a wiretapping order. This surety is virtually impossible when applying the current statutory scheme to modern communications mediums.

V. THE STRUCTURAL FRAMEWORK FOR NEW WIRETAPPING LEGISLATION

Modern communication follows Moore's law: technology grows exponentially.[286] Congress follows the turtle law: slow and steady wins the race. Nonetheless, Congress must overhaul the categorical definitions of ECPA and the artificial distinction between stored and in-transmission communications and replace it with a more holistic regulation that can handle innovation.

Instead of letting the technology govern the structure of wiretapping laws, Congress should let the use of technology govern the laws. In *Katz*, the Court reviewed a FBI's electronic eavesdropping of a bookie using a public telephone.[287] The agents attached a listening device to the outside of the glass-enclosed phone booth and listened in to the conversation between the bookie

---

in "electronic storage system[s]").

283 *See* 18 U.S.C. § 2510(1).

284 *See* Press Release, Ribbit, Ribbit for Salesforce: Voice Automation for Salesforce.com on the Appexchange (Oct. 2008), *in* CRM MAGAZINE, Oct. 2008, at 7.

285 *See* S. REP. NO. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3567.

286 *See* William Aspray, *Preface*, *in* CHASING MOORE'S LAW: CHASING INFORMATION TECHNOLOGY IN THE UNITED STATES (William Aspray ed., 2004). Moore's law is a way to "quantitatively describe the pace of innovation in the semiconductor industry." It states that "the number of electronic switches that can be placed on a computer chip doubles every 18 months." This practical concept has become a "metaphor for the rapid, incessant course of technological innovation that is occurring in the computing and communications field." *Id.* at ix.

287 Katz v. United States, 389 U.S. 347, 348 (1967).

and the gamblers.[288] The Court declared this listening to be an unlawful search because "[o]ne who occupies [a phone booth and makes] a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[289] Despite Katz's physical exposure to the public—that anyone could look through the glass and into the phone booth to see him—the Court held that he was entitled to a reasonable expectation of privacy in his conversation.[290] This distinction exists because:

> the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[291]

Thus a two-part test governs when a person may have a constitutionally protected conversation. The first part of the *Katz* test is that the person must "have exhibited an actual (subjective) expectation of privacy.[292] This prong requires that a person, in claiming that the Fourth Amendment protects their communication, must show that they expected their communication to be private.[293] In the context of communications, an individual has a subjective expectation of privacy when they have a telephone conversation with another party and is not aware that other parties may be listening in by speakerphone.[294]

The second part of the *Katz* test is that the expectation must be something that society is willing to recognize as reasonable.[295] In applying this to the context of communications, courts tend to find that someone who sends an e-mail to another has a subjective expectation of privacy.[296] As one federal court found, "With regard to email communications . . . '[a]lthough e-mail communication, like any other form of communication, carries the risk of unauthorized disclosure, the prevailing view is that . . . confidential information [may

---

288 *Id.*

289 *Id.* at 352–53.

290 *Id.*

291 *Id.* at 351 (internal citation omitted).

292 *Id.* at 361 (Harlan, J., concurring).

293 *Id.* at 351. For example, in *California v. Ciraolo*, the Supreme Court held that a person who grew marijuana in his backyard behind a six-foot outer fence and ten-foot inner fence that completely enclosed his backyard had exhibited a clear "manifest[ation] of his own subjective intent and desire to maintain privacy . . . ." California v. Ciraolo, 476 U.S. 207, 209–211 (1986).

294 *See, e.g.*, State v. Christensen, 102 P.3d 789, 792 (Wash. 2004) (holding that the defendant had a reasonable expectation of privacy in a telephone conversation with his girlfriend when her mother would listen in via a speakerphone).

295 *Katz*, 389 U.S. at 361 (Harlan, J., concurring). In *Ciraolo*, even though Ciraolo sought to shield his backyard from outside viewers, the Court held that that subjective belief did not "preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible." *Ciraolo*, at 213.

296 *See* Brown-Criscuolo v. Wolfe, 601 F.Supp 2d 441, 449 (D.Conn. 2009).

be communicated] through unencrypted e-mail with a reasonable expectation of privacy.'"[297]

Not every communication through the Internet has a "constitutionally protected reasonable expectation of privacy,"[298] but some communications qualify as having both subjective and objective expectations of privacy. The design and use of a communications medium plays a large factor in determining the appropriate level of privacy. After a thorough analysis of all of the modern forms of communications, three categories emerge in determining the reasonableness of a user's expectation of privacy in their communication: public, quasi-public, and private communications.

A. Public Communications

Public communications are those in which there can be no constitutionally protected expectation of privacy. These communications, for Fourth Amendment purposes, are a broadcast to the world.[299] Examples of strictly public electronic communications include hosting a Web site or posting a comment on a blog.[300] However, even these activities may create a subjective or objective expectation of privacy. For example, a person may have a subjective and objective expectation of privacy to their bank transaction information posted on their bank's Web site if it is hosted on a secure Web site and is protected by a username and password.[301] If a communication is truly exposed to the public, then Congress should not attempt to blind law enforcement from viewing the content and no warrant should be necessary to view that material.

The majority of SNW communications are public communications that are

---

[297] *Id.* (citing *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 256 (Bankr. S.D.N.Y. 2005)).

[298] *See Katz*, 389 U.S. at 360.

[299] *See, e.g.*, Edwards v. Bardwell, 632 F.Supp. 584, 589 (M.D.La. 1986), *aff'd* 808 F.2d 54 (5th Cir. 1986) (holding that a conversation broadcast over a radio transmission is not protected by the Fourth Amendment).

[300] *See* United States v. Gines-Perez, 214 F. Supp.2d 205, 225–26 (D.P.R. 2002) (stating that people who post material on the Web sites have no reasonable expectation of privacy).

[301] *See* WAYNE R. LAFAVE, 1 SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.6(f), at 721 (4th ed. 2004).

> The technology for limiting telephone access to computer files is not foolproof, and thus "hackers" sometimes manage to penetrate through the safeguards and reach supposedly private information. However, that risk alone is hardly sufficient to deprive these records of a justified expectation of privacy under *Katz*. 'Reliance on protections such an (sic) individual computer accounts, password protection, and perhaps encryption of data should be no less reasonable than reliance upon locks, bolts, and burglar alarms, even though each form of protection is penetrable.'

Id. § 2.6(f), at 721.

broadcasted to the world or a large group of individuals invited to view the content. Any information that is visible on these SNWs to any other registered member of the SNW should be considered a public communication.[302] This may include status updates, pictures, comments, group affiliations, and other personal details that individuals chose to reveal.

B. Quasi-Public Communications

Quasi-public communications are those communications which are otherwise public communications, but are used in such a way that there is a reasonable expectation of privacy attached to their use. Congress should afford these some level of protection under the Fourth Amendment, depending on the steps taken to secure the communications from general public disclosure. If there is a legitimate expectation of privacy, then a standard search warrant should be required for law enforcement to view this material.

Some SNW allow users to highly restrict dissemination of their information to selective groups of other users.[303] When these privacy filters are configured, a more fact-intensive inquiry must be conducted to determine the subjective intent of the individual to keep that information private. For example, if a SNW user restricted all of the content on his or her Web site to only those friends with whom he or she was personally closest to, then the information carries *some* expectation of privacy. However, if this same individual freely opens their content to people he or she does not know well, then there should be little expectation of privacy to this content.

The distinction is akin to social interactions outside of the electronic realm. Personal information that an individual shares with anyone they meet is not considered to be private information.[304] However, information that is only shared with a person's most trusted confidants carries at least some expectation that that information will not be shared publicly.[305]

C. Private Communications

Private communications are those that carry a presumption of privacy be-

---

[302] *Cf.* Smith v. Maryland, 442 U.S. 735, 743–44 (1967) (holding that a person has no legitimate expectation of privacy in the information they freely provide to others).

[303] *See* JESSE FEILER, HOW TO DO EVERYTHING: FACEBOOK APPLICATIONS 33–34 (2008) (showing how a user of Facebook can limit access of their content to "[a]ll my networks and all my friends", "[s]ome of my networks and all my friends . . .", or to "[o]nly my friends").

[304] *See Smith*, 442 U.S. at 743–44.

[305] *See Katz*, 389 U.S. at 351 ("[W]hat [someone] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.").

cause the nature of the communication would lead reasonable individuals to believe that they are having a private communication. Congress should afford these types of communications the highest levels of protection under the Fourth Amendment and require a strong showing of need, similar to the ECPA's requirement, when law enforcement seeks to wiretap this type of communication.

A phone call between two individuals—whether it exists over the PSTN, VoIP, instant messaging, Skype, or even the next generation Web integrated voice communication—is not intentionally exposed to the public. When people use these forms of technologies to communicate, they expect their conversation to remain private from the outside world. When this type of communication is combined with leading-edge encryption technology, the subjective expectation of privacy in that communication should increase.[306] Likewise, an IM between two individuals is the equivalent of a phone call in written form and should carry the same protections as a phone call.

VI. CONCLUSION

The current balance struck between ensuring the privacy of communications and legitimate law enforcement investigation techniques fails to provide an adequate framework for modern communications. As the lines between categorical wire, oral, and electronic, and stored communications blur, the balance will become even more detrimental to both sides of the equation. A broad redesign of wiretapping law is required to rebalance the competing interests of privacy and law enforcement.

---

[306] *See* Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 56–57 (2008) ("[M]any employees seemed to see the use of encryption as a signal or flag of the secrecy of a message.").