Voice over Internet Protocol and the Wiretap Act: Is Your Conversation Protected?

Daniel B. Garrie,[†] *Matthew J. Armstrong,*[‡] *& Donald P. Harris*[*]

10101101: Is this sequence of digits voice or data? To a computer, voice is a sequence of digits and data is a sequence of digits. The law has defined 10101101 to be data, and 10101001 to be voice communications. Courts have constructed a distinction between data, 10101101, and voice, 10101001. However, that distinction is blurred when voice and data are simultaneously transmitted through the same medium. The courts forbid third parties to tap or monitor voice communications, yet permit data packets to be tracked, stored, and sold by third parties with the implied consent of either party engaged in the transaction. Prior to the convergence of voice and data into a single transmission medium, courts were able to enforce the distinction between voice and data communications by constructing the clickstream data exemption to the Wiretap Act. With the onset of Voice over Internet Protocol (VoIP) and comparable technologies, the privacy rights assigned to 10101101 (data) or 10101001 (voice) have been blended such that it is unclear whether voice communications using VoIP are protected.

---

† Daniel B. Garrie, J.D. Candidate, Rutgers University School of Law, May 2006 with a focus in Cyber Law Litigation; M.A. Computer Science, Brandeis University, 2000 with course work in Artificial Intelligence; B.A., Computer Science, Brandeis University, 1999. Mr. Garrie has, over the past eight years, worked with the Department of Justice (DOJ) and other large organizations as an Enterprise Technical Architect, focusing on web-enabled enterprise systems.

‡ Matthew J. Armstrong, J.D. Candidate, Rutgers University School of Law, May 2006 with a focus on Corporate and Securities Law; B.A. Economics, Drew University, 2002, Summa Cum Laude. Mr. Armstrong currently works as a law clerk for Kenney & Kearney LLP, a law firm specializing in complex civil and criminal litigation.

* Donald P. Harris, LL.M. is an Assistant Professor of Law at James E. Beasley School of Law, Temple University, where he teaches courses focusing on intellectual property, international intellectual property, and commercial law. He previously taught as an Adjunct Professor at Golden Gate Law School, San Francisco, California.

Much thanks to our contributors: Mr. William R. Burdett and Mr. Carlo Cardilli. Mr. Burdett is currently Senior e-Government Architect, Office of the CIO, DOJ. Mr. Cardilli is Vice President of Business Development Telecommunication Systems, Inc. Mr. Cadilli has an M.A. and a B.A. in Economics from Cambridge University and has been published in the Yale Journal on Regulation and Journal of Commerce.

This Article examines VoIP communications in the modern digital arena. More specifically, the Article suggests a new legal framework for courts to analyze VoIP claims brought under the Wiretap Act. Part I of this Article provides a comprehensive overview of VoIP privacy rights and legal treatment. Part II sets out a background primer for readers unfamiliar with Internet technology, including VoIP and clickstream data. Part III discusses relevant privacy case law, and Part IV describes how that case law has been applied to electronic communications. Part V provides a statutory analysis of the different privacy levels that are, and should be, afforded to different types of electronic communications. Part VI identifies the specific problem facing the legislature and courts regarding the treatment of VoIP. To solve this problem, Part VII proposes a modified framework advocating legislative action to re-write the Wiretap Act by creating an explicit clickstream data exception with a corresponding decrease in the mens rea element from intent[1] to recklessness for persons using clickstream data. By adopting this approach, the legislature would enable companies to legitimately tap clickstream data with or without an end-user's consent, though companies doing so would be required to design systems that monitor only clickstream data and do not tap protected oral telephone and electronic communications. In this way, Congress can protect VoIP privacy expectations while maintaining the vitality of the Internet economy.

I. OVERVIEW OF VOICE OVER INTERNET PROTOCOL PRIVACY RIGHTS

This section examines the judiciary's treatment of clickstream data when applying the Wiretap Act's consent exception. By broadly construing the consent exception in data mining[2] cases to include implied

1. 18 U.S.C. § 2511(1)(a) (2004).

2. The term data mining is defined as the process of identifying understandable correlations and patterns in data obtained from an organization's systems. *See* H. M. Chung and P. Gray, *Special Section: Data Mining*, 16 J. MGMT. INFO. SYS. 1 at 11-17 (1999). Data mining extends traditional data analysis and statistical approaches to incorporate analytical techniques drawn from a range of fields, including but not limited to numerical analysis, pattern matching, genetic algorithms, and neural networks. *See* Balaji Rajagopalan & Ravindra Krovi, *Benchmarking Data Mining Algorithms*, J. DATABASE MGMT., Jan.-Mar. 2002, at 13, 25-36. Data mining focuses on either modeling relationships between different types of data or identifying unusual patterns of behavior, such as spending habits for fraud protection. *Id.* While the term data mining is used rather broadly, it focuses on the activities involved in extracting information from data and primarily helps organizations discover important information about data stored on their systems. Halbert White, *A Reality Check For Data Snooping*, 68 ECONOMETRICA 5, 1097-1126 (Sept. 2000). Internet companies utilize data mining to construct and identify consumer trends, patterns, and profiles. This data is collected in a variety of ways using multiple channels. Data collected from the Internet, however, primarily utilizes clickstream data. *See* discussion *infra* Part II.B. This paper examines one type of data mining: that of clickstream data. Other data mining programs, such as spyware and adware, collect different types of

consent where no explicit contract provision limits the scope of interceptions, courts have essentially exempted clickstream data from protection under the Wiretap Act.[3] An examination of congressional intent supports the clickstream data exception, but neither Congress nor the judiciary has affirmatively recognized this.[4] The judiciary has officially acknowledged the difference in treatment between clickstream data and other electronic communications,[5] but unless courts clarify this ambiguity, there is a risk that (1) the clickstream data exception could be eliminated, making a large amount of Internet communications illegal,[6] or (2) the courts could read the exception too broadly, exempting electronic and VoIP telephone communications from protection under the Wiretap Act.[7]

To rectify this judicially created privacy dichotomy, Congress should amend the Wiretap Act to codify the judicially recognized clickstream data exception[8] and to lower the mens rea element from intent[9] to recklessness for companies that knowingly risk making unauthorized third party interceptions of VoIP[10] communications while engaging in judicially protected data mining of clickstream data. The first of these changes would legalize the interception of clickstream data under the Wiretap Act with the implied consent of the computer user or the Web host. At the same time, interceptors of clickstream data would be forced to operate with due care to prevent unauthorized interceptions of other telephone and electronic communications transmitted through the same medium.[11]

Justice Brandeis was correct in 1928 when he anticipated that technological advancement would enable the Government to employ

---

information using different technical tools and sources, which differ notably from those of cookie-driven technology.

3. While most people would expect all the aforementioned communications to be protected, the courts have created a judicial exception by exempting clickstream data from the Wiretap Act. For example, a DSL line permits voice communications to travel on it as an analog signal, while e-mail and VoIP are packetized at the source. When the composite signal gets to the central office, the signal is disassembled, packetized if it was not voice or data, and transmitted to wherever it needs to go. This process applies as well to sending a fax or using an Internet dial-up connection on a telephone line, both of which are digital communications over a voice band. The courts have permitted the tapping of clickstream data but have created various privacy levels for the types of communications discussed above.

4. *See* discussion *infra* Part III.

5. *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 19-22 (1st Cir. 2003); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 503-504 (S.D.N.Y. 2001).

6. *See* discussion *infra* Part V.A.

7. *See* discussion *infra* Part II.B.

8. *See* discussion *infra* Part III.C.

9. 18 U.S.C. § 2511(1)(a) (2004).

10. *See* discussion *infra* Part II.

11. *See* discussion *infra* Part VII.

surveillance tools extending far beyond wiretapping.[12] In his dissenting opinion in *Olmstead v. United States*, Justice Brandeis asserted that Fourth Amendment protections must be interpreted broadly to safeguard against new abuses that were not previously envisioned.[13] Thus, Justice Brandeis sought to protect the individual's "right to be let alone" without regard to the different technologies that might be employed by the government to compromise that right.[14] Justice Brandeis's focus on underlying privacy interests presents a more compelling perspective than the premise of Title III of the Omnibus Crime Control and Safe Streets Act of 1968[15] (hereinafter "Wiretap Act") as currently applied by the courts.[16]

The courts forbid third parties to tap or monitor oral telephone communications,[17] but they routinely permit data packets[18] to be tracked, stored, and sold by third parties with the implied[19] or explicit[20] consent of either party engaged in the transmission. In the digital age, however, the law-made distinction between voice and data has become muddled. With the convergence of oral and data communications into a single transmission medium, the courts are unable to distinguish between oral telephone and electronic communications.[21] The use of VoIP and similar technologies has made this legal distinction impossible to uphold

---

12. *See* Olmstead v. United States, 277 U.S. 438, 466, 472-74, 478 (1928) (Brandeis, J., dissenting) (majority holding that a wiretap not effected through a trespass onto private property did not violate the Fourth Amendment); Edward J. Bloustein, *Privacy, Tort Law, and the Constitution: Is Warren and Brandeis' Tort Petty and Unconstitutional as Well?*, 46 TEX. L. REV. 611 (1968).

13. *Olmstead*, 277 U.S. at 478.

14. *Id.*; *see also* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890) (finding privacy right in penumbra of Supreme Court Fourth Amendment interpretations—were privacy as such specifically envisioned, it would not need such circuitous explanation).

15. Pub. L. No. 90-351, § 802, 82 Stat. 212 (1968).

16. Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000)).

17. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (holding a warrantless government recording of defendant's conversation in an enclosed public phone booth unconstitutional).

18. *See* Vonage Holdings Corp. v. Minnesota Pub. Utils. Comm'n, 290 F. Supp. 2d 993, 994 (D. Minn. 2003) ("Congress also differentiated between 'telecommunications services,' which may be regulated, and 'information services,' which like the Internet, may not.").

19. *See* Register.Com, Inc. v. Verio, Inc., 356 F.3d 393, 409 (2nd Cir. 2004); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874, (9th Cir. 2002); Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 474 (S.D.N.Y. 2004); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 503-504 (S.D.N.Y. 2001); Nissan Motor Co., Ltd. v. Nissan Computer Corp., 204 F.R.D. 460, 465 (C.D. Cal. 2001); U.S. v. Pierre-Louis, No. 00-434-CR-GOLD/SIMON, 2002 WL 1268396, at *3 (S.D. Fla. Mar. 22, 2002); *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *2 (N.D. Cal. Oct 9, 2001).

20. *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 19-22 (1st Cir. 2003); Dyer v. Northwest Airlines Corporations, 334 F. Supp. 2d 1196, 1198 (D. N.D. Sep 08, 2004); Freedman v. America Online, Inc., 325 F. Supp. 2d 638, 643 (E.D. Va. Jul 12, 2004); Directv, Inc. v. Spokish, No. 6:03-CV-680-ORL-22DAB, 2004 WL 741369, at *3, 17 (M.D. Fla. Feb 19, 2004).

21. *See Vonage*, 290 F. Supp. 2d at 1000-03.

because oral telephone and electronic data communications now travel over the same wires simultaneously, encapsulated in digital data packets.[22]

VoIP[23] is a technology for transmitting ordinary telephone calls over the Internet.[24] In other words, VoIP can send oral, fax and other information over the Internet, rather than through the Public Switched Telephone Network (PSTN) or regular telephone network.[25] For example, if you are connected to the Internet, you can simultaneously exchange data, audio or video with anyone while using VoIP, which is impossible with a regular telephone line.[26] This convergence of separate mediums shifts the legal landscape of digital communications and requires further examination. This examination must proceed in light of the disparity in judicial treatment between oral telephone and electronic data communications, with oral telephone communications generally receiving a higher level of privacy protection.[27]

VoIP is no longer a fledgling technology;[28] it is rapidly becoming a mainstream communication product.[29] Both corporate and individual consumers are using VoIP to reduce their phone bills by capitalizing on their existing connections to Internet broadband infrastructure.[30] For example, Nissan North America, based in California, is implementing VoIP globally,[31] though dollar cost savings are not the only factor driving this decision.[32] Nissan and a multitude of other companies are utilizing VoIP to facilitate global communication between their offices

---

22. *See* FROST & SULLIVAN, VOIP EQUIPMENT 2003 WORLD MARKET UPDATE (2003) (stating that companies selling IP telephony equipment generated more than $1 billion in revenues in 2000 and expect those revenues to exceed $14 billion by 2006).

23. Use of Internet Protocol data connections that have traditionally been carried over the public switched telephone network to exchange voice and fax data.

24. *See Vonage*, 290 F. Supp. 2d at 1002.

25. VOIP EQUIPMENT 2003 WORLD MARKET UPDATE, *supra* note 22.

26. *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1999).

27. *Compare* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that electronically listening to telephone conversations constitutes a "search and seizure" within the meaning of the Fourth Amendment), *with* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis.").

28. *See* Peter Grant, *Ready for Prime Time: A New Internet-Based Phone Technology Has an Un-Catchy Acronym: VoIP*, WALL ST. J., Jan. 12, 2004, at R7. Growth projections for VoIP vary widely, but the Wall Street Journal reported in early 2004: "By the end of this year, about 20% of the new phones being shipped to U.S. businesses will use VoIP technology, according to Yankee Group, a technology consulting firm based in Boston. By 2007 that figure should exceed 50%, and eventually almost all of the new phones shipped will use VoIP. Yankee Group predicts." *Id.*

29. VOIP EQUIPMENT 2003 WORLD MARKET UPDATE, *supra* note 22.

30. *See* Stan Gibson, *VoIP Passes Nissan Road Test*, EWEEK, Jan. 24, 2005, at 33.

31. *Id.* at 32.

32. *Id.*

because VoIP offers improved functionality over traditional telephone systems.[33] While large corporations that purchase VoIP systems to improve functionality[34] and decrease costs[35] receive the primary benefit from these services, individual consumers also benefit from Internet-based VoIP services that offer less expensive long distance and local phone service via their own home broadband Internet connections.[36]

VoIP cost savings arise[37] from the ability to transmit oral and data communications simultaneously over the same medium,[38] thereby eliminating the need for multiple phone and data lines in a home[39] or business. VoIP technology threatens to break the oral communication monopolies held by the regional Bell companies[40] because it eliminates the need for consumers to pay non-competitive fees for the use of a telephone line to carry oral telephone conversations.[41] VoIP transmits oral communications via Internet Protocol (IP)[42] instead of the PSTN. Unlike the PSTN,[43] VoIP is unlikely to face legal issues of monopolization and significant government regulation because there are multiple technologies such as satellite, wireless, cable, DSL, and IP over

33. According to PC Magazine, VoIP can save small businesses significant amounts of money, averaging about 30 percent on phone costs and larger companies can save on calls to and from teleworkers or partners—even if they are located in another country—when those calls are placed over the Internet. C. Wolter, *VoIP: The Right Call*, PC MAGAZINE, Jun. 22, 2004.

34. CISCO SYSTEMS, INC., THE STRATEGIC AND FINANCIAL JUSTIFICATIONS FOR IP COMMUNICATIONS, (2001), *at* http://www.cisco.com/warp/public/cc/so/neso/vvda/iptl/cnvrg_wp.htm (last visited Jul. 21, 2005).

35. *See* Kevin Tolly, *VoIP: Neither Panacea Nor Pariah*, NETWORKWORLD, Feb. 18, 2002, at 24, *available at* http://www.nwfusion.com/columnists/2002/0218tolly.html (last visited Jul. 21, 2005).

36. *See* Press Release, Infonet, Infonet Introduces Software Tool to Demonstrate ROI for Converged Networks (Nov. 13, 2001), *available at* http://www.infonet.com/about/newsroom/press_release.asp?month=1113&year=2001 (last visited Jul. 21, 2005).

37. Paul Taylor & Peter Thal Larsen, *Time Warner Cable Plans Big Push Into Internet-Based Phone Services*, FIN. TIMES, Dec. 9, 2003, at A1.

38. *See* Internet Engineering Steering Group, Internet Architecture Board, *IETF Policy on Wiretapping*, RFC 2804, INTERNET ENG'G TASK FORCE (May 2000) (discussing how VoIP uses the Internet's open network architecture and stating that VoIP and Internet communications transmit on a single interconnected digital network).

39. By the end of 2006, more than half of all 110 million-odd households in the U.S. will likely have the option of getting phone service from their cable companies. By 2008, cable companies will be selling phone service to 17.5 million subscribers, compared with 2.8 million at the end of 2003, according to an estimate by research firm Yankee Group. Peter Grant, *Here Comes Cable . . .*, WALL ST. J. Sept. 13, 2004 at R4.

40. *See* Yochai Benkler, *Communications Infrastructure Regulation and the Distribution of Control Over Content*, 22 TELECOMMUNICATION POLICY 3, at 183-97 (1998).

41. *See* Grant, *supra* note 39.

42. *See In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 504 (S.D.N.Y. 2001).

43. Benkler, *supra* note 40, at 190.

power line technology competing to be the communication service provider.[44]

While the market's invisible hand has already fostered technical innovations making some VoIP services superior to those offered by the traditional PSTN,[45] the legislature and the courts have yet to resolve two primary legal issues that are likely to hinder the United States' adoption of VoIP as the new oral communication standard. First, VoIP will have to contend with the extension of Congressional legislation from the PSTN to VoIP carriers[46] to tax the transmission of data[47] and to regulate communication networks and line monopolies.[48] Second, the degree of

---

44. Grant, *supra* note 39.

45. *See, e.g.*, David Sheff, *Betting on Bandwidth*, WIRED, Feb. 2001, at 144-56.

46. The Telecommunications Act of 1996 defines two important categories: "Telecommunications Services" which are subject to mandatory Title II regulation, 47 U.S.C. § 153(46) (1996), and "Information Services" which are exempt from such regulation. 47 U.S.C. § 153(20) (1996). The regulatory classification of a service is of extreme importance to incumbents and new entrants. For example, the Supreme Court recently upheld the F.C.C.'s initial classification of cable-modem service as an information service, *In re* Inquiry Concerning High-Speed Access to the Internet Over Cable and Other Facilities, 17 F.C.C.R. 4798, 4821–22, (2002), while classifying DSL as a telecommunications service. *In re* Deployment of Wireline Services Offering Advanced Telecommunications Capability, 13 F.C.C.R. 24011, 24030–31 (1998). *See* National Cable & Telecommunications Association v. Brand X Internet Services, 125 S. Ct. 2688 (2005). The Court reached this decision by agreeing that the F.C.C's cable-modem was reasonable, *id.* at 2710, after applying the second step in the Chevron test. *Id.* at 2708-09. To assess reasonableness, the Court examined the attributes of an information service under 47 U.S.C. § 153(20) (2004) (generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making information available via telecommunications—in this case, browsing the Web to transfer files via FTP and to access e-mail) vis-à-vis those of a telecommunication service under 47 U.S.C. § 153(43) (2004) ("the transmission, between or among points specified by the user, of information of the user's choosing, without change in the form or content of the information as sent and received."). *National Cable & Telecommunications Association*, 125 S. Ct. 2688 at 2710.

Strikingly, VoIP contains attributes of both an information service and a telecommunication service. The VoIP "stack" certainly stores, transforms, and converts information via telecommunications, so it is an information service. *See* Phillip Carden, *Building Voice Over IP*, NETWORK COMPUTING, May 8, 2000. The purpose of all this storing, transforming, and converting, however, is really to transparently transmit voice information to and from a user and another point of his choosing, all the while minimizing observable differences in the form or content of the information. VoIP providers are graded on how closely they emulate POTS, with the test being "will your Mom notice?" *See, e.g.*, Sam Schechner, *Smooth Operators: Which Internet phone service is best?*, SLATE MAGAZINE, June 29, 2005, *available at* http://slate.com/id/2121742 (last visited July 13, 2005).

Whether VoIP services will be classified as a telecommunications service will eventually depend on whether the F.C.C. considers VoIP a transparent transmission of information. *See National Cable & Telecommunications Association*, 125 S. Ct at 2696-97. Note that the F.C.C. did not consider cable-modem service to be "transparent" because cable-modem service includes DNS resolution and caching. *Id.* at 2698.

47. Congress' decisions to tax and regulate VoIP technology are beyond the scope of this paper.

48. *See generally* Declan McCullagh, *Congress Proposes Tax on All Net, Data Connections*, Jan. 28, 2005, *available at* http://news.com.com/Congress+proposes+tax+on+all+Net,+data+connections/2100-1028_3-5555385.html (last visited July 20, 2005).

privacy, if any, that the law will afford to VoIP oral communications must be defined.[49] The taxation issue lies entirely in the hands of a legislature that is actively attempting to extend PSTN taxation to IP communications networks.[50] The privacy issue, however, will likely be determined, at least initially, by courts integrating VoIP communications into the oral communications[51] legal structure.

Under the current legal framework, unauthorized third-party access to oral telephone communications made from the privacy of one's home constitutes an invasion of any non-consenting person's privacy.[52] Courts will probably extend these privacy rights to VoIP communications[53] because the Supreme Court has recognized oral communication privacy rights within the context of the home.[54] Because it is physically transmitted in the form of digital data packets over the Internet,[55] VoIP oral communications, though essentially indistinguishable from Internet

---

49. *See* Maryland v. Garrison, 480 U.S. 79, 90 (1987) (Blackmun, J., dissenting); Segura v. United States, 468 U.S. 796, 810 (1984) ("The sanctity of the home is not to be disputed"); Welsh v. Wisconsin, 466 U.S. 740, 750, 754 (1984) (noting sanctity of the home); Katz v. United States, 389 U.S. 347, 353 (1967) (use of electronic eavesdropping equipment to overhear conversation inside telephone booth intrudes on legitimate expectation of privacy); *see also* Ferguson v. City of Charleston, 532 U.S. 67, 84 (2001) (describing body and home as "areas afforded the most stringent Fourth Amendment protection"); City of Indianapolis v. Edmond, 531 U.S. 32, 54 (2000) (Rehnquist, C.J., dissenting) (also describing body and home as "areas afforded the most stringent Fourth Amendment protection").

50. *See generally* McCullagh, *supra* note 48.

51. 18 U.S.C. § 2510(2) (2004).

52. *See* cases cited *supra* note 49; United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976) (holding a violation of the Act required that interception occur contemporaneously with transmission). *See also* 18 U.S.C. § 2511(1) (2004), stating: "Except as otherwise specifically provided in this chapter any person who – (a) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication . . . . "

53. *See* cases cited *supra* note 49; United States v. Cassity, 720 F.2d 451, 457 (6th Cir. 1983) (reasonable expectation of privacy in parents' home when defendant had lived there for 20 to 25 years, kept his clothes there, and came and went freely; second defendant had reasonable expectation of privacy in home when he frequently stayed as guest and came and went freely), *vacated and remanded on other grounds*, 104 S. Ct. 3581 (1984). Upwards of 90% of Internet users are concerned about threats to their personal privacy when they use the Internet. *See* Alan F. Westin, *Personalized Marketing and Privacy on the Net: What Consumers Want*, PRIVACY & AM. BUS., NOV. 1999, at 11.

54. *See* cases cited *supra* note 49; United States v. Karo, 710 F.2d 1433, 1441 (10th Cir.1983) (holding that a visitor had legitimate expectation of privacy in the home after spending a couple of days and nights with unfettered access to the house), *rev'd on other grounds*, 468 U.S. 705 (1984). *See also In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 518-20 (S.D.N.Y. 2001) (holding that the Wiretap Act includes a defense of consent by either party to the communication and the courts have found no unlawful interception of communications had occurred in either of these cases because the courts found that the consent of the Web portal entity was sufficient in itself to authorize a third-party to usurp their information).

55. *See* Vonage Holdings Corp. v. Minnesota Pub. Utils. Comm'n, 290 F. Supp. 2d 993, 1000-03 (D. Minn. 2003).

data communications, are legally protected by a constitutional right of privacy preventing third parties from tracking, tapping, storing or selling the communications.[56] VoIP opens a paradigm of oral privacy, which will place a considerable strain on the existing judicial canons protecting oral and data communications. This legal privacy dichotomy poses a substantial risk that parties legitimately monitoring Internet data streams will unlawfully monitor constitutionally protected private VoIP communications.[57] It remains to be seen whether this strain will be severe enough to force courts to extend the same Constitutional privacy right to data communications that it is currently extending to oral communications.[58]

II. TECHNICAL OVERVIEW

This section presents a broad overview of the technology involved in both Internet voice and data transactions. It discusses how VoIP transmits voice communications over the Internet, and provides an in-depth analysis of the inner workings of clickstream data and how it interacts with cookie technology.

A. Phone Conversations Using VoIP

VoIP allows oral communications to be transferred from circuit-switched networks to or over Internet Protocol networks, and vice versa.[59] VoIP transforms standard oral telephone signals into compressed data packets that are sent over the Internet.[60] At this point, the audio signal is captured either by way of a microphone or received from line input.[61] This analog representation is then converted to a digital representation at the audio input device. The resulting digital samples are copied into a memory buffer in blocks of frame length. Here, a silence

56. *See* Bartnicki v. Voppe, 532 U.S. 514 (2001) (noting that the application of the Wiretap Acts' prohibitions against intentional disclosure of illegally intercepted cell phone conversations to media defendants violated First Amendment).

57. *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 12 (1st Cir. 2003) (holding that a third-party data mining company had explicit consent to monitor non-personally identifiable information, but did not have explicit consent to monitor personally identifiable information, such as social security number, last name, phone, and date of birth).

58. *See* Katz v. United States, 389 U.S. 347, 350 (1967).

59. For one overview of the emerging market for VoIP, *see* Grant, *supra* note 28, at R7.

60. *See* UYLESS BLACK, VOICE OVER IP (1995).

61. *See* International Telecommunication Union Telecom Standards, ITU-T Recommendation H.225.0 (1998), *Call Signaling Protocols and Media Stream Packetization for Packet Based Multimedia Communication Systems*, *available at* http://www.itu.int/home/ (last visited July 22, 2005).

detector decides whether the block is silence or a portion of speech.[62] Prior to transmission over the Internet, the block itself is written to a socket. Once this is completed, the communication is transmitted to another VoIP terminal. This terminal examines the header information and the block of audio is decoded applying the same codec and the samples written into a buffer.[63] Next, the block of samples is copied from the buffer to the audio output device.[64] The audio output device converts the samples from digital to analog and outputs the signal.[65] VoIP can be used with either a telephone or a PC as the user terminal.[66] This results in different modes of VoIP operation: PC to PC, PC to telephone, telephone to PC, and telephone to telephone (via the Internet). All VoIP protocols are application layer protocols.[67]

Wiretapping dangers increase considerably in the VoIP world. To eavesdrop over the switched telephone network, there must be physical access to the telephone line and access to some type of hardware device that may or may not be very sophisticated.[68] To eavesdrop on VoIP no

---

62. Based on the detector's evaluation as to whether or not the block is part of talk, it is encoded with the selected codec, then header information is added to block. *Id.*

63. *See generally* Philip Carden, *Building Voice over IP*, NETWORK COMPUTING, May 8, 2000, *available at* http://www.networkcomputing.com/netdesign/1109voipfull.html.

64. *See generally* Darrin Woods, *Connecting to the Voice World*, NETWORK COMPUTING, April 17, 2000.

65. *See* Jon-Olov Vatn, IP Telephony: Mobility and Security 20 (2005) (Doctoral Thesis in Teleinformatics, Stockholm, Sweden).

66. *See* Rachael King, *Home of the Future*, TELEPHONY, June 6, 2005, at 10.

67. Carden, *supra* note 63. An application layer protocol is a layer used to transmit Internet communications existing within the TCP/IP framework. The application layer is defined within the TCP/IP protocols, which are an industry standard group of protocols through which computers find, communicate, and access one another over a transmission medium. *Id.* The protocol group is implemented in the form of a software package known as a TCP/IP stack, which splits the transmission into a number of discrete tasks. *Id.* Each layer corresponds to a different form of communication. *Id.* The TCP/IP architecture has four layers: application, transport, Internet, and the physical layer. *Id.* The transmission of voice communications over the Internet initiates with data being sent from the application layer down the stack to physical layer, where it is then transmitted to the receiver and goes up the stack in the reverse order, ending at the application layer. *Id.*

68. VoIP is a solid technology, however: it requires government regulation to ensure a certain level of product reliability and safety for the consumer. *See* Yumi Nishiyama, Collective Action in a Complex Environment: The Case Study of Network Security in Telecom/IT Convergence (2003) (unpublished Master's thesis) (on file with author). Up until today, the users have seen security issues in the data and voice worlds as completely separate. With the advent of VoIP users are now exposed to the risks of sending data over the Internet while simultaneously having the expectation that telephone conversations are between the parties involved. *Id.*

VoIP is vulnerable because convergent technologies lead to weakness from multiple points. *See id.*

In addition, VoIP must address the security holes in cell phones that arise from the transport mechanisms used when mobile phones are used. *Id.* Adjoining these problems is the reality that cell tracker tools have evolved and people can eavesdrop with much greater ease on cellular transmission. *Id.* Also, hackers can intercept data with greater ease than before when the data travels in soft zones (unprotected) between legitimate users and cell towers. *See* M. Miettinen, *IT-Security*

physical tapping is necessary, and the equipment or software needed, though much more sophisticated, is still within the reach of a sixteen year old hacker. Data-sniffing tools[69] are readily available, and will soon be enhanced to include the new VoIP protocols.[70] Corporations are at especially great risk. In an office environment, VoIP traffic travels over a data network that is used by all of the regular users of the corporate LAN.[71] Therefore, any or all of the conversations traversing a network could theoretically be compromised by anyone with a regular connection on the network.[72] VoIP packets could be identified and stored for re-assembly to be played back at a later time.[73] The idea that only Internet traffic is at risk is simply wrong.[74] Privacy for oral communications could be vastly enhanced by the use of encryption,[75] though most corporate networks do not encrypt VoIP calls.[76]

One of the attractive features provided by VoIP is the ability to locate intelligence at various points in the network. Gatekeeper or call-manager devices, which authenticate users and establish connections,[77]

---

in the Automobile Domain, LEHRSTUHL FÜR KOMMUNIKATIONSSICHERHEIT, RUHR UNIVERSITÄT BOCHUM (Germany), *available at* http://www.cs.helsinki.fi/u/mjmietti/seminaariS03/automobilesecurity.pdf (last visited July 20, 2005). Thus, transmitting information in digital form raises new vulnerabilities and digital devices can be used either for fiscal or and privacy violations. Also, as the VoIP systems run on vulnerable software, they must contend with all of these possible holes. *Id.*

69. Data-sniffing tools are used primarily to steal or transmit end-user data from end-users' machines with or without their knowledge. P. J. Bruening and M. Stephen, *Spyware: Technologies, Issues, and Policy Proposals*, 7 J. INTERNET L. 9, 3-8 (2004). Advertisers can use these tools to identify what sites end-users have visited and deliver targeted ads to the end-user's computer. *Id.* For example, if a user visits a Florida cruise site followed by a later visit to a golfing site, advertising using data-sniffing tools will serve advertisements to the end-user's computer about golf course vacations in Florida. *Id.* Data-sniffing tools encompass cookie technology, spyware, and adware.

70. *See* J. Daniels, *Scumware.biz Educates About Dangers of Adware/Scumware*, 5 COMPUTER SECURITY UPDATE 2 (2004).

71. Local Area Network: a network of interconnected computers such as an office work-group.

72. *See* Dale J. Long, *The Lazy Person's Guide to Voice Telephony—Part II*, CHIPS, Spring 2004, at 43.

73. *See* Amie J. Singer, *Debate Over Voice-Over Internet Protocol Benefits: Cost-Effectiveness, Security Concerns at Heart of Uncertainty*, 22 SAN DIEGO BUS. J. 19 (Dec. 2001).

74. *See* Ian Shepherd, *The Maturity of Internet Telephony Technology Opens Up Network Safety Concerns Voice Over IP: Finding a Balance Between Flexible Access and Risk of External Attack*, COMPUTER WEEKLY, Apr. 19, 2005, at 34.

75. Encryption and decryption are CPU intensive and take time. If the overall latency of a VoIP call is greater than approximately 250m/sec the quality of the call will be noticeably affected. *See* Philip Bednarz, *Security Considerations at Forefront of VoIP Design*, ELECTRONIC ENGINEERING TIMES, Sept. 23, 2002, at 63.

76. *See* Nishiyama, *supra* note 68.

77. A gatekeeper is an optional component of an H.323 enabled network that provides central management and control services. *See generally* K. Percy and M. Hommer, *Tips From the Trenches on VoIP*, NETWORK WORLD 48 (Jan. 27, 2003). Gatekeepers usually deliver the following in relation to VoIP services: (1) address translation; (2) bandwidth management; and (3) routing functionality. *Id.* H.323 is a technical standard that enables VoIP companies to create interoperable Internet

can physically reside on any server[78] on the network. This is really a two-edged sword. Logging information about user calls may be useful for billing or tracking purposes, but these logs can also become targets for hackers. If this type of information is compromised, it can create serious concerns for organizations or individuals.[79] Unfortunately, the home user is usually unaware of any of these vulnerabilities when that user purchases or uses VoIP technology.[80]

B. Clickstream Data and Internet Commerce

This section examines both the technical capabilities and the uses of clickstream data, examining in detail the role played by cookie technology. Cookies are information packets transmitted from a server[81] to an end-user's Web browser, such as Microsoft Internet Explorer or Mozilla Firefox, which then retransmits information back to the server each time the browser accesses its Web page.[82] Cookies usually store information used for authentication, identification or registration of an end-user to a website.[83] This information enables the end-user's Web browser to maintain a continuous relationship between the end-user's computer and the server of a specific site.[84]

---

telephony solutions. Michele Rosen, *The Maturing of the Internet Telephony Market*, ENT, Mar. 18, 1998, at 48.

78. A server is a computer system or a set of processes on a computer system providing services to clients across a network.

79. *See* Edwin Mier, Randall Birdsall & Rodney Thayer, *VoIP Security Wares: Breaking Through IP Telephony*, NETWORK WORLD, May 24, 2004, at 83, 84–88.

80. *See generally* Mike Lee, *Beware! Bugs Can Attack Net Phones: They May be Cheap but They are Also Vulnerable to Hackers, Say Experts, Who Advise Installing Anti-virus Patches*, THE STRAITS TIMES (Singapore), August 22, 2004; Jay Fitzgerald, *Team to Tie Net Phone Hackers: Industry Aims to Stop Scams Before They Start*, BOSTON HERALD, April 26, 2005, at 31.

81. *See supra* note 78 and accompanying text.

82. *See* Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA. L. REV. 551, 554 (1999) ("The data trail, known as transactional data, left behind as individuals use the Internet is a rich source of information about their habits of association, speech, and commerce. Transactional data, click stream [sic] data, or 'mouse droppings,' as it is alternatively called, can include the Internet protocol address ('IP address') of the individual's computer, the browser in use, the computer type, and what the individual did on previous visits to the Web site, or perhaps even other Web sites.").

83. Once a user has accessed a Web site that uses cookie technology or an affiliated site, the embedded cookie on the hard drive begins collecting data about the user's Web activities. In four reported cases, Web sites used cookie technology to mine personal information from the users' machines. *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 12 (1st Cir. 2003); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1155 (W.D. Wash. 2001).

84. Many privacy advocates believe that this automatic transmission of information should not occur absent a requirement of active consent, or "opting-in," by the end-user. *See* Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 910 (2002); *see generally*, Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for*

Cookies[85] were first used in the mid-1990s when Web based businesses began using them to deliver user-specific solutions for each machine that accessed their Web pages.[86] Cookies allowed websites to track end-user activities by placing electronic tracks or markers on an end-user's machine.[87] Collectively, these cookie-driven markers create a trail of information commonly referred to as "clickstream data."[88]

Clickstream data is used because centralized Web server technologies cannot store and sort the vast amounts of data required to authenticate a user or to deliver the respective web solutions to each individual user of a site.[89] Thus, Web sites off-load certain information to the end-user's device where it is stored in cookies.[90] These cookies provide the Web site with a mechanism through which to collect and store data on the storage device of the visitor's machine, thereby enabling a Web site to record, track, monitor, and generate customized dynamic pages reflecting the stored data.[91]

Initially, clickstream data was used to gather basic information from a Web user,[92] such as the type of computer an individual used to

---

Information Privacy, 53 STAN. L. REV. 1393, 1458-60 (2001); Lawrence Jenab, Comment, *Will the Cookie Crumble?: An Analysis of Internet Privacy Regulatory Schemes Proposed in the 106th Congress*, 49 KAN. L. REV. 641, 667-68 (2001); Rachel K. Zimmerman, Note, *The Way the "Cookies" Crumble: Internet Privacy and Data Protection in the Twenty-First Century*, 4 N.Y.U. J. LEGIS. & PUB. POL'Y 439, 459-60 (2000); *but see* Kent Walker, *The Costs of Privacy*, 25 HARV. J.L. & PUB. POL'Y 87, 113-117 (2001).

85. For further discussion of cookie technology, *see In re DoubleClick*, 154 F. Supp. 2d at 502-03 ("Cookies are computer programs commonly used by Web sites to store useful information . . .").

86. A sampling of Web sites that use cookie technology is as follows: www.yahoo.com; www.google.com; www.wamu.com; www.schwab.com; www.ibm.com. Adjoining these web sites is a slew of intranet and Web applications that utilize cookies and clickstream data for authentication. Not only will business be impacted, but so will a large number of government enabled Web applications. Some government sites using this technology are mentioned at http://www.ombwatch.org/article/articleview/587/1/71?TopicID=1 (last visited March 30, 2005). *See also* U.S Census Bureau, *Retail E-commerce Sales for the Fourth Quarter 1999 Reach $5.3 Billion*, U. S. DEP'T OF COMMERCE NEWS, Mar. 2, 2000, *available at* http://www.census.gov/mrts/www/current.html (last visited March 30, 2005).

87. *See* Berman & Mulligan, *supra* note 82.

88. *See* Berman & Mulligan, *supra* note 82.

89. *See generally* MOELLER, R. A., DISTRIBUTED DATA WAREHOUSING USING WEB TECHNOLOGY (2001).

90. *See* MICHAEL J. A. BERRY & GORDON S. LINOFF, MASTERING DATA MINING: THE ART AND SCIENCE OF CUSTOMER RELATIONSHIP MANAGEMENT (Robert M. Elliott ed., 2000); Colin Shearer, *The CRISP-DM Model: The New Blueprint for Data Mining*, J. DATA WAREHOUSING, 13-22 (2000).

91. *See generally* JIAWEI HAN & MICHELINE KAMBER, DATA MINING: CONCEPTS AND TECHNIQUES (Jim Gray ed., 2000); B. Rajagopalan and R. Krovi, *Benchmarking Data Mining Algorithms*, J. DATABASE MGMT., Jan.-Mar. 2002, at 13, 25-36.

92. *See generally Survey: A Key Technology for Online Profitability*, FIN. TIMES (London), April 3, 2002, at 5; *see generally* Randolph E. Bucklin & Catarina Sismeiro, *A Model of Web Site Browsing Behavior Estimated on Clickstream Data*, J. MKTG. RES., August 2003, at 249.

access the Internet, the type of Internet browser utilized, and the identification of each site or page visited.[93] As technology evolved, however, so did clickstream data.[94] Today, when an individual discloses certain information during a visit to a website via their Personal Digital Assistant (PDA), cell phone, Blackberry, laptop computer, iPod, or desktop computer, it is possible that the website will be collecting clickstream data of a much more personal nature.[95]

The functionality of the data mining industry and most web portals would be severely limited, if not rendered useless, in the absence of clickstream data or cookies.[96] Although it is possible for authentication processes to be retooled so as to require users to log in or to affirmatively consent to monitoring by cookies or clickstream data tracking, it is highly unlikely that fully informed end-users would interact with sites that track, monitor, and perhaps sell their personally identifiable information.[97] Internet companies currently rely heavily on tracking clickstream data to deliver customized services and advertisements to Internet users.[98] For example, DoubleClick, an Internet advertising company, stockpiled over 100 million user profiles by 2002.[99] Since then, the technology and ability to profile users has greatly improved and Internet companies now rely on clickstream data more than ever before. Because Web-enabled applications that utilize clickstream data in either a direct or derivative form are so prolific—cell phones and PDAs are just

---

93. *See* Fusun Feride Gonul, *Stereotyping Bites the Dust: Marketers No Longer Focusing On Demographic Profiling*, PITTSBURGH POST-GAZETTE, February 26, 2002, at B3; Karen Dearne, *You are Being Monitored Online*, THE AUSTRALIAN, September 24, 2002, at 31.

94. Clickstream data is a trail of information that a user leaves behind while browsing on the Web. Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 BERKLEY TECH. L.J. 1085, 1104 (2002). *See generally* Herbert A. Edelstein, *Pan for Gold in the Clickstream*, INFORMATIONWEEK.COM, Mar. 12, 2001, at 77-91; IAN H. WITTEN & EIBE FRANK, DATA MINING: PRACTICAL MACHINE LEARNING TOOLS AND TECHNIQUES WITH JAVA IMPLEMENTATIONS (Diane D. Cerra et al. eds., 2000); Jane Kaufman Winn & James R. Wrathall, *Who Owns the Consumer? The Emerging Law of Commercial Transactions in Electronic Consumer Data*, 56 BUS. LAW. 213, 234-35 (2000). Webster's New Millennium Dictionary of English, Preview Edition (v 0.9.5), defines clickstream as "a series of mouse clicks made by a user of the Internet, esp. when logged and analyzed for marketing research; the virtual record of an Internet user's activity including every Web site and every Web page visited and how long the user was at each," *available at* http://dictionary.reference.com/search?q=clickstream (last visited Mar. 20, 2005).

95. This information could be passwords, e-mail addresses, credit card numbers, medication, stock trades, and other sensitive information that your machine stores. *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 15 (1st Cir. 2003).

96. The operations of many commercial and secure websites depend on cookies and clickstream data interception. For a sampling of those impacted, *see supra* note 86.

97. *See Special Report—Online Marketing: Traffic control*, PRECISION MARKETING, March 18, 2005, at 17.

98. *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 503-507 (S.D.N.Y. 2001); Berry & Linoff, *supra* note 90.

99. *See In re DoubleClick*, 154 F. Supp. 2d at 505.

the beginning—if the courts construe the Wiretap Act to protect clickstream data in the same way as it protects "electronic communications,"[100] the business world and government functions alike will be disrupted.[101] To demonstrate this expansive reliance on cookie technologies, simply view the cookies stored on your own computer.[102]

III. THE LEGAL TREATMENT OF VOICE, MAIL, AND INTERNET-BASED COMMUNICATIONS

When people step outside of their homes, their expectation of privacy diminishes because their actions are exposed to the public view.[103] When people write letters or place telephone calls from within the privacy of their own homes[104] they expect heightened privacy protection despite using semi-public means of communication.[105] While oral telephone conversations[106] and first class mail[107] are protected on an equal footing with actions that occur within a person's home,[108] human

100. 18 U.S.C. § 2510(12) (2004).

101. *But see* FEDERAL TRADE COMM'N., 106TH CONG., PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, at 7, 10-20, 29-33, 38 (F.T.C. Rep. 2000), (recommending that Congress enact legislation requiring websites to ask users' permission before collecting personal information), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf (last visited July 22, 2005).

102. An end-user can view all of the cookies stored on a local machine using Internet Explorer by following these steps: (1) open Internet Explorer; (2) select "Internet Options" under the "Tools" menu; (3) click on the "General" tab and click the "Settings" button; (4) click the view files button; (5) sort files by type by clicking on "Type"; (6) find documents of the type labeled "Text Document." To see the information stored by the cookie in its raw and likely unintelligible format, double-click on one of these text files containing "cookie" in its file name.

103. *See* United States v. Karo, 710 F.2d 1433, 1441 (10th Cir. 1983) (legitimate expectation of privacy in home which one owns and in home which ones shares with others), *rev'd on other grounds*, 468 U.S. 705 (1984); United States v. Issacs, 708 F.2d 1365, 1368 (9th Cir. 1983) (reasonable expectation of privacy in locked safe located in defendant's residence; defendant had standing to challenge search of safe although he denied ownership of drug transaction ledgers seized from safe during search), *cert. denied*, 464 U.S. 852 (1983).

104. *See generally* Jeremiah Courtney, *Electronic Eavesdropping, Wiretapping and Your Right to Privacy*, 26 FED. COMM. B.J. 1 (1973); JAMES G. CARR & PATRICIA L. BELLIA, THE LAW OF ELECTRONIC SURVEILLANCE (West 2001).

105. *See* United States v. Van Leeuwen, 397 U.S. 249, 251-52 (1970) (discussing the close relationship between free speech and the search of first-class mail); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) ("Letters and sealed packages . . . in the mail are as fully guarded from examination and inspection . . . as if they were retained by the parties forwarding them in their own domiciles.").

106. *See* 18 U.S.C. §§ 2510-20 (2004); Katz v. United States, 389 U.S. 347, 353 (1967) (holding that electronically listening to telephone conversations constitutes a "search and seizure" within the meaning of the Fourth Amendment).

107. *See* cases cited *supra* note 105.

108. *See Ex parte Jackson*, 96 U.S. at 732-34.

and machine-written cyberspace communications are not, and receive a lower level of protection under the law.[109]

A. Telephone Communications are Protected from Governmental Privacy Invasions

Telephone communications are protected from governmental privacy invasions in two principal ways.[110] First, parties to a voice conversation are entitled to a "reasonable expectation of privacy" under the Supreme Court opinion of *Katz v. United States*.[111] Second, the Federal Wiretap Act of 1968 prevents unauthorized third-party interceptions of telephone communications, unless the interceptor has a court order or the consent of either party involved in the conversation.[112] The *Katz* opinion explains the rationale behind the Supreme Court's oft-quoted statement that the Fourth Amendment "protects people, not places,"[113] and concludes that an individual's reasonable expectation of privacy must be protected from government searches.[114] The Federal Wiretap Act was Congress' response to the *Katz* opinion and was an attempt to prevent electronic surveillance of oral telephone communications without a court order.[115]

The Supreme Court's 1967 decision in *Katz* disposed of the long-standing idea that property rights governed a person's right to be free from unreasonable searches and seizures.[116] *Katz* stands for the proposition that an individual can control which of his actions and information is accessible by the public,[117] and what remains private and protected by the Fourth Amendment.[118] The Court found that, while people assume certain risks whenever they communicate, the risks

---

109. *See* Paul Frisman, *E-Mail: Dial 'E' for 'Evidence,'* NEW JERSEY LAW J., Dec. 25, 1995, at 12 (commenting that ECPA provides more protection for phone calls then for e-mail); *see also* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis.").

110. *See* Frierson v. Goetz, 227 F. Supp. 2d 889, 896-97 (M.D. Tenn. 2002) (describing a two-part test for determining qualified immunity).

111. 389 U.S. 347, 350 (1967).

112. 18 U.S.C. §§ 2510-2521 (2004).

113. *See Katz*, 389 U.S. at 351.

114. *Id.* at 353 (government's actions "violated the privacy upon which [petitioner] justifiably relied" and thus triggered Fourth Amendment protections).

115. *See* United States v. Andonian, 735 F. Supp. 1469, 1471 (C.D. Cal. 1990); S. REP. NO. 90-1097, at 66-72 (1968); 1968 U.S. CODE & ADMIN. NEWS 2110, 2153-2159.

116. *See Katz*, 389 U.S. at 351.

117. *See id.* ("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.").

118. *Id.* at 352.

change once electronic surveillance enters the scene, and individuals lose all sense of security and privacy, even when the door is closed.[119] The *Katz* doctrine of Fourth Amendment protections has a twofold requirement: first, a person must exhibit a subjective expectation of privacy, and second, that expectation must be one that society is prepared to recognize as reasonable.[120] Although courts have read *Katz* quite narrowly in recent years,[121] most people would agree that expecting privacy while at home, on the phone, or in a letter sent via first class mail is reasonable.[122]

Since the Fourth Amendment's privacy protections only insulate individuals from governmental privacy encroachments,[123] the Wiretap Act is the main cause of action protecting telephone communicants from non-governmental third-party interceptors.[124] Telephone communicants can obtain redress under the Wiretap Act for unauthorized third party interceptions of telephone communications unless the interceptor has a court order[125] or the consent of either party involved in the conversation.[126] Courts may award triumphant plaintiffs actual damages plus any profits made by the violator resulting from the violation,[127] or statutory damages of the greater of $100 per day for each day of violations or $10,000.[128] Punitive damages[129] can be awarded for wanton, reckless or malicious violations.[130] Finally, successful plaintiffs may be awarded reasonable attorney's fees.[131]

---

119. *Id.* at 351-53.

120. *See id.* at 361 (Harlan, J., concurring).

121. *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case For Caution*, 102 MICH. L. REV. 801, 852 (2004) (stating that "despite *Berger* and *Katz*, courts have proved surprisingly reluctant to find that the occasional holes in the Wiretap Act violate the Fourth Amendment"). Moreover, "wiretapping law may be constitutional in theory, but it is statutory in practice . . . When wiretapping occurs inside the United States, courts generally refuse to construe the Fourth Amendment as going beyond the scope of the Wiretap Act." *Id.* at 853.

122. Thus, a person who makes efforts to keep his words private is "entitled to assume that the words he utters . . . will not be broadcast to the world." *Katz*, 389 U.S. at 352.

123. *See* Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614 (1989) (stating that "although the Fourth Amendment does not apply to a search or seizure, even an arbitrary one, effected by a private party on his own initiative, the Amendment protects against such intrusions if the private party acted as an instrument or agent of the Government"); Schmerber v. California, 384 U.S. 757, 767 (1966) ("The overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State.").

124. 18 U.S.C. §§ 2510-2521 (2004).

125. 18 U.S.C. §§ 2511(2)(a)(ii)(A) (2004).

126. 18 U.S.C. §§ 2511(2)(d) (2004).

127. 18 U.S.C. § 2520(c)(2)(a) (2004).

128. 18 U.S.C. § 2520(c)(2)(b) (2004).

129. 18 U.S.C. § 2520(b)(2) (2004).

130. *See* Bess v. Bess, 929 F.2d 1332, 1335 (8th Cir. 1991) (citing Jacobson v. Rose, 592 F.2d 515, 520 (9th Cir.1978), *cert. denied*, 442 U.S. 930 (1979)).

131. 18 U.S.C. § 2520(b)(3) (2004).

B. The Legal Treatment of Non-Oral Internet Communications and E-Mail

While Title III of the 1968 Omnibus Crime Control and Safe Streets Act (hereinafter "Wiretap Act")[132] initially afforded extensive protection to wire communications, oral communications were protected only when there was a reasonable expectation of privacy.[133] Because the legislation covered both face-to-face oral communications and traditional point-to-point wired communications, courts were faced with myriad interpretive difficulties.[134] To correct the problems with Title III, Congress amended the Wiretap Act by passing the Electronic Communications Privacy Act of 1986 (ECPA).[135] Congress designed the ECPA to prohibit the intentional interception of oral, wire, and electronic communications.[136] Because Congress was concerned with advancements in electronic technology that would be capable of defeating any privacy expectations,[137] the ECPA enacted a strict set of standards for the interception of oral, wire, and electronic communications.[138] Congress further expanded the protection of wireless communication by passing the Communications Assistance for Law Enforcement Act of 1994 (CALEA), which extended Title III to the radio portions of cellular and cordless phones.[139] In the wake of September 11, 2001, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (Patriot Act).[140] The Patriot Act contained a number of important changes to Title III that expanded the government's ability to conduct surveillance.[141]

---

132. Pub. L. No. 90-351, tit. III, § 802, 82 Stat. 212 (1968).

133. *See* United States v. McKinnon, 985 F.2d 525, 527 (11th Cir. 1993) (stating that Congress drafted the definition of "oral communication" to reflect the Supreme Court's standards for determining when a reasonable expectation of privacy exists).

134. *See* Edwards v. Bardwell, 632 F. Supp. 584, 589 (M.D. La.), *aff'd,* 808 F.2d 54 (5th Cir. 1986) (treating radio telephone communications as oral communications and holding that because communications through cellular devices could easily be intercepted, the requisite reasonable expectation of privacy did not exist).

135. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510-2521, 2701-2710, 3117, 3121-3126 (1986)).

136. *See* S. REP. NO. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555-3557.

137. *Id.* at 3555.

138. 18 U.S.C. § 2518 (2004).

139. Pub. L. No. 103-414, 108 Stat. 4279 (1994) (amending 18 U.S.C. § 2510 (2004)).

140. Pub. L. No. 107-56, 115 Stat. 272 (2001).

141. The scope and impact of the Patriot Act is beyond the scope of this paper. *See* John P. Elwood, *Prosecuting the War on Terrorism: The Government's Position on Attorney-Client Monitoring, Detainees, and Military Tribunals*, 17 CRIM. JUST. 30, 51 (2002).

1. Non-Oral Internet Communications

Like "wire communications,"[142] Internet communications are protected from unauthorized third-party interceptions as "electronic communications" under the Wiretap Act.[143] Internet communications, however, do not receive the same level of protection as do oral communications under a Fourth Amendment privacy rights analysis.[144] Decisions addressing this topic have focused on an expectation of privacy in two categories: (1) information knowingly passed online to other Web users,[145] and (2) information voluntarily passed offline to ISPs when signing up for Internet service.[146] Both lines of authority conclude that, under *Katz,* Internet users lack legitimate expectations of privacy in data, either because the information is knowingly exposed to public view or because Internet users assume the risk that the intended recipient will share the information with others.[147]

Courts have employed the knowing exposure and the assumption of the risk rationales to deny expectations of privacy in electronic information voluntarily exposed online, such as Internet postings.[148] For instance, courts have found that Internet users lose their expectations of privacy in personal information that is voluntarily disclosed to an ISP.[149] In *United States v. Hambrick,*[150] a district court noted that the Internet, a "computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis" under *Katz.*[151] However, "[s]o

142. "Wire communications" are defined by the Wiretap Act as the following:

> 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.

18 U.S.C. § 2510(1) (2004).

143. 18 U.S.C. § 2511 (2004).

144. *See* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis.").

145. *See In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *1 (N.D. Cal. Oct. 9, 2001).

146. *See Hambrick*, 55 F. Supp. 2d at 508.

147. *See In re Toys R Us*, 2001 WL 34517252, at *1 (N.D. Cal. Oct. 9, 2001); *Hambrick*, 55 F. Supp. at 508.

148. *See Hambrick*, 55 F. Supp. 2d at 508.

149. *Id.*

150. *Id.* ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis. So long as the risk-analysis approach of *Katz* remains valid, however, this court is compelled to apply traditional legal principles to this new and continually evolving technology.").

151. *Id.*

long as the risk-analysis approach of *Katz* remains valid . . . court[s] [are] compelled to apply traditional legal principles to this new and continually evolving technology."[152] In applying the *Katz* risk-analysis approach to the defendant's motion to suppress ISP sign-up information obtained by law enforcement, the *Hambrick* court found that, absent a specific non-disclosure agreement, the defendant had no reasonable expectation of privacy because he knowingly revealed his personal information to the ISP and all of its employees.[153]

Under the current jurisprudence, courts are likely to conclude that Web users lack a legitimate expectation of privacy based upon two rationales. First, users lack a subjective expectation of privacy in their data packets, excluding those containing any VoIP communications.[154] Second, any actual expectation of privacy is objectively unreasonable since users assume the risk that their data will be disclosed to law enforcement.[155] While courts apply the *Katz* risk analysis approach to both oral telephone and Internet-based communications, the public nature of most Internet communications prevents courts from finding that Web users have reasonable expectations of privacy when communicating through these means.[156]

2. E-mail

As with other Internet communications, e-mail communications are protected from unauthorized third party interceptions while in transmission as "electronic communications" under the Wiretap Act. Unlike other Internet communications, e-mail is considered to retain a legitimate expectation of privacy while in transmission.[157] This expectation of privacy, however, evanesces once the e-mail is received and read by another person.[158] Courts analogize e-mail to postal mail, and hold that the sender assumes the risk that the recipient will disclose the contents of the e-mail to law enforcement.[159] Because e-mail is often

---

152. *Id.*

153. *Id.*

154. *See generally In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 16-21 (1st Cir. 2003).

155. *Id.*

156. It is, however, conceivable that a court could find a reasonable expectation of privacy for an instant messaging conversation between two users that does not occur in a public forum and where the users do not realize that the contents of their communications are stored on a central server.

157. *See* Fraser v. Nationwide Mut. Ins. Co., 135 F. Supp. 2d 623, 634-35 (E.D. Penn. 2001) (finding that e-mail in transit is protected under the Wiretap Act).

158. *See id.* at 114.

159. *See* Lois R. Witt, *Terminally Nosy: Are Employers Free to Access Our Electronic Mail?* 96 DICK. L. REV. 545, 548-53 (1992) (discussing the exemptions and unequal treatment of the

stored electronically on a server before being read by the recipient, e-mail communications are also protected by the Stored Communications Act, which protects communications that are electronically stored from being intercepted or altered.[160]

C. The Legal Treatment of Clickstream Data

Courts have treated clickstream data as an exception to the Wiretap Act by broadly inferring consent between Web businesses and third-party data mining companies that intercept users' personal information.[161] The data can then be monitored and recorded by prying eyes and mined for information that is used to profile a Web user or to recreate her online experience.[162]

Courts have primarily dealt with clickstream data in *Chance*,[163] *Pharmatrak*,[164] *Intuit*,[165] *Toys R Us*,[166] and *DoubleClick*,[167] where plaintiffs alleged violations of the Wiretap Act for the use of cookie technology to intercept clickstream data.[168] The outcome of each of these

---

ECPA); Thomas R. Greenberg, *E-Mail and Voice Mail: Employee Privacy and the Federal Wiretap Statute*, 44 AM. U. L. REV. 219, 239-41 (1994).

160. 18 U.S.C. § 2701 (2004).

161. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 511 (S.D.N.Y 2001) ("Although the users' requests for data come through clicks, not keystrokes, they nonetheless are voluntary and purposeful. Therefore, because plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated Web sites are all 'intended for' those Web sites, the Web sites' authorization is sufficient to except DoubleClick's access under § 2701(c)(2).").

162. *See* Tal Z. Zarsky, *Mine Your Own Business!: Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE SYMP. L. & TECH. 1, 4 (2002-2003); *see also* U.M. Fayyad et al, *From Data Mining to Knowledge Discovery: An Overview*, ADVANCES IN KNOWLEDGE DISCOVERY AND DATA MINING 6 (1996).

163. *See* Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1156-57 (W.D. Wash. 2001).

164. *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 16 (1st Cir. 2003). The ECPA provides for a private right of action versus one who "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a) (2004).

165. *See In re* Intuit Privacy Litig., 138 F. Supp. 2d 1278, 1278 (C.D. Cal. 2001).

166. *See In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *1 (N.D. Cal. Oct. 9, 2001).

167. *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 503-504 (S.D.N.Y. 2001).

168. Spyware, although somewhat difficult to define, is a generic class of software security threats with malicious intent that includes technologies such as keystroke logging, malware, homepage hijacking, and adware. *See* U.S. Dep't of Justice, *Special Report on 'Phishing,' Criminal Division* (2004) (unpublished article), *available at* http://www.usdoj.gov/criminal/fraud/Phishing.pdf. The hallmark of spyware is its installation on a user's computer without his or her knowledge, consent or permission while connected to the Internet. It can be transferred via spam emails or be contained in freeware, shareware or games downloaded from the Internet. *Id.* Unsuspecting users may even consent to the installation of spyware with the click of a mouse in agreement to an application or program's licensing terms and conditions. *See* Federal Trade Commission, *National and State Trends in Fraud and Identity Theft*, CONSUMER SENTINEL (Feb.1, 2005), at 1, *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2004.pdf. The dangers

cases relied entirely upon the Wiretap Act, and examinations of reasonable expectations of privacy under *Katz* were cursory at best.[169] Recently, however, the First Circuit Court of Appeals in *Pharmatrak*[170] has reduced the effects of this judicially created exception by stipulating that consent can only be inferred where there is actual notice and where one party actually consents to the interception.[171]

In dealing with clickstream data[172] and cookie-related technology, the Second and Ninth Circuit district courts in *DoubleClick*[173] and *Intuit*,[174] respectively, construed the Wiretap Act's consent exception broadly,[175] requiring only implied consent, whereas the First Circuit Court of Appeals in *Pharamatrak*[176] narrowly construed the exception requiring actual consent.[177] In these cases, the courts heard Wiretap Act claims brought by plaintiffs alleging unauthorized third party access to communications.[178] In all three cases, end-users conveyed digital information to second-party entities that then used the information to construct user profiles in a process commonly referred to as data mining.[179]

---

of spyware include its ability to: (1) track a user's online activities without the user's knowledge or consent; (2) steal a user's personal information from his or her computer; (3) track a user's each and every keystroke (including the entry of password and financial information); (4) hijack homepages and substitute unacceptable sites; (5) create an endless stream of pop-up ads; (6) change computer settings (such as changing a user's default homepage settings); (7) disable hardware and software computer settings; (8) drastically slow infected computers; (9) remain on a user's computer in spite of attempts to uninstall it; and (10) result in hard drive corruption. *Id.*

169. The Supreme Court has historically applied a two-part test to determine whether the Fourth Amendment protects an asserted privacy interest. *See* Katz v. United States, 389 U.S. 347, 351-53 (1967) (announcing a test to determine expectations of privacy). First, the individual must exhibit a subjective expectation of privacy. Second, the expectation must be "one that society is prepared to recognize as reasonable." *Id.* at 361; United States v. Thomas, 729 F.2d 120, 122-23 (2d Cir. 1984) (applying two-part test), *cert. denied*, 469 U.S. 846 (1984).

170. *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 19-22 (1st Cir. 2003).

171. *Id.* "Without actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception." (Quoting Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir.1998)). Moreover, "knowledge of the capability of monitoring alone cannot be considered implied consent." (Quoting Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983)).

172. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 505 n.14 (S.D.N.Y 2001).

173. *See id.* at 500-505 (discussing cookies and the collection of data, where the plaintiffs again did not prevail).

174. *See In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001).

175. *See id.* at 1278; *In re DoubleClick*, 154 F. Supp. 2d at 503-04.

176. *See In re* Pharmatrak, Inc. Privacy Litig., 292 F. Supp. 2d 263, 266-68 (D. Mass. 2003).

177. *See id.* at 19-22.

178. *See* Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1155-57 (W.D. Wash. 2001); *In re DoubleClick*, 154 F. Supp. 2d at 503-04; *In re Pharmatrak*, 329 F.3d at 12; *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *1 (N.D. Cal. Oct. 9, 2001); *In re Intuit*, 138 F. Supp. 2d at 1274 (C.D. Cal. 2001).

179. Definitions are problematic in the data mining field, as every writer uses the terms differently. The term "data mining" is used in two distinct ways: both to define the entire process

Both the *Intuit*[180] and *DoubleClick*[181] courts permitted Web businesses to intercept clickstream data utilizing cookie technology, thereby extracting personal information off users' machines.[182] The defendant Web businesses placed cookies on end-users' computers, which then transmitted personal information back to the website's owner or to a third-party data mining company.[183] The courts did not find that there had been a violation of the users' privacy rights in either case;[184] rather, both courts found that the Web businesses' unilateral consent was sufficient to authorize third-party usurpation of user's personal information using cookie technology.[185] Both courts found that the third-party data mining companies did not violate the Wiretap Act under 18 U.S.C. § 2511(2)(d) because they were given implied consent and because their actions were not conducted for tortious or illegal purposes.[186]

In contrast, the *Pharmatrak*[187] court challenged the sweeping implications of the implied consent argument established in *DoubleClick*[188] and *Intuit*[189] by requiring the consenting party to both know about and consent to interceptions before consent can be inferred.[190] The *Pharmatrak* court found in favor of the Internet users, holding that neither party to the communication consented to the web monitoring company's interception of personally identifiable information.[191] The court reasoned that "[w]ithout actual notice, consent can only be implied when the surrounding circumstances *convincingly*

---

and to describe the specific stage in which the algorithms are applied. *See generally* Joseph S. Fulda, Data Mining and Privacy, 11 ALB. L.J. SCI. & TECH. 105 (2000).

180. *See In re Intuit*, 138 F. Supp. 2d at 1278.

181. *See In re DoubleClick*, 154 F. Supp. 2d at 503-04.

182. *See id.* at 505 n.14; *In re Intuit*, 138 F. Supp. 2d at 1278.

183. *See In re DoubleClick*, 154 F. Supp. 2d at 503-04; *In re Intuit*, 138 F. Supp. 2d at 1278.

184. *See In re DoubleClick*, 154 F. Supp. 2d at 514-515; *In re Intuit*, 138 F. Supp. 2d 1278-79.

185. *See In re DoubleClick*, 154 F. Supp. 2d at 518-520; *In re Intuit*, 138 F. Supp. 2d at 1278.

186. *See In re DoubleClick*, 154 F. Supp. 2d at 518-520; *In re Intuit*, 138 F. Supp. 2d at 1278.

187. *See In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 19-22 (1st Cir. 2003).

188. *See In re DoubleClick*, 154 F. Supp. 2d at 518-520 (holding that the Wiretap Act includes a defense of consent by either party to the communication and that the courts have found no unlawful interception of communications had occurred in either of these cases because the courts found that the consent of the Web portal entity was sufficient in itself to authorize a third-party to usurp their information).

189. *See In re Intuit*, 138 F. Supp. 2d at 1278.

190. *See In re Pharmatrak,* 329 F.3d at 20 (stating that "[w]ithout actual notice, consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception" (quoting Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998))). Moreover, "knowledge of the capability of monitoring alone cannot be considered implied consent" (quoting Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983)).

191. *See In re Pharmatrak*, 329 F.3d 9, 19-22.

show that the party knew about and consented to the interception."[192] Where the parties had an explicit contract limiting the permissible scope of the interception to non-personally identifiable data,[193] the court refused to find implied consent between the parties to collect personally-identifiable information that clearly exceeded the bounds of the express contract.[194] The *Pharmatrak*[195] requirement of actual consent represents a stricter stance on inferring consent than is taken in *Intuit*[196] and *DoubleClick*.[197] However, even under this construction, end-users never input all of the written information transmitted by cookie via clickstream technology over the Internet; thus, the courts have imputed consent by reasoning that end-users and their computers are the same entity. By limiting courts' abilities to infer consent to situations where actual consent has been obtained,[198] the *Pharmatrak* holding took a major step towards eliminating the judicially created clickstream data pseudo-exception under the Wiretap Act.[199] If this trend continues, courts may eliminate the clickstream data exception on their own by requiring either explicit or implicit actual consent for all third-party clickstream data interceptions under the Wiretap Act, including those data sent by end-users' machines without any end-user input.

IV. THE LEGAL SETTING OF VOIP COMMUNICATIONS

In the existing judicial environment, it is not clear whether VoIP communications will receive similar judicial treatment as oral telephone communications[200] or whether they will be treated as Internet based electronic communications.[201] The Wiretap Act's protective provisions apply equally to oral, wire, and electronic communications.[202] In

192. *See id.* at 20.

193. *See id.* at 19-22.

194. *Id.* at 21. Nevertheless, Pharmatrak collected personal information on a subset of users and distributed 18.7 million cookies via the Netcompare technology framework. *Id.* at 15.

195. *See id.* at 21.

196. *See In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1278 (C.D. Cal. 2001).

197. *See In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 514-15 (S.D.N.Y. 2001).

198. *See In re Pharmatrak*, 329 F.3d at 19 (stating that "consent may be explicit or implied, but it must be actual consent rather than constructive consent").

199. *Id.*

200. *See* Katz v. United States, 389 U.S. 347, 351-52 (1967) (stating that "[w]hat 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." (citation omitted)). Since it is possible that both the computer and the VoIP phone used by the communicants are within a home, their dialog should be protected as well.

201. *See* discussion *supra* Part II.

202. *See* Bartnicki v. Vopper, 532 U.S. 514, 526 (2001) ("The basic purpose of the Title III is to 'protec[t] the privacy of wire ... and oral communications.'") (quoting S. REP. NO. 90-1097, at 66 (1968)).

practice, however, courts have permitted the interception of Internet electronic communications under the Wiretap Act more than interceptions of oral telephone communications because (1) corporate web portals using clickstream technology frequently consent to the interception of end-user data for purposes of data mining, whereas telephone users rarely consent to third-party interceptions of telephone conversations;[203] (2) end-users are more likely to consent to interceptions of Internet electronic communications in return for increased online functionality than they are when engaging in traditional telephone conversations;[204] and (3) Internet electronic communications are more likely to be stored on an end-user's computer, making them fair game for third-party interceptors, since the Wiretap Act only applies to communications intercepted contemporaneously with transmission.[205]

---

203. *See* Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001) (holding that "[i]t is implicit in the web pages' code instructing the user's computer to contact Avenue A, either directly or via DoubleClick's server, that the web pages have consented to Avenue A's interception of the communication between them and the individual user"); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 514 (S.D.N.Y. 2001) (finding that "the DoubleClick-affiliated Web sites are 'parties to the communication[s]' from plaintiffs and have given sufficient consent to DoubleClick to intercept them").

204. A telephone communicant need not give express consent to authorize an interception under the Wiretap Act; such consent can be inferred from the surrounding circumstances. *See* United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987) (holding that consent can be inferred where circumstances indicate that a party knowingly agreed to surveillance), *cert. denied*, 485 U.S. 1021 (1988). However, inferring consent under the Wiretap Act for a telephone communication requires the party to have knowledge or notification, without which consent cannot be implied. *See In re* State Police Litigation, 888 F. Supp. 1235, 1266 (D. Conn. 1995) (holding that Plaintiff's claim under the Wiretap Act established sufficient evidence of an absence of either knowledge or notification to prevent the court from implying consent to the interception of a telephone communication).

205. *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 878 (9th Cir. 2002) (holding that for a Web site to be "intercepted" in violation of the Wiretap Act, it must be acquired during transmission, not while it is in electronic storage).

VoIP transmits in real time, offering comparable services to the traditional telephone. *See* Philip Carden, *Network Design Manual: Building Voice over IP*, NETWORK COMPUTING, *available at* http://www.networkcomputing.com/netdesign/1109voipfull.html (last visited July 12, 2005). As with telephone communications, VoIP interceptors will usually be intercepting the communications contemporaneously with transmission. *See* Nikita Borisov, Ian Goldberg, & David Wagner, *Intercepting Mobile Communications: The Insecurity of 802.11*, SEVENTH ANNUAL INTERNATIONAL CONFERENCE ON MOBILE COMPUTING AND NETWORKING, (July 2001); *see also* NIKITA BORISOV, IAN GOLDBERG, AND DAVID WAGNER, SECURITY OF THE WEP ALGORITHM, *available at* http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (last visited July 13, 2005). Unlike telephone communications, VoIP communications can be intercepted prior to post transmission while stored or cached on servers or end-users' computers. *See FBI Protests VoIP Approach*, Jan. 9, 2004, *available at* http://www.lightreading.com/document.asp?site-lightreading&doc_id45695. Possibly, the courts will hold that such interceptions do not violate the Wiretap Act because the communications were not intercepted contemporaneously with transmission. *Id.* In some situations, however, these VoIP interceptions may be prohibited by the Stored Communications Act, 18 U.S.C. §2701 (2004), or the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2004).

Currently, courts permit data tapping when actual consent is given by either party to the data transaction and the interception is not done for a criminal or tortious purpose.[206] VoIP communications are a hybrid type of communication, combining traditional telephone communication with Internet data transmission.[207] Even if courts treat VoIP as oral telephone communication as opposed to Internet data communication, scenarios will likely arise, such as in the case of spyware,[208] where courts may infer actual consent to interceptions of VoIP or other Internet electronic communication based on the willful use of spyware with notice of its capabilities, or a broad contractual consent agreement included in the spyware's end-user license agreement.[209]

This dichotomy in legal treatment between Internet communications and oral telephone communications is exacerbated in the realm of governmental surveillance because courts afford Fourth Amendment privacy protection to oral telephone communications[210] yet do not extend this protection to Internet electronic communications.[211] Courts have held that oral telephone communicants are entitled to a "reasonable expectation of privacy" for telephone conversations conducted in private.[212] Courts, however, have refused to recognize a "reasonable expectation of privacy" in Internet electronic

---

This Article's solution advocates that the legislature amend the Wiretap Act to prevent data mining companies from intentionally or recklessly intercepting VoIP conversations in transmission while they are legally mining other clickstream data. *See* discussion *infra* Part VII.

206. 18 U.S.C. § 2511(2)(d) (2004); *see also* Sussman v. American Broadcasting Companies, Inc., 186 F.3d 1200 (9th Cir. 1998) (affirming summary judgment in favor of defendant journalists who eavesdropped on telephone conversations. The court reasoned that "[u]nder section 2511, the focus is not upon whether the interception itself violated another law; it is upon whether the purpose for the interception—its intended use—was criminal or tortious . . . ."), *cert. denied* 528 U.S. 1131 (2000).

207. *See* Vonage Holdings Corp. v. Minnesota Public Utilities Comm'n, 290 F. Supp. 2d 993, 995 (D. Minn. 2003) ("Voice over Internet Protocol ('VoIP') . . . allows customers to place and receive voice transmissions routed over the Internet. . . . Voice communication using the Internet has been called Internet Protocol ('IP') telephony, and rather than using circuit switching, it utilizes 'packet switching,' a process of breaking down data into packets of digital bits and transmitting them over the Internet."). *See also* State *ex rel.* Cincinnati Bell Tel. Co. v. Pub. Util. Comm., 824 N.E.2d 68, 70 (Ohio 2005).

208. New.Net, Inc. v. Lavasoft, 356 F. Supp. 2d 1071, 1080 (C.D. Cal. 2003).

209. *Id. See also* Benjamin Adelman, *Gator's EULA Gone Bad, at* http://www.benedelman.org/news/112904-1.html (last visited July 13, 2005).

210. *See* Katz v. United States, 389 U.S. 347, 353 (1967) (use of electronic eavesdropping equipment to overhear conversation inside telephone booth intrudes on legitimate expectation of privacy).

211. *See* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis.").

212. *See Katz,* 389 U.S. at 353 (use of electronic eavesdropping equipment to overhear conversation inside telephone booth intrudes on legitimate expectation of privacy).

communications[213] reasoning that, as the Internet is public in nature, communications therein should receive a disfavored privacy protection status.[214] Some Internet communications, however, such as e-mail, are afforded a "reasonable expectation of privacy" under the Fourth Amendment[215] because they can be analogized to a letter placed in the postal mail, which is afforded privacy protection under the Fourth Amendment.[216]

Like oral telephone communicants, VoIP communicants can personally record their own dialogue[217] or can contract their privacy rights away to a third party, such as Vonage, that can record and resell the dialogue.[218] Today, this technology is being used in corporate voice mail systems, enabling companies to eavesdrop on any oral telephone conversations saved on the company's VoIP network server.[219] These conversations are often not protected by the Fourth Amendment or the Wiretap Act because employees consent to the interception in their employment contracts, leaving them with no reasonable expectation of privacy.[220] While the courts have recognized exceptions to absolute oral

213. *See Hambrick*, 55 F. Supp. 2d at 508 ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis.").

214. *Id.*

215. *See id.*

216. *See* cases cited *supra* note 105.

217. *See* Sussman v. American Broadcasting Companies, Inc., 186 F.3d 1200 (9th Cir. 1999) (holding that the Wiretap Act permits interception of wire, oral, or electronic communications to which that person is party, unless the communication is intercepted for purpose of committing any criminal or tortious act), *cert. denied*, 528 U.S. 1131 (2000).

218. *See generally* Vonage Holdings Corp. v. Minnesota Pub. Utilities Comm'n, 290 F. Supp. 2d 993, 994 (D. Minn. 2003). While the technology to catalogue and store oral communications is in its infancy, hypothetically it will develop given its market potential once most corporate entities begin using VoIP systems. *Id. See also* STEVEN TAYLOR, DISTRIB. NETWORKING ASSOC., INC., 2004 VOIP STATE OF THE MARKET REPORT (2004), *at* http://www.webtorials.com/abstracts/VoIPSurvey2004.htm (last visited Feb. 10, 2005).

219. *See, e.g.*, Dan McIntosh, *E-monitoring@workplace.com: The Future of Communication Privacy in the Minnesota Private Sector Workplace*, 23 HAMLINE L. REV. 539, 549 (2000) (describing the Business Use, Consent and Provider exceptions to the ECPA and stating that "the exceptions have been applied favorably to employers and thus, have posed significant hurdles to employee claims under the ECPA that allege unlawful interception or access of workplace communications"). *See also* Konrad L. Trope & Paula K. Royalty, *Current Legal Issues Surrounding the Regulation of Voice Over Internet Protocol*, 16 J. PROPRIETARY RTS. 10, 11, (2004) ("Some companies like MetaSwitch and Cisco Systems, Inc., have already cooperated with the FBI's request for CALEA compliance to make their VoIP hardware products 'surveillance friendly.' These two companies have 'developed backdoor technology in their VoIP products that enables the FBI to eavesdrop at will.'").

220. *See, e.g.*, United States v. Angevine, 281 F.3d 1130, 1132, 1134 (10th Cir. 2002) (holding that a professor had no reasonable expectation of privacy in his work computer when the university had a written computer policy stating that it reserved the right to "view or scan any file or software stored on the computer or passing through the network"); *see also* Dir. of Thrift Supervision v. Ernst & Young, 795 F. Supp. 7, 10 (D. D.C. 1992) (finding that employees and partners of accounting firm

telephone communication privacy rights for interceptions that occur with the consent of a party,[221] in the ordinary course of business,[222] by a spouse,[223] or in prison,[224] they do not permit unauthorized third-party eavesdropping.

VoIP communications should be placed squarely within the realm of traditional telephone conversations and, because they both use a wire to enable oral communications, they should be identical in the eyes of the law.[225] The Wiretap Act prohibits the interception of wire, oral, or electronic communications[226] without a court order[227] unless one of the parties to the communication consents to the interception.[228] Under this reasoning, oral VoIP communications cannot be intercepted without a court order[229] unless one of the parties to the communication actually consents to the interception.[230] To maintain parity in the Wiretap Act's protections, courts should refuse to liberally infer consent to the interception of VoIP communications based on an Internet user's consent to the interception of Internet data communications in general. If courts

---

had no reasonable expectation of privacy in work-related diaries kept in their offices for business reasons).

221. 18 U.S.C. § 2511(2)(d) (2004).

222. *See* Arias v. Mutual Cent. Alarm Servs., Inc., 182 F.R.D. 407, 413 (S.D.N.Y. 1998) (holding that an alarm service company's recording of all incoming and outgoing telephone calls, including employee calls, did not violate the ECPA since the company's recording of the conversations was justified by "their legitimate interests in timely provision of emergency services, ensuring employee fidelity, and protecting themselves against unfounded claims since it intercepted telephone calls within its ordinary course of business"), *aff'd*, 202 F.3d 553 (2d Cir. 2000); *but see* Campiti v. Walonis, 611 F.2d 387 (1st Cir. 1979) (rejecting an ordinary course of business argument in a prison monitoring case because the call in question was not routinely monitored and, indeed, was "an exceptional course of conduct").

223. *See* Thompson v. Dulaney, 838 F. Supp. 1535, 1544-45 (D. Utah 1993) (stating that "as long as the guardian has a good faith basis that is objectively reasonable for believing that it is necessary to consent on behalf of her minor children to the taping of the phone conversations, vicarious consent will be permissible in order for the guardian to fulfill her statutory mandate to act in the best interests of the children." The court, however, held that a divorced wife's defense of consent under the Wiretap Act was inapplicable for public policy reasons because the interceptions amounted to criminal and civil violations of Utah law, rendering the consent exception inapplicable.).

224. *See* United States v. Van Poyck, 77 F.3d 285 (9th Cir. 1996) (holding that the routine monitoring of inmate telephone calls by federal prison authorities was within the ordinary course of their duties), *cert. denied*, 519 U.S. 912 (1996).

225. 18 U.S.C. § 2510(1) (2004).

226. 18 U.S.C. § 2511 (2004).

227. Court ordered surveillance is limited to law enforcement bugs or wiretaps. Section 2518 establishes strict requirements for court authorized interceptions of wire communications. 18 U.S.C. § 2518 (2000).

228. 18 U.S.C. §§ 2511(2)(c)-(d) (2000) (containing consent defenses).

229. Court ordered surveillance is limited to law enforcement bugs or wiretaps. Section 2518 establishes strict requirements for court authorized interceptions of wire communications. 18 U.S.C. § 2518 (2000).

230. 18 U.S.C. §§ 2511(2)(c)-(d) (2000) (containing consent defenses).

define consent broadly, VoIP communications will become a less secure means of oral communication than traditional oral telephone communications, even though they are explicitly protected as "wire communications" under the Wiretap Act.[231]

V. STATUTORY CONSTRUCTION ANALYSIS

The Wiretap Act's language can be read to support either a broad or narrow construction of consent, though VoIP's oral nature favors the narrower.[232] This narrow interpretation is driven by the Supreme Court's holding in *Katz*,[233] where the Court recognized that oral telephone communications are entitled to a higher level of legal protection based on the Constitution's Fourth Amendment Privacy Rights.[234] Ideally, the legislature would resolve the judicial ambiguities that have arisen in interpreting the Wiretap Act by redrafting it[235] to distinguish oral communications whether transmitted over a wire, via a telephone network, or by VoIP from electronic communications, thereby addressing the clickstream data exemption.[236]

The Wiretap Act's express language categorically includes written information, but by examining the drafters' intent and applying a little common sense, one could argue that Congress created a pseudo-clickstream data exception.[237] As discussed above, the federal courts

---

231. 18 U.S.C. § 2510(1) (2004).

232. 18 U.S.C. § 2511 (2004). Interception and disclosure of wire, oral, or electronic communications prohibited.

(1) Except as otherwise specifically provided in this chapter any person who—

(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication;

(b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when . . . ."

Id.

233. Katz v. United States, 389 U.S. 347, 359 (1967).

234. *See supra* text accompanying note 12; Olmstead v. United States, 277 U.S. 438, 466, 472-74, 478 (1928) (Brandeis, J., dissenting) (majority holding that a wiretap not effected through a trespass onto private property did not violate the Fourth Amendment.); Edward J. Bloustein, *Privacy, Tort Law, and the Constitution: Is Warren and Brandeis' Tort Petty and Unconstitutional as Well?*, 46 TEX. L. REV. 611 (1968).

235. The regulatory distinction between oral and data has been derived from the regulatory objective to cross-subsidize local service and 911 service with the result that interstate service is heavily taxed and/or levied. Voice over IP is less expensive to use than end-user because it bypasses most of the taxes and levies. *See generally* DECLAN MCCULLAGH, CONGRESS PROPOSES TAX ON ALL NET, DATA CONNECTIONS (Jan. 28, 2005), *available at* http://news.com.com/Congress+proposes+tax+on+all+Net,+data+connections/2100-1028_3-5555385.html (last visited July 18, 2005).

236. It is beyond the scope of this article to discuss the appropriate statutory language for the revised Wiretap Act.

237. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 505 n.14 (S.D.N.Y 2001).

have created a clickstream data exception, which permits the interception of machine-generated Internet data communications under the Wiretap Act by inferring, on behalf of the transmitting party's computer, actual consent to the interception of the "electronic communication."[238] Analyzing the Wiretap Act using statutory construction techniques yields two different lines of argument.[239] The first and strongest applies the *plain meaning* approach and concludes that the Wiretap Act protects all "electronic communications," including machine-generated Internet electronic communication, from all unauthorized interceptions. The statutory language does not support the argument that some but not all "electronic communications" are protected. Analyzing the Wiretap Act through the plain meaning approach[240] leads to the conclusion that all oral, written, and electronic communications transmitted over a wire, without the consent of one of the parties or a court order, are protected.[241]

The second interpretation applies the statutory *intent* technique,[242] arguing that the drafters of the Wiretap Act and its subsequent amendments intended to distinguish between human and clickstream data.[243] This argument has never been directly applied by the courts[244] because the courts have focused on interpreting "consent" to permit the

238. *See id.* at 511 ("Although the users' requests for data come through clicks, not keystrokes, they nonetheless are voluntary and purposeful. Therefore, because plaintiffs' GET, POST and GIF submissions to DoubleClick-affiliated websites are all 'intended for' those websites, the websites' authorization is sufficient to except DoubleClick's access under § 2701(c)(2).").

239. *See, e.g.*, Cass R. Sunstein, *Interpreting Statutes in the Regulatory State*, 103 HARV. L. REV. 405, 411 (1989) (discussing interpretative rules for regulatory statutes).

240. *See* United States v. American Trucking Ass'ns, Inc., 310 U.S. 534, 543 (1940) (stating that there is "no more persuasive evidence of the purpose of a statute than the words by which the legislature undertook to give expression to its wishes"); Caminetti v. United States, 242 U.S. 470, 490 (1917) ("when words are free from doubt they must be taken as the final expression of the legislative intent").

241. 18 U.S.C. § 2511 (2004).

242. *See, e.g.*, International Bhd. of Teamsters v. United States, 431 U.S. 324, 350-51 (1977); McDonald v. Santa Fe Trail Transp. Co., 427 U.S. 273, 280 (1976); Griggs v. Duke Power Co., 401 U.S. 424, 434 n.11 (1971).

243. S. REP. No. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112 [hereinafter S. REP. NO. 90-1097].

244. *See In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272 (C.D. Cal. 2001); *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *1 (N.D. Cal. Oct. 9, 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001). In each case, the court held that no unlawful interception had occurred because, even if the transmission to the third party constituted an "interception" of the user's communications with the Web site, it was done with the consent of the Web site, which was a party to the communication. *But see In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 15 (1st Cir. 2003) (finding that there was no consent under the Wiretap Act, 18 U.S.C. § 2511(2)(d) (2004), where a corporate entity had an explicit agreement prohibiting a third-party from collecting personal identifiable information).

interception under the Wiretap Act.[245] In Internet electronic communication interception cases, the courts have read the Wiretap Act's consent exception[246] broadly by finding implied consent absent any explicit agreement between the parties to authorize third-party interception under the Wiretap Act.[247] By using this argument, the courts were able to sidestep the prohibition against third-party interception of electronic communications supported by the plain meaning of the Wiretap Act.

Because the two statutory analysis approaches are in direct conflict with one another, the onset of VoIP compels a reexamination of which interpretation is most appropriate for the Wiretap Act. This Article argues that the "plain meaning" of the Wiretap Act establishes comprehensive statutory protection for all forms of "electronic communications."[248] The legislature, therefore, should either reinforce this strict prohibition or redraft the Wiretap Act to separate oral[249] from machine-generated Internet electronic communications, thus resolving the ambiguities that have arisen through judicial interpretation of the Wiretap Act.[250]

A. Plain Meaning Analysis Supports Comprehensive Protection for All Communications Including Clickstream Data and VoIP

The plain meaning approach[251] has many formulations, but its central tenet is that there is no need to interpret unambiguous language.[252] Courts that have applied the plain meaning rule have even

---

245. *See In re DoubleClick*, 154 F. Supp. 2d 497; *In re Intuit*, 138 F. Supp. 2d 1272; *In re Toys R Us*, No. 00-CV-2746, 2001 WL 34517252, at *1; *Chance*, 165 F. Supp. 2d 1153. In each case, the court held that no unlawful interception had occurred because, even if the transmission to the third party constituted an "interception" of the user's communications with the Web site, it was done with the consent of the Web site, which was a party to the communication. *But see In re Pharmatrak*, 329 F.3d at 15 (finding that there was no consent under the Wiretap Act, 18 U.S.C. § 2511(2)(d) (2004), where a corporate entity had an explicit agreement prohibiting a third-party from collecting personal identifiable information).

246. 18 U.S.C. § 2511(2)(c) (2004).

247. *See* cases cited *supra* note 244.

248. 18 U.S.C. § 2510(12) (2004).

249. 18 U.S.C. § 2510(2) (2004).

250. It is beyond the scope of this article to discuss the appropriate statutory language for the revised Wiretap Act.

251. *See* William N. Eskridge, Jr., *Dynamic Statutory Interpretation*, 135 U. PA. L. REV. 1479, 1483 (1987).

252. *See* United States v. American Trucking Ass'ns, Inc., 310 U.S. 534, 543 (1940) (holding that there is "[n]o more persuasive evidence of the purpose of a statute than the words by which the legislature undertook to give expression to its wishes"); *see also* Miller v. French, 530 U.S. 327, 336 (2000)); Northbrook Nat'l Ins. Co. v. Brewer, 493 U.S. 6, 9 (1989) ("[W]e must take the intent of Congress with regard to the filing of diversity cases in Federal District Courts to be that which its language clearly sets forth" (alteration in original) (quoting Horton v. Liberty Mutual Insurance Co.,

refused to look at a statute's title.[253] In federal courts, the most common effect of the plain meaning rule is to preclude extensive review of the legislative history through reports, hearings, and debates.[254] The plain meaning rule denies any need to examine the legislative intent unless the words are so ambiguous that the plain meaning leads to an absurd result.[255]

The Wiretap Act's text makes explicit reference to "writing" in electronic form.[256] The literal text of the Wiretap Act applies to both written and oral communications transmitted over a wire: the prohibited action is one that "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication."[257]

Arguably, these words leave little room for any creative interpretation. The application of this statutory language to oral communications includes voice communications utilizing VoIP technology that fall under the protected scope[258] of the Wiretap Act as wire and electronic communications. Also, VoIP transmits oral communication over a wire,[259] and thus should receive extended privacy rights according to *Katz*[260] as discussed above.[261] In summation, the courts have repeatedly held that where the plain meaning of a statute is

---

367 U.S. 348, 352 (1961) (internal quotation marks omitted)); United States v. Vest, 813 F.2d 477, 481 (1st Cir. 1987).

253. *See* Caminetti v. United States, 242 U.S. 470, 490 (1917) ("when words are free from doubt they must be taken as the final expression of the legislative intent"); Hayden v. The Collector, 72 U.S. 107, 110 (1866); Abdul-Akbar v. McKelvie, 239 F.3d 307, 313 (3d Cir. 2001) (stating that the plain meaning of a statute controls unless the language is ambiguous or leads to absurd results). The title may not be used to add or to take from the body of the statute, but it may be used to assist in the interpretation of its meaning. *Hayden*, 72 U.S. at 110. The title of the Wiretap Act, 18 U.S.C. § 2511 (2004), is "[i]nterception and disclosure of wire, oral, or electronic communications prohibited." This title is ambiguous as to whether or not electronic communications can be attributed to both humans and machines, or to solely humans.

254. *See, e.g., Abdul-Akbar*, 239 F.3d at 317 (stating that "[h]aving applied the American Plain Meaning Rule and having determined that there is no ambiguity," the court is not required to answer Plaintiff's contention that the plain meaning of the statute is inconsistent with Congress' intent).

255. *See* United States v. Brown, 333 U.S. 18, 27 (1948) (holding that a court can reject the plain language interpretation of a statute if such an interpretation would lead to "patently absurd consequences").

256. 18 U.S.C. § 2510(12) (2004) (definition of electronic communications includes "writing").

257. 18 U.S.C. § 2511(1)(a) (2004).

258. 18 U.S.C. § 2511(a)-(e) (2004).

259. VoIP transmissions can also be transmitted over Wi-Fi. For a general overview, *see* Joel Conover, *Anatomy of IEE 802.11b Wireless*, NETWORK COMPUTING, Aug. 7, 2000.

260. *See* Katz v. United States, 389 U.S. 347, 351-52 (1967).

261. *See* discussion *supra* Section III.A.

not ambiguous it should be followed as written;[262] therefore the courts should rigidly enforce the Wiretap Act to prohibit unauthorized interceptions of wire, oral and electronic communications.[263] Arguably, however, Congress intended the Wiretap Act to apply only to wire, oral, and electronic communications generated by humans, thereby exempting clickstream data.[264]

B. Intent Arguments Support a Clickstream Data Exception

The plain meaning argument is not dispositive because the Wiretap Act's legislative history[265] and text[266] both focus on direct inter-human communications initiated by the parties to the communication,[267] thereby permitting the clickstream data exception.[268] "[O]ral communication"[269] privacy is essential for entering into and altering personal, intimate, and political associations.[270] As some jurists have observed, "[n]o one talks to

---

262. *See* United States v. Montejo, 353 F. Supp. 2d 643, 647 (E.D. Va. 2005) (stating that courts "should not look beyond [the plain meaning] unless there is ambiguity or unless the statute as literally read would contravene the unambiguously expressed legislative intent gleaned from the statute's legislative history. Even if the result appears to be anomalous or absurd in a particular case, the court may not disregard unambiguous language.") (citing United States v. Sheek, 990 F.2d 150, 152-153 (4th Cir. 1993)).

263. 18 U.S.C. § 2511 (2004).

264. *See* H.R. REP. NO. 99-647, at 18 (1986) (stating that "[l]egal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology."

265. S. REP. NO. 1097, *supra* note 243, at 2153-54.

266. 18 U.S.C. § 2511 (2004).

267. Common sense dictates that the Wiretap Act was intended to apply to communications between humans because computers cannot be held in violation of the Wiretap Act subject to criminal or civil liability unless they are acting as some persons' agent, including corporations. Senator McClellan, who co-sponsored Title III, remarked that "[t]o assure the privacy of oral and wire communications, Title III prohibits all wiretapping . . . by persons other than duly authorized law enforcement officers." United States. v. Jones, 542 F.2d 661, 669 (6th Cir. 1976). This statement enforces the common sense argument because it plainly states that the statute's focus is on inter-human communications.

268. *See In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272 (C.D. Cal. 2001); *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *1 (N.D. Cal. Oct. 9, 2001); Chance v. Avenue A., Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001). In these cases, the courts held that no unlawful interception had occurred because, even if the transmission to the third party constituted an "interception" of the user's communications with the Web site, this was done with the consent of the Web site owner, which was a party to the communication. *But see In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 15 (1st Cir. 2003) (finding that there was no consent under the Wiretap Act, 18 U.S.C. § 2511(2)(d) (2004), where a corporate entity had an explicit agreement prohibiting a third-party data from collecting personal identifiable information).

269. 18 U.S.C. § 2510(2) (2004).

270. *See* United States v. United States Dist. Court for E.D. Mich., 407 U.S. 297 (1972) (holding that the President did not have the inherent power to wiretap phones of United States citizens); Commonwealth v. Blood, 507 N.E.2d 1029 (Mass. 1987) (noting that Massachusetts law prohibits unreasonable searches and seizures by electronic surveillance of conversations in the home unless all of the parties have consented); *see also* Bartnicki v. Vopper. 532 U.S. 514, 532 (2001)

a recorder as he talks to a person."[271] If the plain meaning argument were correct, and if the Wiretap Act was intended to prohibit all unauthorized interception of "electronic communications,"[272] Internet commerce would be disrupted because a large number of website operations that rely upon clickstream data would be unlawful.[273] This result arguably creates an unworkable interpretation, and such an interpretation is not entitled to deference.[274] Thus, the intent of the drafters should be examined to see if it conforms to the plain meaning construction.[275]

A strong intent-based[276] counterargument can be made that the drafters of the Wiretap Act intended[277] "electronic communications" to include only human-generated communications. 18 U.S.C. §2510(12) defines "electronic communications" as including "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire . . . ."[278] An argument can be made that the Wiretap Act's drafters intended it to prohibit unauthorized interceptions of human "oral" and "electronic communications" in "writing," while exempting machine-generated clickstream data from its scope.[279] When interpreting a statute, it is paramount to determine the

---

(recognizing the role of privacy in communications in an "uninhibited exchange of ideas" amongst citizens).

271. *See* Holmes v. Burr, 486 F.2d 55, 72 (9th Cir. 1973) (Hufstedler, J., dissenting).

272. 18 U.S.C. § 2510(12) (2004).

273. Pitofsky, *supra* note 101 and accompanying text.

274. *See, e.g.*, Barry v. St. Paul Fire & Marine Ins. Co., 555 F.2d 3, 7 (1st Cir. 1977) ("We would be justified in probing legislative history if the language were ambiguous or if, even though unambiguous, the language literally read produced a senseless or unworkable statute.").

275. *See* Calderon v. Atlas S.S. Co., 170 U.S. 272, 281 (1898) (holding that the intent must be gathered from the words such that it avoids a result of "absurdity, which the legislature ought not to be presumed to have intended" (quoting United States v. Hartwell, 73 U.S. (6 Wall.) 385, 396 (1868)).

276. *See* United States v. Rio Grande Dam & Irrigation Co., 174 U.S. 690, 706-07 (1899) (refusing to acknowledge a construction ignoring "the spirit of the legislation and carr[ying] the statute to the verge of the letter and far beyond what under the circumstances of the case must be held to have been the intent of Congress").

277. *See* S. REP. NO. 99-541, at 13 (1986) ("Section 101(a)(2) of the Electronic Communications Privacy Act amends the definition of 'oral communication' in current section 2510(2) of title 18 to exclude electronic communications. There have been cases involving radio communications in which the court having determined that the radio communication was not a wire communication then analyzes it in privacy terms to determine if it is an oral communication. The bill rejects that analysis by excluding electronic communications from the definition of oral communications. An oral communication is an utterance by a person under circumstances exhibiting an expectation that the communication is not subject to interception, under circumstances justifying such an expectation. In essence, an oral communication is one carried by sound waves, not by an electronic medium.").

278. 18 U.S.C. § 2510 (2004).

279. *See In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272 (C.D. Cal. 2001); *In re* Toys R Us, Inc., Privacy Litig., No. 00-CV-2746, 2001 WL 34517252, at *1 (N.D. Cal. Oct 9, 2001); Chance v. Avenue A., Inc.,

purpose that should be attributed to it.[280] In the case of the Wiretap Act, it is particularly appropriate to consider the drafters' intent[281] because the advancement of new technology has created a great deal of ambiguity regarding the Wiretap Act's plain meaning.[282] The primary objective of the Wiretap Act is to protect the privacy of human communications;[283] the recognition of the clickstream data exception is necessary so that the purpose of the legislature is enforced and not subverted.[284]

The Wiretap Act's legislative history demonstrates that Congress intended the Wiretap Act to encompass instances of third-party wiretapping of oral, written, and electronic communications. The legislative history of the original 1967 Wiretap Act and all of its subsequent amendments focused on human-generated communications.[285] In 1967, Congress intended the Wiretap Act to establish the authority and standards for government wiretaps for criminal investigations[286] and to protect individuals against unauthorized

---

165 F. Supp. 2d 1153 (W.D. Wash. 2001). In these cases, the courts held that no unlawful interception had occurred because, even if the transmission to the third party constituted an "interception" of the user's communications with the Web site, this was done with the consent of the Web site owner, which was a party to the communication. *But see In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 15 (1st Cir. 2003) (finding that there was no consent under the Wiretap Act, 18 U.S.C. § 2511(2)(d), where a corporate entity had an explicit agreement prohibiting a third-party data from collecting personal identifiable information).

280. *See* Zuber v. Allen, 396 U.S. 168, 186 (1969); *see also* Thornburg v. Gingles, 478 U.S. 30, 43-44 n.7-8 (1986) (committee reports are the "authoritative source for legislative intent"); Garcia v. United States, 469 U.S. 70, 76 (1984) (the "authoritative source for finding the Legislature's intent lies in the Committee Reports on the bill . . . ."); Schwegmann Bros. v. Calvert Distillers Corp., 341 U.S. 384, 395-96 (1951) (Jackson, J., concurring) (arguing that the court should look no further than the committee reports in examining the legislative history).

281. Title III was amended in December 1986. The Act now sets forth restrictions and imposes civil and criminal sanctions for the unlawful interception of "electronic communications" as well as retaining those on "wire" and "oral" communications. *See* Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2520 (2004).

282. The ECPA was drafted with the intent to provide protection against unauthorized interceptions in areas of recent technological advancement, e.g., cellular and cordless telephones, pen registers, electronic mail, etc. *See* S. REP. NO. 99-541, at 13 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555-57.

283. *See* Katz v. United States, 389 U.S. 347, 351 (1967).

284. *See* H.R. REP. NO. 99-647, at 18 (1986) ("Legal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology.").

285. In a Senate report pertaining to Title III, it was stated that "[18 U.S.C. § 2511(1)(a)] establishes a blanket prohibition against the interception of any wire communication." S. REP. NO. 90-1097 at 2180. The report also stated that the definition of a "person" in 18 U.S.C. § 2510(6) (2004) is "intended to be comprehensive." *Id.* at 2179.

286. 18 U.S.C. § 2520 (2004); *see also* United States v. Giordano, 416 U.S. 505, 514 (1974) ("The purpose of the legislation, which was passed in 1968, was effectively to prohibit, on the pain of criminal and civil penalties, all interception of oral and wire communications, except those specifically provided for in the Act, most notably those interceptions permitted to law enforcement officers when authorized by court order in connection with the investigation of the serious crimes listed in § 2516.").

invasions of their private oral telephone communications via wiretapping.[287]

In 1986, Congress passed the ECPA,[288] which made notable amendments to the Wiretap Act in order to keep up with technological advancements.[289] Congress intended the ECPA to re-establish the balance between privacy and law enforcement that had been upset, to privacy's detriment, by the development of new communication devices, computer technology, and changes in the structure of the telecommunications industry.[290] In passing the ECPA, Congress specifically acknowledged "large-scale electronic mail operations, cellular and cordless phones, paging devices, miniaturized transmitters for radio surveillance, and a dazzling array of digitized networks."[291] The legislative history suggests that Congress sought to prevent the Wiretap Act from being gradually eroded as technology advanced.[292] It is evident that Congress drafted the ECPA to focus on human communications, not on clickstream data.[293] In addition to the goals of privacy and law enforcement, the ECPA sought to advance the development and use of these new technologies and services.[294] Although Congress intended to encourage the proliferation of new communications technologies, it recognized that consumers would not trust new technologies if the privacy of individuals using them was not protected.[295]

Congress designed the ECPA to provide rules for government surveillance in the modern age. However, technology has evolved in unanticipated ways. The interactive nature of the Internet now includes a multitude of communications, some of which are generated by computers without the end-user even knowing that they are communicating information.[296] In this context, a person's electronic communications encompass much more today than they would have in 1986.[297] Congress' intent in drafting the Wiretap Act and its subsequent amendments has

287. 18 U.S.C. § 2511 (2004).

288. Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-3127 (2004).

289. *See* H.R. REP. NO. 99-647, at 2 (1986).

290. *Id.* at 17-19.

291. *Id.* at 18.

292. *See* S. REP. NO. 99-541, at 2-3, 5 (1986); H.R. REP. NO. 99-647, at 16-19 (1986).

293. *See* H.R. REP. NO. 99-647, at 18 (1986) ("Illegal protection against the unreasonable use of newer surveillance techniques has not kept pace with technology.").

294. *See* S. REP. NO. 99-541, at 5 (1986) (noting that legal uncertainty over the privacy status of new forms of communications "may unnecessarily discourage potential customers from using innovative communications systems").

295. *See* S. REP. NO. 99-541, at 5 (1986); H.R. REP. NO. 99-647, at 19 (1986).

296. *See In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001) ("Cookies are computer programs commonly used by Web sites to store useful information . . . .").

297. *See* H.R. REP. NO. 106-932, at *9 (2000).

consistently focused on protecting "oral,"[298] "wire,"[299] or "written"[300] human communication; because privacy rights apply to people and not machines, a clickstream data exception is an absolute necessity.[301]

A number of courts have adopted this view.[302] In discerning Congressional intent, courts have concluded that Congress intended to exempt clickstream data from the Wiretap Act, finding that the interception of clickstream data[303] falls outside the scope of the Wiretap Act's protection. The courts in *DoubleClick* and *Intuit* recognized the existence of an exception for clickstream data because they found implicit consent where explicit consent was lacking, thereby enabling third parties to intercept clickstream data. While on its face this exception violates the plain meaning of the Wiretap Act,[304] the courts, by focusing on consent, interpreted the Wiretap Act in the spirit of its legislative purpose.[305] When this reasoning is applied to VoIP, it is possible that neither party will consent to the interception of its communication, but such an interception would be permissible because of clickstream technology's indirect role in the facilitation of VoIP communication.[306]

Further supporting an intent-based approach is the judicial canon that a statute should always be presumed to be the work of reasonable men.[307] This common sense rule requires the courts to give deference to an interpretation that is both reasonable and constitutional.[308] Here, the intent approach is both reasonable and constitutional because machine generated clickstream data does not deserve constitutional protection since it cannot have a reasonable expectation of privacy. The plain meaning approach would bring the Internet to a standstill because of the

298. 18 U.S.C. § 2510(2) (2004).

299. 18 U.S.C. § 2510(1) (2004).

300. 18 U.S.C. § 2510(12) (2004) (defining electronic communications to include "writing").

301. The Fourth Amendment protects people, not places. Katz v. United States, 389 U.S. 347, 351 (1967). Courts have held that students occupying college dormitories enjoy the protection of the Fourth Amendment. Piazzola v. Watkins, 442 F.2d 284, 289 (5th Cir. 1971).

302. *See In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1278, 1278 (C.D. Cal. 2001).

303. *See In re DoubleClick*, 154 F. Supp. 2d at 503-04; *In re Intuit*, 138 F. Supp. 2d at 1274.

304. 18 U.S.C. § 2511 (2004).

305. Sunstein, *supra* note 239.

306. *See* discussion *supra* Section II and II.B.

307. *See, e.g.*, International Bhd. of Teamsters v. United States, 431 U.S. 324, 350-51 (1977); McDonald v. Santa Fe Trail Transp. Co., 427 U.S. 273, 280 (1976); Griggs v. Duke Power Co., 401 U.S. 424, 434 n.11 (1971).

308. *See* Crowell v. Benson, 285 U.S. 22, 62 (1932) ("When the validity of an act of the Congress is drawn in question, and even if a serious doubt of constitutionality is raised, it is a cardinal principle that this Court will first ascertain whether a construction of the statute is fairly possible by which the question may be avoided.").

Internet's reliance on clickstream technology.[309] While not offering an ideal solution, the statutory intent approach provides a viable solution until Congress rewrites the Wiretap Act or explicitly acknowledges the plain meaning interpretation.[310]

VI. THE PROBLEM OF CLICKSTREAM DATA AND CONVERGING COMMUNICATIONS

While the courts have solved the immediate problem concerning data communications by distinguishing between explicit consent and pseudo-implicit consent, their solution is untenable. Courts have recognized that oral telephone and Internet electronic communications are subject to different levels of privacy rights: oral telephone communications fall under the umbrella of the Fourth Amendment construction of "reasonable expectations of privacy"[311] while Internet electronic communications do not.[312]

Proponents of VoIP technology advocate less stringent regulations and judicial interference in VoIP than exists today in telephone technology,[313] which, while logical, contradict the intent of both the Supreme Court[314] and Congress.[315] Between the landmark *Katz* case and

309. *See* discussion *supra* Part II.B.

310. *See* discussion *infra* Part VII.

311. *See* Katz v. United States, 389 U.S. 347, 351 (1967) (holding that the respondent need not be at "home," in order to enjoy a reasonable expectation of privacy). "[T]he Fourth Amendment protects people, not places," *id.*, and provides sanctuary for citizens wherever they have a legitimate expectation of privacy. *Id.* at 359.

312. *See* United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) ("For Fourth Amendment purposes, this court does not find that the ECPA has legislatively determined that an individual has a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of Internet connection. The fact that the ECPA does not proscribe turning over such information to private entities buttresses the conclusion that the ECPA does not create a reasonable expectation of privacy in that information. This, however, does not end the court's inquiry. This court must determine, within the constitutional framework that the Supreme Court has established, whether Mr. Hambrick's subjective expectation of privacy is one that society is willing to recognize.").

313. *See* Jeffrey Citron, Presentation at the FCC Forum on Voice Over Internet Protocol (Dec. 1, 2003) (transcript available at http://www.fcc.gov/voip/presentations/citron.doc).

314. In *Katz*, the Court drew a line between oral statements that are considered private under the Constitution and those statements that lack constitutional protection. 389 U.S. at 351-53. The Court properly ruled out the "constitutionally protected area" test, which afforded a bright line, but an irrational one. *Id.* at 351.

315. When Congress passed the Wiretap Act, it covered almost all aspects of an intangible conversation, thereby obviating the complexity that would have arisen if it distinguished between its various attributes. The Wiretap Act protected the "contents" of communications, but expansively defined "contents" as "any information concerning the identities of the parties to such communication or the existence, substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (1968). The definition of contents was designed to be comprehensive. *See* S. REP. NO. 90-1097, at 91 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2179 (defining "contents" to include "all aspects of the communication").

the passage of the Wiretap Act, the Court and Congress have sought to create a zone of oral communication privacy. The Supreme Court in *Katz*[316] recognized an individual's reasonable expectation to conversational privacy within the context of his or her own home.[317] Despite this precedent, lower courts have, in data privacy cases, focused primarily on "consent,"[318] not on who or what has authored the information.[319] By electing to focus on "consent,"[320] the courts have constructed a lower level of privacy with respect to clickstream data transmissions[321] which, when applied to Internet voice communications such as VoIP, contradicts the plain meaning of the Wiretap Act, obviates the *Katz* line between protected and unprotected,[322] and violates an individual's right to privacy.

Nevertheless, the lower courts' creation of the clickstream data exception is commendable because it enabled the Internet to flourish.[323] If the courts had relied only upon the Wiretap Act's plain meaning and found that the statute was unambiguous, the Internet economy would have been disrupted.[324] Though using the intent approach and creating the clickstream data exception is not perfect, it is a more appropriate interpretation of the Wiretap Act given the potential adverse impact of the plain meaning approach.

VII. SOLUTION

Applying the judicially created clickstream data exception[325] to the Wiretap Act creates a substantial risk that companies and individuals legally engaged in tracking clickstream data could simultaneously intercept oral VoIP and other electronic communications, both of which

316. *See Katz*, 389 U.S. at 351-353.

317. *See id.* at 353; United States v. Smith, 978 F.2d 171, 177 (5th Cir. 1992) (finding that the Fourth Amendment clearly protects communications carried by land-based telephone lines). On the other hand, pure radio communications are afforded no such protection because "[b]roadcasting communications into the air by radio waves is more analogous to carrying on an oral communication in a loud voice or with a megaphone than it is to the privacy afforded by a wire." *See* Goodall's Charter Bus Serv., Inc. v. San Diego Unified Sch. Dist., 178 Cal. Rptr. 21 (1981).

318. In four reported cases, cookie technology was used by websites to mine personal information from the users' machines. *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 12 (1st Cir. 2003); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1155 (W.D. Wash. 2001).

319. *See* discussion *supra* Part III.C.

320. *See* cases cited *supra* note 318.

321. *See* discussion *supra* Part II.B.

322. *See Katz*, 389 U.S. at 350.

323. *See* discussion *supra* Part III.C.

324. *See supra* note 101 and accompanying text.

325. *See In re* DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 505 n.14 (S.D.N.Y 2001).

are protected by the Wiretap Act.[326] The Wiretap Act's high mens rea requirement of an intentional interception permits the negligent, reckless, or knowing interception of communications.[327] This high mens rea requirement, coupled with the judicially created clickstream data exception, makes the simultaneous mining of clickstream data and VoIP communications permissible so long as it is done unintentionally.[328] By finding implied consent through the clickstream data exception, the courts are condoning the interception of both electronic data and oral VoIP communications that likely fall outside of end-users' authorized consent if the intercepting parties are acting unintentionally.[329] This creates the all-too-likely scenario wherein third-party interceptors who are pervasively deploying data tapping technology across the Internet Protocol network may be simultaneously tapping additional communications protected by the Wiretap Act as well as constitutionally protected communications in the case of governmental interceptions. This unauthorized tapping violates both the statutory intent and plain meaning interpretations of the Wiretap Act.[330]

The only viable judicial interpretation of the Wiretap Act in the twenty-first century is the statutory intent approach, which recognizes that the Act is ambiguous and that Congress intended to exempt clickstream data.[331] Congress can resolve the problem of conflicting judicial interpretations by creating an explicit clickstream data exception, with a corresponding decrease in the mens rea element from intent[332] to recklessness, for persons intercepting clickstream data. By lowering the mens rea element, Congress would be able to protect privacy expectations in VoIP and all other electronic communications while continuing to foster the development of the Internet economy.

Adopting this approach would enable companies relying upon the Internet to continue using clickstream data while simultaneously compelling these companies to utilize systems that prevent unauthorized interceptions of protected electronic communications, including VoIP.

---

326. *See* discussion *supra* Part II; *see also* 18 U.S.C. § 2511 (2004).

327. 18 U.S.C. § 2511(1)(a) (2004).

328. *See* discussion *supra* Part III.C.

329. 18 U.S.C. § 2511(1)(a) (2004).

330. The continued adoption of VoIP further exacerbates the problems caused by the clickstream data exception. VoIP uses some clickstream data when authenticating each party to the conversation. Thus, data mining companies will, under the current law, be able to intercept VoIP conversations without violating the Wiretap Act as long as they do so unintentionally while they are legitimately intercepting clickstream data under the Wiretap Act.

331. Although other technology exists beyond cookie-driven authentication, the Internet in its current state would not support these technologies. Furthermore, the billions of dollars that have been invested in cookie-based authentication would overnight vanish.

332. 18 U.S.C. § 2511(1)(a) (2004).

Companies using clickstream data would no longer face the uncertainty of acquiring adequate consent to satisfy the Wiretap Act, though they would be required to use systems that tap only clickstream data and not other electronic or oral VoIP communications. Under this innovative approach, lack of intent would no longer be a viable defense for companies engaging in unauthorized simultaneous interceptions of protected oral, wire, and electronic communications. The new law would require these companies to act responsibly given their privileged position, and to use technology designed to prevent the unauthorized interception of other protected communications.

By explicitly recognizing the clickstream data exception, Congress would resolve the problem of differing consent levels for indistinguishable electronic communications arising from the convergence of communication mediums. In so doing, Congress would close the current consent loophole[333] that allows companies mining consumers' personal information by way of clickstream data to simultaneously mine other protected communications, while maintaining the recognition of the legitimate applications of clickstream data in commerce.[334]

CONCLUSION

In both *DoubleClick*[335] and *Pharmatrak,*[336] the federal courts emphasized consent with respect to cookie-driven data mining technology, commonly referred to as clickstream data. In each case, the cookies were never fully written by the end-users of the website themselves,[337] but were generated by various algorithms and technologies to mine *personal information* from the end user's computer.[338] Since the end-users never input all of the written information transmitted by the cookie across a wire, the courts imputed consent by reasoning that end-users and their computers are the same entity.[339] This finding arguably contradicts both the higher expectation of

333. Courts allowed interception of personal information through cookie technology in four cases: *In re* Pharmatrak, Inc. Privacy Litig., 329 F.3d 9, 12 (1st Cir. 2003); *In re* Intuit Privacy Litig., 138 F. Supp. 2d 1272, 1274 (C.D. Cal. 2001); *In re* DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 502-03 (S.D.N.Y. 2001); Chance v. Avenue A, Inc., 165 F. Supp. 2d 1153, 1155 (W.D. Wash. 2001).

334. *See* discussion *supra* note 86.

335. *See In re DoubleClick*, 154 F. Supp. 2d at 503-04.

336. *See In re Pharmatrak*, 329 F.3d at 21.

337. *See* discussion *supra* Part III.C.

338. *See* discussion of data mining *supra* note 2.

339. *See* discussion *supra* Part III.C.

privacy afforded to oral communications by the Constitution[340] and the Wiretap Act's prohibition of unauthorized third-party interceptions of oral telephone and electronic communications.[341]

In order to ensure that oral communications utilizing VoIP technology will receive the same treatment and protection under the law as their non-VoIP oral communication counterparts enjoy, the courts and the legislature must act. They must either explicitly recognize the legislative privacy distinction between clickstream data and other oral, wire and electronic communications irrespective of the issue of consent as discussed in *Pharmatrak* and *DoubleClick*,[342] or the courts must halt all use of data mining technology and wait for Congress to deliver a legislative solution.[343] A Congressional amendment would provide courts a new legal framework in which to analyze VoIP claims brought under the Wiretap Act, enabling them to differentiate between data transmissions and other oral, data, and electronic transmissions. Without Congressional action and court application, VoIP technology remains at risk of unauthorized access and mining, which threatens the free communication of us all.

---

340. *See supra* text accompanying note 27; *compare* Katz v. United States, 389 U.S. 347, 353 (1967) (holding that electronically listening to telephone conversations constitutes a "search and seizure" within the meaning of the Fourth Amendment) *with* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis.").

341. *See supra* text accompanying note 52. *See also* 18 U.S.C. § 2511(1) (2004) ("Except as otherwise specifically provided in this chapter any person who – (a) Intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral or electronic communication . . . ."); Ferguson v. City of Charleston, 532 U.S. 67, 84 (2001) (describing body and home as "areas afforded the most stringent Fourth Amendment protection"); City of Indianapolis v. Edmond, 531 U.S. 32, 54 (2000) (Rehnquist, C.J., dissenting) (describing body and home as "areas afforded the most stringent Fourth Amendment protection"); Maryland v. Garrison, 480 U.S. 79, 90 (1987) (Blackmun, J., dissenting); Segura v. United States, 468 U.S. 796, 810 (1984) (stating that "the sanctity of the home is not to be disputed"); Welsh v. Wisconsin, 466 U.S. 740, 750, 754 (1984) (noting sanctity of the home); United States v. Turk, 526 F.2d 654, 658 (5th Cir. 1976) (holding a violation of the Act required that interception occur contemporaneously during transmission); *Katz*, 389 U.S. at 353 (use of electronic eavesdropping equipment overhear conversation inside telephone booth intrudes on legitimate expectation of privacy).

342. *See* discussion *supra* Part III.

343. *See* discussion *supra* Part VII.