NOTE

GOVERNMENT ACCESS TO TRANSACTIONAL INFORMATION AND THE LACK OF SUBSCRIBER NOTICE

Brian D. Kaiser[*]

TABLE OF CONTENTS

[*] J.D. *cum laude*, Boston University School of Law, 2002; B.A. *cum laude*, Chaminade University of Honolulu, 1997.

All ran headlong for their chains in the belief that they were securing their liberty; for although they had enough reason to see the advantages of political institutions, they did not have enough experience to foresee their dangers.[1]

I. INTRODUCTION

Today, more than ever, personal communications take place through computers.[2] These communications include not only e-mail messages, but also voice communications made via telephones.[3] Computers have also become the preferred means of storing information for both personal and business purposes.[4]

Law enforcement officials were well aware of this trend in computer-based communications in 1994 when they strongly lobbied Congress to modify the federal wiretapping laws to make government interception of computer-based communications easier.[5] The goal of both the Communications Assistance to Law Enforcement Act ("CALEA") of 1994[6] and its predecessor, the Electronic Communications Privacy Act ("ECPA") of 1986,[7] was to balance law

---

[1] JEAN-JACQUES ROUSSEAU, DISCOURSE ON THE ORIGIN OF INEQUALITY 68-69 (Franklin Philip Trans., Patrick Coleman ed., Oxford University Press 1994) (1755).

[2] *See* U.S. CONGRESS, OFFICE OF TECHNOLOGY ASSESSMENT, ELECTRONIC SURVEILLANCE IN A DIGITAL AGE 29-35 (1995) [hereinafter ELECTRONIC SURVEILLANCE].

> Since about the 1970s the technology of electronic switching, digital processing, computer architecture, and optical transmission have progressively developed into commercial devices and applications whose low costs and broad capabilities have made these technologies the foundation of a new era of communications. . . .[T]he nation's communication system is shifting from a wire-based analog system to digital computer-controlled switches.

Id. at 29. Digital packet switching is a system in which a communication is broken up into discrete packets of information each with a time code and destination address. *See id*. at 35. Each packet moves through the communications network via a different route depending on network traffic and then they are reassembled at the receiving end of the communication. *See id*. This is the method by which Internet communication takes place. *See id*. Because a large volume of traditional telephone communications is routed through similar switches, *see id*. at 29, law enforcement is faced with a technological challenge to maintaining its ability to wiretap. *See id*. at 35.

[3] *See id*. at 35.

[4] *See* S. REP NO. 99-541, at 3 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

[5] *See* ELECTRONIC SURVEILLANCE, *supra* note 2, at 29 ("By 1993 the proportion of digital switches had grown to 80 percent."). *See id.* at n.2 (citing testimony of A. Richard Metzger, Jr., Deputy Chief, Common Carrier Bureau, Federal Communications Commission, before the U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Telecommunications and Finance, Sept. 13, 1994, 103d Cong., 2d. sess.).

[6] Communications Assistance to Law Enforcement Act of 1994, 47 U.S.C. §1002 (2000).

[7] Electronic Communications Privacy Act of 1986, 18 U.S.C. §2511 (2000).

enforcement's interest in maintaining its ability to intercept communications and the privacy interests of the general public.[8]

The proliferation of computer use in transmitting communications is both a curse and a blessing from the perspective of law enforcement. While fast-advancing technology threatens to limit law enforcement's surveillance ability, it also opens the door to vast amounts of information never before available.[9] This Note will focus on one broad category of information known as "transactional information."

Transactional information is a term used to refer to information about a communication that is not itself part of the content of the communication.[10] Such transactional information includes the time of the communication, the parties to the communication, and the duration of the communication.[11] With respect to the Internet, transactional information is sometimes referred to as "click-stream" data or "mouse droppings."[12] On the Internet, click-stream data comprise a step-by-step record of the online locations one visits, the length of time one visits those locations, and what actions one takes.[13] Both individual Web sites and Internet Service Providers ("ISP's") monitor transactional information.[14] With respect to ISP's, and to a limited extent individual Web sites, the click-stream data can be combined with personal information volunteered by the user to create a "profile" of the user.[15]

---

[8] *See* H.R. REP. NO. 103-827, at 22 (1994); S. REP. NO. 99-541, at 5 (1986) ("The Committee believes that S. 2575, t[h]e Electronic Communications Privacy Act of 1986, represents a fair balance between the privacy expectations of American citizens and the legitimate needs of law enforcement agencies.").

[9] *See* ELECTRONIC SURVEILLANCE, *supra* note 2, at 1-2 (stating that law enforcement was losing its ability to wiretap effectively because of the rapid developments in communications technology).

[10] *See* Jerry Berman and Deirdre Mulligan, *The Internet and the Law: Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 549, 554 (1999); Lillian R. BeVier, *Symposium: The Communications Assistance for Law Enforcement Act of 1994: A Surprising Sequel to the Break up of AT&T*, 51 STAN. L. REV. 1049, 1054 (1999); Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. Cal. L. REV. 949, 953-55 (1996) (using the term "communication attributes" to refer to transactional information).

[11] *See* Freiwald, *supra* note 10, at 954-55. Freiwald also notes that the subject matter line of an e-mail could be considered transactional information though it is to an extent part of the content of the communication. *See id.* at 953.

[12] *See* Berman & Mulligan, *supra* note 10, at 554; Gavin Skok, *Establishing A Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. TECH. L. REV. 61, 64 (2000) (explaining that "clickstream" refers to the mouse clicks a user makes as they travel the Web).

[13] *See* Skok, *supra* note 12, at 64-65.

[14] *See* Freiwald, *supra* note 10, at 958; Skok, *supra* note 12, at 65-67; Joshua B. Sessler, Note, *Computer Cookie Control: Transaction Generated Information and Privacy Regulation on the Internet*, 5 J. L. & POL'Y 627, 632-34 (1996) (discussing how Web sites use "cookies" to track visitors and recognize them when they return to the site).

[15] *See* Freiwald, *supra* note 10, at 959 (offering as an example of misuse of transactional

The collection of such data by ISP's and other Web hosts is generally done without the consent of the user.[16] While some of the data collected is essential to the function of a computer network,[17] other forms of data collected primarily serve a marketing function.[18] Since the ISP's are the user's gateway to the Web, the transactional records they are able to compile are far more detailed than those of individual Web sites.[19] Unless a user offers some personally identifiable information to an individual Web site, only the ISP can connect the transactional data with the person.[20]

Some might think that transactional information would be of little value. Law enforcement entities, however, have found some creative ways to take advantage of transactional information.[21] During the investigation of President Clinton's relationship with Monica Lewinsky, Special Prosecutor Ken Starr sought to confirm the purchase of a specific book by Lewinsky.[22] Rather than trying to get a warrant based on probable cause to search her home, Starr simply delivered a subpoena to a local bookstore demanding records of Lewinsky's purchasing activity.[23] Thus, police access to information is enhanced not only through the use of computers but also because the legal requirements for access to electronic information are far less prohibitive than they are for voice communications.

In part, this Note seeks to determine the degree to which Congress has successfully balanced law enforcement and privacy interests with respect to transactional information. This Note argues that the scheme of protections afforded electronic data in the ECPA and the CALEA are reasonable in most respects. However, protections granted to transactional information are critically limited by the lack of an exclusionary clause or a notice requirement. This makes protections for transactional information effectively nonexistent. This Note argues that transactional information could be better protected by requiring notice to the target of the search either prior to or shortly after a

---

data a study in which researchers obtained the user names of visitors to a pornographic Web site simply by requesting the list from the bulletin board); Skok, *supra* note 12, at 67-68.

[16] *See* Skok, *supra* note 12, at 68.

[17] *See* Berman & Mulligan, *supra* note 10, at 554; Sessler, *supra* note 14, at 635-37.

[18] *See* Skok, *supra* note 12, at 65-67; Sessler, *supra* note 14, at 637-41.

[19] *See* Skok, *supra* note 12, at 67 (noting that an ISP is capable of gathering a larger amount of data about a single user that any given Web site could).

[20] *See id.*

[21] *See id.* at 68-70 (discussing ways police could use clickstream data).

[22] *See* Berman & Mulligan, *supra* note 10, at 570.

[23] *See id.* As a further example of the use of transactional information, Berman discusses an instance in which the Drug Enforcement Agency was reviewing purchasing data compiled through "frequent shopper" programs. *See* Berman & Mulligan, *supra* note 10, at 572. They were trying to identify shoppers who made large purchases of small plastic bags and baking powder, which are common items used in the drug trade. *See id.* (citing Robert O'Harrow, Jr., *Bargains at a Price Shoppers' Privacy, Cards Let Supermarkets Collect Data*, WASH. POST, Dec. 31, 1998, at A1).

search is conducted.[24]

Part I of this Note will discuss the development of wiretapping laws. Part II will discuss where transactional information fits into the scheme of wiretapping laws and whether it is adequately protected. Part III proposes that a notice requirement be added to the statutory section relating to transactional information in order to allow defendants to challenge such searches.

II. BACKGROUND: DEVELOPMENT OF WIRETAPPING LAW

A. Early Case Law: Bringing Wiretapping within the Scope of the Fourth Amendment

The constitutionality of wiretapping by law enforcement was first considered in *Olmstead v. United States*.[25] In *Olmstead*, the Court found no violation of the Fourth Amendment because there was neither a physical trespass to property nor a seizure of anything tangible.[26] Chief Justice Taft's majority opinion stated that while the Fourth Amendment did not limit wiretapping, Congress might do so through legislation.[27] Accordingly, Congress took notice and enacted the Federal Communications Act of 1934.[28] In 1937, the Supreme Court held that the Act precluded the admissibility of

---

[24] A recent article on transactional information argues that current protections for transactional information are too weak. *See* Skok, *supra* note 12, at 62. However, the premise of the Skok article is that courts should be encouraged to rethink doctrine and precedent in terms of what constitutes a Fourth Amendment search. *See id.* This Note argues that the better course for protecting transactional information is to encourage congressional action.

[25] *See* Michael Goldsmith, *Criminal Law: The Supreme Court and Title III: Rewriting the Law of Electronic Surveillance*, 74 J. CRIM. L. & CRIMINOLOGY 1, 7 (1983). *Olmstead v. United States*, 277 U.S. 438 (1928) involved an alleged conspiracy to violate the National Prohibition Act. *See id.* at 455. The government had conducted a five-month warrantless wiretapping operation involving eight telephones. *See id.* at 471.

[26] *See Olmstead*, 277 U.S. at 466. The taps were placed without trespassing on private property. *See id.* at 457. Additionally, what was taken was not tangible. *See id.* at 463-64. The court strictly construed the Fourth Amendment to require the thing seized to be something tangible and finds that the evidence was secured by the sense of hearing only. *See id.* at 464. In his dissent, Justice Brandeis questioned this analysis saying that a non-trespassory invasion was potentially more dangerous to liberty than a physical one. *See id.* at 474 (Brandeis, J., dissenting). Brandeis prophetically envisioned a time when papers might be reproduced in court without the need for entry upon private property. *See id.* He stated that if wiretapping was covered by the Fourth Amendment it must be barred and not merely restricted. *See id.*

[27] *See id.* at 465-66. Congress attempted to do just that but in the years shortly after the *Olmstead* decision nothing comprehensive was passed. *See also* Goldsmith, *supra* note 25, at 11.

[28] *See* 47 U.S.C. § 151 (2000); *see also* Goldsmith, *supra* note 25, at 12. *See also* BeVier, *supra* note 10, at 1065 ("[T]he Act's legislative history does not support the inference that Congress intended thereby to change the result in *Olmstead*.").

wiretap evidence in *Nardone v. United States*.[29] The Court broadly held that the statute prohibited wiretapping entirely.[30] At this stage in the development of the law the Court was unable to see past its literal interpretation of the Fourth Amendment to find that wiretapping was actually a search or a seizure. This interpretation would have had long lasting effects,[31] and it would be forty years before the Court would apply the Fourth Amendment directly to wiretapping and electronic surveillance in general.

In *Berger v. New York*,[32] the Court brought wiretapping and "bugging" within the ambit of the Fourth Amendment.[33] In that case, the police had applied for and received a warrant to "bug," or surreptitiously conduct electronic surveillance of, the defendant's offices.[34]

The Court found that the New York statute that had permitted search warrants for electronic surveillance was too broad.[35] While clearly stating that the Fourth Amendment applied to warrants for electronic surveillance,[36] the Court failed to expressly overrule *Olmstead* and the trespass-tangibles doctrine. The Court thus raised the question of whether the Fourth Amendment would have applied in this case had the police accomplished the surveillance without trespassing on the defendant's property to plant the bug.[37] Some contend that the *Berger* majority's real purpose was to strike down the New York statute as an undesirable statutory model for other states and the federal government, while stopping short of holding eavesdropping to be per se

---

[29] *See* 302 U.S. 379, 382 (1937).

[30] *See id*. at 381-82. *Nardone* was the Court's opportunity to put a stop to wiretapping by way of a statutory interpretation rather than application of the Fourth Amendment. *Nardone*'s holding meant that while wiretapping was still constitutionally protected, and therefore could be practiced, any evidence gathered from a wiretap was inadmissible in federal court. *See id*. at 382; BeVier, *supra* note 10, at 1065-66 (stating that the result of *Nardone* was that wiretapping could still be conducted constitutionally, it just could not be used in federal courts as evidence). This holding was subsequently narrowed by later decisions, and the switch between *Olmstead* and *Nardone* did very little to provide consistency in wiretapping law. *See* Goldsmith, *supra* note 25, at 13.

[31] *See* Ira Glasser, *The Internet and the Law: The Struggle for a New Paradigm: Protecting Free Speech and Privacy in the Virtual World of Cyberspace*, 23 NOVA L. REV. 625, 637-41 (1999) (comparing effect of introduction of printing press on First Amendment law to introduction of telephone on Fourth Amendment law and finding that failure of courts to recognize that the telephone had fundamentally changed communications and look to the basis of the Fourth Amendment rather than strictly interpreting it resulted in erosion of privacy protection).

[32] 388 U.S. 41, 51 (1967).

[33] *See* Goldsmith, *supra* note 25, at 21.

[34] *See* Berger v. New York, 388 U.S. at 44-45; *see also* Goldsmith, *supra* note 25, at 22.

[35] *See Berger*, 388 U.S. at 44.

[36] *See Berger*, 388 U.S. at 53 (quoting *Mapp v. Ohio*, 367 U.S. 643, 655 (1961) which states that "the Fourth Amendment's right of privacy has been declared enforceable against the States through the Due Process Clause of the Fourteenth Amendment").

[37] *See Berger*, 388 U.S. at 63-64; *see also* Goldsmith, *supra* note 25, at 24.

illegal.[38]

A few months after the *Berger* decision the Court put to rest any remaining concerns about the application of the Fourth Amendment to electronic surveillance with its decision in *Katz v. United States*.[39] In *Katz*, unlike in *Berger*, the electronic surveillance at issue took place without any trespass.[40] Police had attached an electronic surveillance device to the top of a phone booth the defendant was known to use.[41] The defendant argued that a public phone booth was a "constitutionally protected area" and that use of the listening device had violated his right of privacy.[42] In response, the Court stated that "the Fourth Amendment protects people, not places."[43] The Court explained that the proper question was whether the defendant had intended his telephone conversation to be private, regardless of where that conversation had taken place.[44]

In *Katz*, the government first contended the search was valid under *Olmstead* because there was no physical trespass involved.[45] Since *Katz*, however, physical trespass is no longer a requirement to bring an electronic search under Fourth Amendment protection.[46] The Court did not hold electronic surveillance unconstitutional. Instead, the Court indicated that electronic surveillance is constitutionally permissible provided a proper

---

[38] *See* Goldsmith, *supra* note 25, at 26. The court cites *Osborn v. United States*, 385 U.S. 323 (1966) as an example of a valid eavesdropping warrant, indicating that a valid warrant for electronic surveillance could be issued. *See Berger*, 388 U.S. at 56-57.

[39] Katz v. U.S., 389 U.S. 347 (1967).

[40] *See id*. at 348.

[41] *See id*.

[42] *See id*. at 349.

[43] *Id*. at 351.

[44] *See id.* at 351-52. Justice Harlan's concurrence used the key phrase "reasonable expectation of privacy" with reference to the majority's definition of when the Fourth Amendment applied. *See id.* at 360 (Harlan, J., concurring). As the Court's opinion stated,

> the Fourth Amendment protects people, not places. The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a "place." My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person has exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'

Id. at 361. *See also* 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1 (3d ed. 1996) (discussing the *Katz* expectation of privacy test).

[45] *See* LAFAVE, *supra* note 44, at 383.

[46] *See id*. at 383-84. ("[A]lthough a closely divided Court supposed in *Olmstead* that surveillance without any trespass and without the seizure of any material object fell outside the ambit of the Constitution, we have since departed from the narrow view on which that decision rested . . . We conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling.") *Id*. at 383.

warrant is obtained prior to such surveillance.[47]

The progression of the case law between *Olmstead* and *Katz* is important for two reasons. First, it points out the difficulty the Court has encountered in stepping away from its initial strict interpretation of the Fourth Amendment. Some commentators have argued that early decisions by the Court with respect to privacy have had lingering effects.[48] This is important to keep in mind when looking at how the Court has treated searches of computers in the upcoming section. Second, it demonstrates the Court's matter-of-fact acceptance of the notion that electronic surveillance is something law enforcement entities should be doing in the first instance. When the *Katz* Court overruled *Olmstead*, one might have expected the *Katz* Court to give some consideration to whether electronic surveillance is constitutional as a threshold issue.[49] Instead, the Court proceeded straight to the notion that wiretapping can be conducted within the requirements of the Fourth Amendment.[50] One commentator argues this is *Olmstead's* lasting impact.[51] *Katz* clearly indicated the Court's desire to maintain wiretapping as a law enforcement tool, and placed the ball squarely in Congress's court to devise a statutory scheme that outlined the proper Fourth Amendment protections for wiretapping and eavesdropping.[52] Within seven months of *Katz*, Congress did just that with the passage of Title III.[53]

B. Passage of Title III: The Basis of the Modern Wiretapping Statutory Scheme.

In formulating Title III, Congress paid special attention to the Berger and Katz decisions, citing them 16 times in the statute's legislative history.54 The framework of Title III was designed to regulate non-consensual55 electronic surveillance.56 Title III incorporates both criminal penalties and civil

---

[47] *See id*. at 384-85.

[48] *See* Glasser, *supra* note 31, at 641, 644 (comparing slow progress of First Amendment free speech protections historically to progression of Fourth Amendment rights).

[49] *See* 277 U.S. at 474 (Brandeis, J., dissenting) (arguing that if wiretapping was a search within the meaning of the Fourth Amendment then it must be banned).

[50] *See* Goldsmith, *supra* note 25, at 31.

[51] *See* Glasser, *supra* note 31, at 644.

[52] *See* Goldsmith, *supra* note 25, at 32.

[53] *See* Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510-2520 (2000)). Note that *Katz* was decided on December 18, 1967. *See* 387 U.S. at 347. Title III was passed on June 19, 1968. *See* Pub. L. No. 90-351, 82 Stat. 197 (1968).

[54] *See* Goldsmith, *supra* note 25, at 38.

[55] *See id*. at 39. Non-consensual refers to situations in which neither party consents. *See id*. at 39 n.226. But if just one party does consent the surveillance does not fall under Title III. *See id*.

[56] Consensual surveillance is far more common than non-consensual surveillance. *See* Goldsmith, *supra* note 25, at 46. Generally, the consenting party is an officer or cooperating

remedies against anyone who intentionally intercepts, uses, or discloses information in violation of the statute.[57] It also provides an exclusionary rule for disclosure of evidence that is obtained in violation of the statute.[58] This combination of factors serves both to limit the use of electronic surveillance and encourage authorized users to do so in compliance with the statute.[59]

Title III outlines a detailed set of requirements to obtain a search warrant for electronic surveillance.[60] One commentator has broken down the requirements into three categories: jurisdictional, documentary, and executional.[61] To obtain a valid eavesdropping order, (1) "the order's application must be for surveillance pertaining to a crime designated by the statute;"[62] (2) "it must initially have been authorized by a designated executive official;"[63] and (3) "it must be filed before a judge of competent jurisdiction."[64] These requirements control the use of electronic surveillance both by limiting the crimes to which it can be applied, and by requiring approval for its use from a high-level official.[65]

Title III also contains documentary requirements. Specifically, each eavesdropping application must be made in writing and under oath.[66] The application must provide a "full and complete" statement showing probable

---

citizen. *See id*. Recall that *Osborn* was a case in which a prior warrant was obtained for a consensual monitoring situation. *See Osborn* 385 U.S. at 327. Despite the fact that *Berger* and *Katz* had pointed to *Osborn* as a model case, there was no reason to think that *Berger* or *Katz* had overruled the essential holding in *Lopez v. United States*, 373 U.S. 427 (1963) that one assumes the risk of disclosure by entering into a conversation, and has no right to rely on the possible flaws of the agent's memory of the conversation. *See* Goldsmith, *supra* note 25, at 47. In 1971, the Supreme Court held that consensual monitoring was not covered by the Fourth Amendment. *See* United States v. White, 401 U.S. 745, 752-54 (1971).

[57] *See* 18 U.S.C. §§ 2511(1)(a), 2520.

[58] *See id.* § 2515.

[59] *See* Goldsmith, *supra* note 25, at 39-40.

[60] *See* 18 U.S.C. §§ 2510 – 2520.

[61] *See* Goldsmith, *supra* note 25, at 41.

[62] *Id*.; 18 U.S.C. § 2516(1). Note that according to § 2516(3), in the case of electronic communications interception, the request may be based on any federal felony and not just those set forth in § 2516(1). *See* 18 U.S.C. § 2516(3); *see also* ELECTRONIC SURVEILLANCE MANUAL: VOLUME I - PROCEDURES AND FORMS, U.S. Department of Justice, Criminal Division - Office of Enforcement Operations 6 (1991) [hereinafter ELECTRONIC SURVEILLANCE MANUAL].

[63] Goldsmith, *supra* note 25, at 41; *see also* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 5. "The application must be in writing and signed by the United States Attorney, (or an Assistant United States Attorney) and made under oath." *Id*. at 5.

[64] Goldsmith, supra note 25, at 41; *see also* 18 U.S.C. §§ 2510(9)(a), 2518(1).

[65] *See* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 5 (stating that the application must identify the type of communication to be intercepted); Goldsmith, *supra* note 25, at 41.

[66] *See* 18 U.S.C. § 2518(1); ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 5.

cause regarding the person to be monitored,[67] and detailing the crime alleged,[68] the conversation sought to be monitored,[69] the location of the monitoring,[70] and the time frame during which the monitoring is to take place.[71] These requirements are thought to eliminate the possibility of indiscriminate monitoring since the application must not only specify the target of the surveillance, but, additionally, must describe the kind of conversation sought and the offenses to which it relates.[72] In addition, the application must contain a "full and complete" statement showing that the applicant has exhausted alternative investigative techniques, and must provide details of any prior surveillance of the target by the current applicant.[73]

Even if all of the above requirements are met, the judge still has discretion as to whether to grant the requested surveillance order.[74] If and when surveillance begins, only properly authorized personnel are permitted to participate[75] and surveillance must be done in a way that minimizes the interception of conversations not covered by the warrant.[76] Where possible, all monitored conversations should be taped.[77] Then, immediately after the

---

[67] *See* § 2518(1)(b); ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 6.

[68] *See* 18 U.S.C. § 2518(1)(b)(i); ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 6.

[69] *See* 18 U.S.C. § 2518(1)(b)(iii); ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 6.

[70] *See* 18 U.S.C. § 2518(1)(b)(ii); ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 6.

[71] *See* 18 U.S.C. § 2518(1)(d); ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 8.

[72] *See* Goldsmith, *supra* note 25, at 52 (citing 18 U.S.C. § 2518(1)(b)(i), (1)(b)(iv), 4(a), 4(c)).

[73] *See* 18 U.S.C. § 2518(1)(c), (e); ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 7.

[74] *See* 18 U.S.C. § 2518(3) (stating that the "judge *may* enter an ex parte order . . . authorizing or approving interception of wire, oral, or electronic communications . . . .") (emphasis added).

[75] *See* 18 U.S.C. §§ 2510(7), 2518(1)(a), 2518(4)(d); ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 8.

> If a state or local law enforcement officer is the affiant in a federal electronic surveillance affidavit, he must be deputized as a federal officer. Section 2518(5) permits non-officer government personnel or individuals acting under contract with the government to monitor conversations pursuant to the interception order. These individuals must be acting under the supervision of an investigative or law enforcement officer when monitoring communications . . . .

Id.

[76] *See* 18 U.S.C. § 2518(5); ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 8.

[77] *See* 18 U.S.C. § 2518(8)(a); ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 14 ("The statute permits after-the-fact minimization for wire and oral communications where the intercepted communications are in code, or in a foreign language when a foreign language expert is not reasonably available. After-the-fact minimization is a necessity for the interception of electronic communications over a digital display pager or an electronic

surveillance is ended, the tapes must be turned over to the authorizing judge and sealed.[78] The statute requires a post-interception notice to all persons named in the order, but leaves to the discretion of the judge notice to secondary parties who were overheard.[79] Title III also contains a broad suppression penalty for failure to comply with its statutory requirements.[80] Seemingly, the intent of the statute's exclusionary clause is to strongly encourage police to conduct surveillance in conformity with the statute or face suppression of the evidence gathered.[81]

C. Supreme Court Interpretation of Title III: Moving from Protecting Privacy to Protecting an Investigative Technique.

While the Supreme Court periodically stated that the government had to strictly enforce Title III, its decisions did not conform with these proclamations.[82] Title III's exclusionary clause is one of its key privacy protection features.[83] Congressional sponsors intended the clause to encourage law enforcement's compliance with the statute, but early Supreme Court decisions blunted its seemingly broad mandate.[84]

In *United States v. Chavez*,[85] the Court refused to suppress wiretap evidence when it was shown that the government failed to comply section 2516(1)'s requirement that the Attorney General or designated assistant approve the eavesdropping application.[86] The Court refused suppression because, while the misrepresentation of the authorizing official did violate the statute, the Court did not consider the authorization requirement "central" to the statutory scheme.[87] This interpretation of the statute let the Court itself determine when a violation of the statute was important enough to warrant suppression.[88] The

---

facsimile machine. In such cases, all communications are recorded and then examined by a monitoring agent and/or supervising attorney to determine their relevance to the investigation.").

[78] *See* 18 U.S.C. § 2518(8)(a).

[79] *See id.* § 2518(8)(d).

[80] *See id.* § 2515.

[81] *See infra* notes 85-88 and accompanying text (noting that the "centrality" doctrine has limited the effectiveness of the exclusionary clause).

[82] *See* Goldsmith, *supra* note 25, at 56. *See also* BeVier, *supra* note 10, at 1068 ("In practice, Title III has perhaps been implemented in neither as constrained nor as significant a crime-fighting way as its literal terms would suggest.").

[83] *See* 18 U.S.C. § 2515.

[84] *See* Goldsmith, *supra* note 25, at 40, 44 (describing the exclusionary rule of Title III as broad) (stating that congressional sponsors of Title III repeatedly stated the statute was meant to be strictly enforced).

[85] 416 U.S. 562 (1973).

[86] *See* U.S. v. Chavez, 416 U.S. at 579; *see also* 18 U.S.C. § 2516(1).

[87] *See* 416 U.S. at 579. The dissent argued that the exclusionary rule in section 2515 of the statute was unqualified and any violation warranted suppression. *See id.* at 584-85 (Douglas, J., dissenting).

[88] *See* Goldsmith, *supra* note 25, at 79-80 (explaining that the *Chavez* centrality doctrine

Chavez decision is an example of the Court's willingness to bend Title III to preserve the government's ability to conduct electronic surveillance.[89] While Congress gave the Court what it asked for in *Katz*, the Court nonetheless was unwilling to strictly apply the Fourth Amendment requirements to electronic surveillance.[90] *Chavez* involved wire communications, which are clearly constitutionally protected, and the Court's refusal to apply Title III's exclusionary rule does not bode well for communications that are not constitutionally protected.

D. Electronic Communications Privacy Act of 1986 ("ECPA").

As communications methods changed, Congress attempted to keep wiretapping law current with the passage of the Electronic Communications Privacy Act.[91] The ECPA purported to extend Title III coverage to electronic communications,[92] that is, not just to voice or face-to-face communications to which Title III was previously limited.[93] In reality, however, the ECPA excluded electronic communications from some of the key protections that Title III grants to voice and face-to-face communications.[94]

Specifically, under Title III, a wiretap was only an option if law enforcement officials were investigating one of a few enumerated felonies.[95] After the ECPA, however, police could obtain a warrant to tap electronic communications pursuant to the investigation of any federal felony.[96] In

---

was understood to mean that if the specifics of Title III were somehow violated by police the court would determine if the violation involved a "central" facet of the statute and, if it is not, then suppression was not required).

[89] For a discussion of other post-Title III decisions that limit the privacy protection aspects of Title III, see generally Goldsmith, *supra* note 25, at 56-119.

[90] *See id.*

[91] *See* S. REP. NO. 99-541, at 1 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555, 3555 ("The bill amends the 1968 law to update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies.").

[92] An electronic communication is defined as:

> [A]ny transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include—
>
> (A) any wire or oral communication;
>
> (B) any communication made through a tone-only paging device;
>
> (C) any communication from a tracking device (as defined in section 3117 of this title); or
>
> (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

18 U.S.C. § 2510(12) (2000).

[93] See James X. Dempsey, Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy, 8 ALB. L. J. SCI. & TECH. 65, 73 (1997).

[94] See id.

[95] See 18 U.S.C. § 2516(1)(a).

[96] See id. § 2516(3).

addition, the ECPA contains no exclusionary rule that applies to the interception of non-voice communications.[97] Thus, if police gather e-mails based on a flawed warrant, the EPCA does not require the Court to suppress such evidence.[98]

i. Requirements for Access to Stored Data

The ECPA created a new warrant standard for access to stored electronic data.[99] This section made two important distinctions. The first is between storage of communications with a "provider of electronic communication service"[100] and storage of communications with a "remote computing service."[101] If a communication is stored with a communications service provider, access requirements are dependent on how long the communication has been stored. [102] If a communication is stored with a remote computing service, on the other hand, the time stored has no affect on the access requirements.[103]

The basis of this first distinction derives from the Supreme Court's decision in *United States v. Miller*,[104] which held that a bank customer had no expectation of privacy in the records of his banking transactions because he had voluntarily conveyed those records to the bank.[105] Thus, sending e-mail through a service provider assumes a risk of disclosure.[106] In his dissent, Justice Brennan took issue with this assumption of risk application, arguing that "[f]or all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is

---

[97] See id. § 2515.

[98] See id.

[99] See id. § 2703.

[100] *See id.* § 2703(a). Electronic communication service is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." *Id.* § 2510(15).

[101] *See id.* § 2703(b). Remote computing service is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." *Id.* § 2711(2). Electronic communications system is defined as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." *Id.* § 2510(14).

[102] *See id.* § 2703(a) (stating that access requirements are different depending on whether the communication has been in storage more or less than 180 days); CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING AND EAVESDROPPING § 26:9 (2d ed. 1995) (explaining that when an e-mail stays on a server longer than 180 days Congress felt that the service provider was less like a Post Office and more like a remote storage facility).

[103] *See* 18 U.S.C. § 2703(b).

[104] 425 U.S. 435 (1976).

[105] *See id.* at 442.

[106] *See* United States v. White, 401 U.S. 745, 751-52 (1971) (finding that one of the risks involved in disclosure of information to third parties is the risk that that person will give it to the government).

impossible to participate in the economic life of contemporary society without maintaining a bank account."[107] This practical understanding of the reality of commerce would seem equally applicable to the necessity of communicating through the use of a telephone in the 1970s (when *Miller* was decided) and to the necessity of communicating through an on-line computer in the near future.[108]

The second important distinction outlined by the ECPA is the 180-day cut off regarding access to communications stored with an electronic communications service.[109] The government can only access a communication that has been in storage for less than 180 days with a probable cause warrant.[110] The government can access a communication stored with an electronic communications service that is more than 180 days old in the same way the government could access any communication stored with a remote computing service.[111] The rationale for the 180-day distinction is understandable if one considers why Congress made the distinction between an electronic communications service and a remote computing service.[112] Clearly, when a communication is in storage for more than six months the electronic storage begins to look more like a remote computing service and less like a communications service.

ii. Requirements for a Pen-Register Search Warrant

The ECPA also created the pen-register warrant.[113] A pen-register is "a device which records or decodes electronic impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which the device is attached."[114] Prior to these statutory requirements courts granted

---

[107] *Miller*, 425 U.S. at 451 (Brennan, J., dissenting).

[108] Frustration with the traditional expectation of privacy doctrine has led some courts to consider the party's "expectation of noninterception" rather than simply expectation of privacy. *See* Walker v. Darby, 911 F.2d 1573, 1579 (11th Cir. 1990). On this theory, one may expect that a telephone conversation could be overheard by a person in the room, but may have a reasonable expectation that it will not be recorded by others. *See id.*

[109] *See* 18 U.S.C. § 2703(a) (2000).

[110] *See id.* § 2703(a); FISHMAN & MCKENNA, *supra* note 102, § 26:9 (analogizing an e-mail to a postal letter and saying police would need a warrant to search mail still in the possession of the Post Office).

[111] *See* 18 U.S.C. § 2703(a), (b). Under section 2703(b)(1)(B) the government entity has two access options. One is an administrative, grand jury or trial subpoena. *See id.* § 2703(b)(1)(B)(i). The other is a court order outlined in section 2703(d). *See id.* § 2703(b)(1)(B)(ii). Notice that no matter which option is chosen, prior notice to the subscriber or customer is required. *See id.* § 2703(b)(1)(B); *see also* FISHMAN & MCKENNA, *supra* note 102, § 26:9 (stating that Congress likely compared the communications service provider to a Post Office, whereas they saw a remote computing service as more like third-party file storage).

[112] *See* FISHMAN & MCKENNA, *supra* note 102, § 26:9.

[113] *See* 18 U.S.C. §§ 3121-3127.

[114] *Id.* § 3127(3).

pen-register warrants under their general warrant powers.[115] The ECPA creates a set of minimal requirements for issuing a pen-register warrant.[116] The statute requires the application for a warrant to state that "the information likely to be obtained is relevant to an ongoing criminal investigation."[117] The order issued by the court must specify the identity of the telephone owner,[118] the person who is the subject of the investigation,[119] the physical location of the phone,[120] and the offense to which the information likely to be obtained relates.[121] Most importantly, the ECPA does not require disclosure of the fact that a pen-register was installed.[122]

The creation of a warrant requirement for pen-registers is thought by many to have been a congressional response to the Supreme Court's holding in *Smith v. Maryland.* [123] In *Smith*, the Court held that pen-registers are not subject to Fourth Amendment protection because there is no expectation of privacy in the numbers dialed on their telephone.[124] Therefore, none of the constitutional requirements for a Title III warrant are applicable to pen-registers.[125]

---

[115] *See* Michael A. Rosow, Note, *Is "Big Brother" Listening? A Critical Analysis of New Rules Permitting Law Enforcement Agencies To Use Dialed Digit Extraction*, 84 MINN. L. REV. 1051, 1057 (2000) (citing *United States v. New York Tel. Co.*, 434 U.S. 159, 168-69 (1977)).

[116] *See* ELECTRONIC SURVEILLANCE MANUAL, *supra* note 62, at 33-34 (discussing the basic requirements for a pen- register warrant).

[117] *See* 18 U.S.C. § 3122(b)(2).

[118] *See id.* §3123(b)(1)(A).

[119] *See id.* §3123(b)(1)(B).

[120] *See id.* §3123(b)(1)(C).

[121] *See id.* §3123(b)(1)(D).

[122] *See id.* §3123(d)(1).

[123] 442 U.S. 735 (1979). *See, e.g.*, Freiwald, *supra* note 10, at 971-72. *See also* Steven P. Oates, *Caller ID: Privacy Protector or Privacy Invader?* 1992 U. ILL. L. REV. 219, 222 (1992).

[124] *See* Smith, 442 U.S. at 740-44 (1979).

[125] Note that under 18 U.S.C. § 2703(c)(1)(C) telephone billing records are available to investigators who present an administrative, grand jury or trial subpoena. Some have argued this represents a confluence of pen registers and transactional information. *See* Freiwald, *supra* note 10, at 995. However, these sorts of records are historical in nature and would be of limited use in an ongoing investigation. Freiwald argues that because newer computer-based pen registers are capable of gathering more information than older mechanical versions, law enforcement may in the future seek the sort of transactional information covered by 18 U.S.C § 2703(c) by way of the lower warrant standard for a pen register under 18 U.S.C. §3122. *See id*. at 988-89. While this is a possibility, the statute and Congress have expressly limited pen register devices to accessing phone numbers and their use to acquire, say, Internet transactions would not likely be allowed by a judge issuing a pen register warrant. The fact that newer pen registers allow acquisition of the time of a phone call and whether a connection was actually made is of little concern. *See id*. at 982-84. Given that police could collect such information from the phone company and then simply cross reference it with the information gathered by the pen register, police are not getting more information, they are simply getting information that was always available

iii. Introduction of Transactional Information

The ECPA is also important because it introduced the concept of transactional data.[126] The ECPA's requirements for access to transactional information were superseded by the passage of CALEA. With respect to transactional data, the ECPA required an administrative, trial or grand jury subpoena.[127] While this requirement constitutes very weak protection, it is doubtful anyone in 1986 would have predicted the explosion of transactional information that actually took place.[128] The rapid development of the Internet mirrored the rapid pace of development in the telecommunications industry as a whole, and eight years after the ECPA was enacted, Congress was attempting once again to revise the electronic surveillance statutes.

E. Communications Assistance to Law Enforcement Act of 1994 ("CALEA").

CALEA represents congressional recognition of wiretapping as an important government investigative tool and seeks to preserve it.[129] In lobbying for CALEA's passage, law enforcement advocates claimed their aim was not to expand wiretapping but merely to keep pace with changing technology.[130] Some argue the result is an expansion of the government's ability to wiretap.[131] Much of the Act deals with requirements placed on the communications industry to develop their equipment in a way that allows the government to easily tap into it.[132] For purposes of this Note, the most significant aspect of CALEA is in the changes it makes to the warrant requirements applicable to transactional information.

In CALEA Congress recognized for the first time that transactional information constituted more than just a name and address.[133] Rather,

---

more quickly.

[126] *See* 18 U.S.C. § 2703; S. REP. NO. 99-541 at 3 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 ("Title II of S. 2575 addresses access to stored wire and electronic communications and transactional records.").

[127] *See* S. REP. NO. 99-541 at 38-39 (1986) *reprinted in* 1986 U.S.C.C.A.N. 3555, 3592-93 (detailing the various means by which a governmental entity can access "information pertaining to a customer or subscriber").

[128] It is interesting to note that in 1986 the concept of transactional information was limited to "subscriber information." *See id.* at 38 *reprinted in* 1986 U.S.C.C.A.N. at 3592.

[129] *See* H.R. REP. NO. 103-827, at 22 (1994) *reprinted in* 1994 U.S.C.C.A.N. 3489, 3489-50.

[130] *See Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: Joint Hearings on H.R. 4922 and S. 2375 Before the Subcomm. On Civil and Constitutional Rights of the House Comm. on the Judiciary*, 103d Cong. 112-13 (1994) (testimony of Louis J. Freeh, FBI Director).

[131] *See id.* at 53, 70 (statement of Roy Neel, President, U.S. Telephone Association) (statement of Jerry Berman, Executive Director, Electronic Frontier Foundation).

[132] *See generally* H.R. REP. NO. 103-827 (1994) *reprinted in* 1994 U.S.C.C.A.N. 3489.

[133] *See id.* at 31-32 (1994) *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511-12.

H.R. 4922 includes provisions, which FBI Director Freeh supported in his testimony,

transactional information was a "hybrid" form of information falling somewhere between the traditional content-based communications that required a probable cause warrant and the non-content based communications that fell under the pen register statute.[134] Congress claimed that the new warrant standard for transactional information reflected this middle ground by requiring something more than a pen register warrant and something less than probable cause.[135] The legislative history of CALEA points out that transactional information has the ability to reveal much more about the user than a simple phone number.[136]

The statute distinguished between two types of information that may be disclosed under this section. Information like name, address, telephone number or other subscriber numbers or identities may be disclosed on the basis of an administrative subpoena, grand jury, or trial subpoena.[137] However, requirements are more stringent if the government seeks more than just a subscriber's demographic information.[138] Section 2703 offers three ways the government may access this information, only one of which requires notice to the subscriber.[139] Under Section 2703, the government may obtain the information sought through a probable cause warrant,[140] a court order as specified in subsection (d),[141] or consent of the subscriber.[142] The court order discussed in subsection (d) requires that the government offer "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or other information sought, are relevant to an ongoing criminal investigation."[143]

Some contend that the rationale for this lower standard is that transactional information is thought to reveal no more than police could discover through

---

that add protections to the exercise of the government's current surveillance authority. Specifically, the bill eliminates the use of subpoenas to obtain e-mail addresses and other similar transactional data from electronic communications service providers. Currently, the government can obtain transactional logs containing a person's entire on-line profile merely upon presentation of an administrative subpoena issued by an investigator without any judicial intervention. Under H.R. 4922, a court order would be required.

See id.

[134] See id.

[135] See id.

[136] See id.

[137] See 18 U.S.C. § 2703(c)(1)(C) (2000); FISHMAN & MCKENNA, supra note 102, § 26:16 (noting that prior to the passage of CALEA transactional logs were also available on the basis of a subpoena alone).

[138] See 18 U.S.C. § 2703(c)(1)(A).

[139] See id. § 2703(c)(2).

[140] See id. §2703(c)(1)(B)(i).

[141] See id. § 2703(c)(1)(B)(ii).

[142] See id. § 2703(c)(1)(B)(iii).

[143] See id. § 2703(d). For a discussion of what "specific and articulable facts" means in practice, see infra Part II.A.1.

use of a pen register. Thus, the requirements for access under Section 2703 are similar to those for issuing pen register warrants.[144] It is clear from the legislative history, however, that in Section 2703, Congress sought to define a warrant standard somewhere between that of probable cause and the basic investigatory subpoena, implying a standard higher than that required for a pen register warrant.[145]

PART III. ANALYSIS: TRANSACTIONAL INFORMATION IN THE STATUTORY SCHEME

The protection given to each type of communication is part of a larger statutory scheme. Stepping back and viewing the statutory scheme as a whole is helpful in determining not only the relative value Congress places on each type of communication, but also how Congress articulates that judgment in terms of the privacy-protective features granted to each type of communication.

A. Hierarchy of Protection

Voice communication is the first of five categories of protection distinguished in the statutory scheme of Title III. It gets the maximum protection available under the wiretapping laws.[146] Law enforcement must show probable cause to get the warrant, and it is subject to stringent requirements in the execution of that warrant.[147] Among the key protections afforded by Title III is the exclusionary clause.[148] While some sort of warrant is required to access other forms of communication, none of those other warrants is subject to suppression for failure to comply with Title III. Another key privacy protection feature is the requirement that once the surveillance is completed, the target of the surveillance must be notified.[149]

The second category of protection applies to information stored for less than 180 days with an electronic communications service provider.[150] A probable cause warrant is required to access information in this category.[151] Under section 2703(a), however, there is neither an exclusionary clause nor a notice

---

[144] See FISHMAN & MCKENNA, supra note 102, § 26:16.

[145] *See* H.R. REP. NO. 103-827, at 31-32 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511-12 ("Recognizing that transactional records from on-line communication systems reveal more than telephone toll records or mail covers . . .").

[146] *See* Freiwald, *supra* note 10, 968-69 (characterizing Title III protection as "strong").

[147] *See generally* 18 U.S.C. §§ 2515-2519; *see generally* Goldsmith, *supra* note 25, at 39-56 (discussing in detail the various requirements for a Title III search warrant).

[148] *See* 18 U.S.C. § 2515; *see generally* Goldsmith, *supra* note 25, at 39-40, 44-45 (discussing purpose and scope of exclusionary clause).

[149] *See* 18 U.S.C. § 2518(8)(d) (stating that notification is required within 90 days of completion of surveillance or denial of application for surveillance, but judge has discretion to postpone notification).

[150] *See id.* § 2703(a).

[151] *See id.*

requirement. Thus, one seeking to access information in this category (stored for less than 180 days with an electronic communications service provider) must make a strong showing, but once access has been granted, the customer receives little protection in that any evidence gathered cannot be excluded.

The third category of protection applies to both communications stored with an electronic communications service provider for more than 180 days and any communication stored with a remote computing service.[152] Investigators have three options for access under this section,[153] the simplest of which is the subpoena.[154] It is important to note that when a probable cause warrant is sought, no notice to the subscriber is required. If, however, investigators seek only a subpoena or court order, they must give prior notice to the subscriber.[155] For this category of information, then, the notice requirement appears to be a protective measure when access is sought based on something less than probable cause, as notice given pursuant to the requirement allows the target of the search to challenge the subpoena or court order.[156]

The fourth category of protection covers transactional information.[157] Under section 2703(c), notice is not required no matter what method is chosen by investigators.[158] The entity conducting the surveillance need not give notice to the target before or after it completes that surveillance.[159] This section of the statute, however, provides two of the same options for accessing the applicable information that are also available in the third category under section 2703(a) above.[160] Thus, the lack of the notice requirement is what most distinguishes this fourth category (transactional information) from the others.

The lowest category of protection applies to pen registers.[161] An applicant for a pen register warrant need only show that "the information likely to be obtained is relevant to an ongoing criminal investigation . . ."[162] Further, there is no notice requirement for those seeking pen register warrants.

---

[152] *See id.* § 2703(a), (b).

[153] *See id.* § 2703(b).

[154] *Id.* § 2703(b)(1)(B)(i); *see also* FISHMAN & MCKENNA, *supra* note 102, § 26:11 (explaining that a subpoena requires no factual showing but that the disadvantage of this method is the requirement of notice to the subscriber).

[155] *See* 18 U.S.C. § 2703(b)(1)(A), (B). However, the government may ask to delay notification. *See id.* § 2705(a).

[156] *See* 18 U.S.C. § 2704(b); *see also* FISHMAN & MCKENNA, *supra* note 102, §§ 26:11, 26:15 (explaining that under § 2705 government may ask that notice be postponed or under § 2704 they can have backup copies of the information made before notice to the subscriber is served).

[157] *See* 18 U.S.C. § 2703(c).

[158] *See id.* § 2703(c)(2).

[159] *Compare* 18 U.S.C. § 2703(b)(1) *with* 18 U.S.C. § 2703(c)(1)(B).

[160] *See id.* § 2703(c)(1)(B). Under this section, government can gain access with the consent of the subscriber as well as by warrant or court order. Additionally, if demographic information is all that is sought, a subpoena will suffice. *See id.* § 2703(c)(1)(C).

[161] *See id.* § 3122.

[162] *Id.* § 3122(b)(2).

i. The Logic of the Hierarchy

There are three distinguishing features among these five categories. The first is the relative burden investigators bear in gaining access to the information. The second is whether investigators must give notice to the target of the search. The third, which is really a function of the second, is the ability of the target of the search to suppress the evidence or halt the surveillance.

Congress has applied these three privacy-enhancing requirements to each of the five categories based on two value judgments. The first is that the less "content" a communication contains the less privacy protection that communication requires.[163] The second is that where the customer takes cognizable steps to protect information, that information receives more privacy protection.[164] Obviously, there is little one can do to maintain the privacy of the telephone numbers one dials.[165] Note, however, that storing computer information with a third party is tantamount to voluntarily giving up some protection of that information, perhaps on the theory that one could store the information in a more private fashion.[166]

Conceding that the level of protection Congress has allocated to each form of information is correct, one must then ask whether Congress has included the proper privacy-protective features in each category. The more direct question is whether the privacy-protective features allocated to transactional information are sufficient. While there are three methods by which an investigator can gain access to transactional information that constitutes more than demographic information,[167] evaluation of the easiest method of access is most relevant to the question of privacy protection.[168] That "easiest" method of access is the court order.[169] To understand the protection that the court order offers one must first understand the court order's required burden of

---

[163] *See id* § 2510(8) (defining "contents" as "any information concerning the substance, purport, or meaning of that communication").

[164] This is really just another way of saying subjective expectation of privacy. This is understood to require that a person take steps to keep an activity private. *See* LAFAVE, *supra* note 44, at 388-89**.** Note that in *Smith v. Maryland* the court found that, at least with respect to dialing phone numbers, taking steps to keep them private does mean that a telephone user will succeed on the expectation of privacy test. *See Smith v. Maryland*, 442 U.S. 735, 743 (1979). This might suffice to establish a subjective expectation of privacy, but it is not enough to make that expectation objectively reasonable. *See id.* The Court cites *United States v. Miller*, 425 U.S. 435, 442-44 (1976) for the proposition that a person does not have a legitimate expectation of privacy in information voluntarily given to third parties. *See id.* at 742-44.

[165] *See Smith*, 442 U.S. at 742 (1978) (stating that when a person uses a phone they understand they are conveying information to the phone company and even if they subjectively expect that information to be private there is no objective expectation of privacy).

[166] *See* FISHMAN & MCKENNA, *supra* note 102, § 29:9.

[167] *See* 18 U.S.C. § 2703(c)(1)(B).

[168] *See id.* § 2703(c)(1)(B)(ii).

[169] *See id.* § 2703(d).

proof.

ii. What are "Specific and Articulable Facts?"

When a law enforcement entity seeks transactional information based on a court under section 2703(d), it must offer "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought are relevant and material to an ongoing criminal investigation."[170]

In two cases dealing directly with the interpretation of this phrase courts have offered little help.[171] Consider that for a pen register warrant to issue, the government must show "that the information likely to be obtained is relevant to an ongoing criminal investigation."[172] Again, for a transactional information warrant to issue, the government must show "specific and articulable facts" showing reasonable grounds to believe that the information sought is relevant to an ongoing criminal investigation.[173] The latter implies something more than simply the willingness of an officer to certify under oath that the information sought by a pen register is likely to be relevant. Rather, it requires that a more specific (and "articulable") basis be offered to the judge to make him or her believe the information sought is relevant.[174]

The Court used the phrase "specific and articulable facts" in defining the requirements of "reasonable suspicion," the requirement police must meet before conducting a *Terry* Search.[175] While there is no reference to either a

---

[170] Id.

[171] See United States v. Kennedy, 81 F. Supp. 2d 1103, 1109-1110 (D. Kan. 2000).

> The government's application merely listed that the subscriber information connected to IP address 24.94.200.54 would possibly relate to an on-going criminal investigation . . . [T]he government should have articulated more specific facts such as how the government obtained the information it did have at the time and how this information lead the agents to believe that the attainment of the subscriber information of this particular IP address would assist in the investigation.

Id.; *see also* In re Application of the United States of America for an Order Pursuant to 18 U.S.C. 2703(d), 36 F. Supp. 2d 430, 433 (D. Mass 1999) (refusing to reach the issue for lack of ripeness).

[172] 18 U.S.C. § 3122(b)(2).

[173] *See id.* § 2703(d).

[174] *See* U.S. v. Kennedy, 81 F. Supp. 2d at 1109-11.

[175] A *Terry* Search is a search in which an officer searches a suspect they reasonably believe has committed or is about to commit a crime. *See* Terry v. Ohio, 392 U.S. 1, 21-22 (1968). This is a very limited search that involves a pat-down of the subject and nothing more. *See id.*

> [I]n justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion. . . . And in making that assessment it is imperative that the facts be judged against an objective standard: would the facts available to the officer at the moment of the seizure or the search "warrant a man of reasonable caution in the belief" that the action taken was appropriate?

Id. at 21-22.

Terry search or "reasonable suspicion" in the legislative history, one might argue that when Congress uses a legal term with an established definition, it means to incorporate that definition into the new law.[176] The definition of "reasonable suspicion," while not concrete, has been articulated and modified by the Court on several occasions.[177]

Generally, the reasonable suspicion standard is thought to require something less than that of probable cause.[178] While the requirement that police state specific and articulable facts serves to make the reasonable suspicion standard less vague, there is by no means a certain definition of the standard.[179] The courts have avoided defining reasonable suspicion in terms of the level of certainty it requires in comparison to probable cause.[180] Instead, the Court has emphasized the factual basis of the suspicion saying that it requires more than "unreflective or reflexive" action.[181] When viewed within the scope of the larger statutory scheme, this standard seems to fit. It is something more than is required for a pen register warrant and something less than probable cause.[182]

B. Is This Protection Adequate?

Two cases involving transactional information searches are instructive in showing the degree to which CALEA's statutory scheme effectively gives no protection to transactional information. In *United States v. Allen*,[183] the government had acquired a copy of the defendant's Internet transactional log from his service provider without a warrant.[184] The lower court had denied the defendant's motion for suppression of the information, and that ruling was affirmed by the Court of Appeals for the Armed Forces.[185] The latter court held that although a warrant was required under the statute, the evidence would not be suppressed because there was no exclusionary rule in the statute.[186] The court opined that while the defendant may have had an expectation of privacy

---

[176] *See* H.R. REP. NO. 103-827, at 31-32 (1994) *reprinted in* 1994 U.S.C.C.A.N. 3489, 3511-12.

[177] *See* C.M.A. McCauliff, *Burdens of Proof: Degrees of Belief, Quanta of Evidence, or Constitutional Guarantees?*, 35 VAND. L. REV. 1293, 1309-13 (1982) (citing Ybarra v. Illinois, 444 U.S. 85 (1979); Michigan v. Summers, 452 U.S. 692 (1981); United States v. Cortex, 449 U.S. 411 (1981)).

[178] *See id.* at 1309-10.

[179] *See id.* at 1312-13 (stating that whether reasonable suspicion is equivalent to probable cause is still an open question).

[180] *See id.*

[181] *See id.* (citing United States v. Lopez, 328 F. Supp. 1077 (E.D.N.Y. 1971)).

[182] That is that probable cause is at the top of the scheme, and at the bottom is the requirement for a pen register warrant. *See supra* Part II.A.

[183] 53 M.J. 402 (2000).

[184] *See id.* at 404-05.

[185] *See id.* at 405, 409-10.

[186] *See id.* at 409. Note that the logs in question tracked the defendant's movements on the Internet over the course of several months. *See id.*

in the contents of his Internet communications, he had little if any such expectation in the applicable transactional logs.[187]

In a similar prosecution, a civilian court denied a defendant's motion to suppress transactional data after information regarding the defendant's screen name was acquired by police with a subpoena.[188] In *United States v. Hambrick*, a New Hampshire police officer had visited on-line chat rooms posing as a young boy, presumably to catch Internet pedophiles.[189] Based on these chat room conversations, the officer sought to subpoena records from the defendant's ISP to determine his identity and location.[190]

The prosecution admitted the subpoena was invalid,[191] but the court refused to accept the defendant's claim that he had an expectation of privacy in the transactional information sought.[192] The court explained that while Congress had raised the bar with respect to access to transactional information, CALEA did not specifically establish suppression as a remedy for unauthorized access by the government.[193] The court stated that this was good evidence that the defendant's expectation of privacy was not "objectively reasonable,"[194] and further noted that CALEA allows an ISP to turn over such information to *private* entities without customer consent, thus implying that the expectation of privacy does not rise to a constitutional level.[195]

In *Hambrick*, the only information turned over to authorities was demographic information: the defendant's name, address, phone number, etc.[196] Arguably this sort of information is not as worthy of protection as the transactional logs in *Allen* because it, unlike the latter, reveals little about the individual.[197] While people generally should have the right to surf the Internet anonymously, law enforcement should be able to ascertain people's identities if and when there is a strong possibility of criminal conduct, just as it can with people driving down a highway.

The ECPA and CALEA were not Congress' first attempts at dealing with the question of how much protection transactional information should have.[198]

---

[187] See id.

[188] See United States v. Hambrick, 55 F. Supp. 2d 504 (W.D. Va. 1999).

[189] See id. at 505.

[190] See id.

[191] See id. at 506.

[192] See id. at 507-09.

[193] See id at 507.

[194] Id.

[195] See id. Note, however, that under 18 U.S.C § 2707, the provider may be held civilly liable for such actions.

[196] See U.S. v. Hambrick, 55 F. Supp. 2d at 507.

[197] See id. at 508 (pointing to the Supreme Court's risk-analysis doctrine in United States v. Miller and noting that defendant volunteered the information to his ISP); see also 18 U.S.C. § 2703(c)(1)(C) (2000) (specifically allowing access to this sort of information on the basis of a mere subpoena).

[198] *See, e.g.*, Video Privacy Protection Act of 1988, Pub. L. No. 100-618, § 2(a)(2), 102

In 1984, Congress similarly attempted to address the cable industry with the Cable Communications Policy Act ("CCPA").[199] One section of the statute applied to the protection of a consumer's transactional information.[200] While there is little discussion of the section in the CCPA's legislative history, Congress's apparent concern was that cable operators had the ability to keep track of viewing habits and use this information for marketing purposes.[201] The statute specifies that cable operators must seek written permission to sell such information and must notify consumers of exactly what sort of information they are tracking.[202]

The sort of information a cable service provider might obtain about its subscribers would be quite similar to what an ISP might obtain about its subscribers. The cable service provider would know what channels to which subscribers have access and when the subscribers watch those channels.[203] The CCPA, however, offers a much higher standard of protection than does CALEA.[204] The different statutory standards raise the question of why Congress would protect transactional information so strongly in the cable television regime, but give relatively weak protection within the Internet regime.[205]

One possible explanation is that transactional information in one regime typically is fundamentally distinct from transactional information in the other regime. An argument can be made that Congress could see little legitimate law

---

Stat. 3195 (codified at 18 U.S.C. § 2710). The act requires both probable cause before issuance of a warrant to search and also requires prior notice to the target of the search. *See* 18 U.S.C. § 2710(b); *see also* Freiwald, *supra* note 10, at 1013-16 (discussing the Video Privacy Protection Act and the respective level of protection it gives transactional information compared to ECPA and CALEA).

[199] *See* H.R. REP. NO. 98-934 at 19 (1984) *reprinted in* 1984 U.S.C.C.A.N. 4655, 4656-57; Cable Communications Policy Act, Pub. L. No. 98-549, § 2, 98 Stat. 2794 (1984) (codified at 47 U.S.C. § 551 (2000)).

[200] *See* 47 U.S.C. § 551 (1994).

[201] *See* H.R. REP NO. 98-934 at 29-30 (1984), *reprinted in* 1984 U.S.C.C.A.N. 4655, 4666-67.

[202] *See* 47 U.S.C § 551(a)(1), (c).

[203] *See* H.R. REP NO. 98-934 at 29-30 (1984), *reprinted in* 1984 U.S.C.C.A.N. 4655, 4666-67.

[204] *Compare* 18 U.S.C. § 2703(d) (2000) (requiring specifically articulable facts showing the information sought is relevant to an ongoing criminal investigation) *with* 47 U.S.C. § 551(h) (2000) (requiring a showing of clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought is material evidence, and requiring the subject have an opportunity to appear before issuance of the warrant).

[205] Note that there are practical implications of the different standards given by CALEA and the CCPA. *See* In re Application of the United States of America for an Order Pursuant to 18 U.S.C. 2703(d), 36 F. Supp. 2d 430, 433 (D. Mass 1999) (noting that cable operators are beginning to offer Internet service, thus raising the question of which statutory standard should apply to them).

enforcement interest in people's television viewing habits, while finding a distinct law enforcement interest in people's use of the Internet. Clearly, the Internet offers a wide array of communicative possibilities that a television does not. Furthermore, the regulation of government searches of cable television providers does not implicate the wiretapping laws. Transactional information in the Internet setting encountered regulation from a well-developed statutory scheme when the matter first arose. Thus the resulting protection of transactional information in the wiretapping regime may not be due to the type of information at issue, but to the statutory scheme already in place. That is, if Congress were to give Internet transactional information the same protection it did under the CCPA, this heightened standard would place transactional information on a level of protection above even that of voice communications.[206]

C. Challenging a Transactional Information Search

Two arguments are commonly raised in opposition of the level of protection given to transactional information. The first argument is founded on a claim of Fourth Amendment protection: transactional information should be afforded a reasonable expectation of privacy. The second argument is that transactional information involves the content of the communications, and is therefore protected under Title III unless a probable cause warrant is obtained prior to access.

i. Reasonable Expectation of Privacy

Determining whether there is a reasonable expectation of privacy in certain information invokes a two-prong test first articulated by Justice Harlan in his concurring opinion in *Katz*.[207] The first prong is the subjective portion of the test, which asks if a reasonable person could believe that the communication at issue was in fact private.[208] The second prong of the test, the objective portion, asks if society in general recognizes this expectation as reasonable.[209]

One commentator has argued that there should be a reasonable expectation of privacy in transactional information.[210] Another commentator has offered that educating the public might be one way of establishing an expectation of privacy in transactional information.[211] At this point, however, there is little recognition in the courts of an expectation of privacy in more content-based forms of communication like e-mail, let alone any serious recognition of an expectation of privacy in transactional information. The argument for a reasonable expectation of privacy, however, is gaining ground.

---

[206] *See* McCauliff, *supra* note 177, at 1303 (equating probable cause with the preponderance of the evidence standard).

[207] *See* LAFAVE, *supra* note 44, at 386.

[208] *See id.*

[209] *See id.* at 389.

[210] *See* Skok, *supra* note 12, at 81-82.

[211] *See* Freiwald, *supra* note 10, at 1017-18.

One court, at least in dicta, has recognized that there may be an expectation of privacy in an e-mail message before it is opened.[212] *United States v. Maxwell* was a case before the United State Court of Appeals for the Armed Forces involving the alleged possession and transmission of child pornography by an Air Force base commander.[213] The defendant challenged the validity of an FBI search warrant[214] for his e-mail account, claiming he had an expectation of privacy.[215]

The court offered that one's expectation of privacy diminishes when messages are sent on a computer.[216] The court stated, "the more open the method of transmission . . . the less privacy one can reasonably expect."[217] This reasoning implies that a sliding scale of privacy expectations may exist.[218] The court compared an e-mail message to a first class letter: "the sender [of both] can reasonably expect the contents to remain private and free from the eyes of the police absent a search warrant founded upon probable cause."[219] The court continues, "once the letter is received and opened, the destiny of the letter then lies in the control of the recipient . . . ."[220] The court seems to have held that a probable cause warrant would be required for access to an unopened e-mail,[221] while a warrant would not be required for a chat room message or an e-mail that has been opened.[222]

---

[212] *See* United States v. Maxwell, 45 M.J. 406, 417 (1996).

[213] *See id.* at 410-15.

[214] *See id.* at 413, 415. The question of the validity of the warrant centered on the fact that the initial warrant specified the files to be searched by user name. *See id.* The defendant had more than one user name and the initial search was conducted by AOL employees who knew the identification of the person attached to the user names to be searched. *See id.* at 414. AOL thereby conducted a search by subscriber name rather than user name, turning up the fact that the defendant had another account. *See id.* at 416. The contention was that police had no probable cause to search this other account because, at the time the warrant was executed, they did not know of its existence. *See id.*

[215] *See id.* at 416-17 (stating that there were numerous problems with the execution of the search and the scope of the items seized under the warrant).

[216] *See id.* at 417 (citing Gouled v. United States, 255 U.S. 298 (1921)).

[217] *Id.* The court holds that messages sent in public chat-rooms or in e-mail that is forwarded have no expectation of privacy. *See id.* at 418-19. Furthermore, the court reasons that the more people to whom a message is addressed will affect the expectation of privacy. *See id.* at 419.

[218] Interestingly, the court phrases the expectation of privacy in terms of an expectation that a message's contents will not be revealed to police, as distinguished from the expectation that an employee of the service provider might access the message. *See id.* at 418. This reasoning tracks that of *Walker v. Darby*, 911 F.2d 1573, 1579 (11th Cir. 1990) where the court stated that there is a difference between an expectation of privacy and an expectation of non-interception.

[219] *Maxwell*, 45 M.J. at 417.

[220] *Id.*

[221] A holding such as this would destroy the statutory distinction between electronic communications service providers and remote computing services in that, no matter the

A chat room is an electronic environment in which users can communicate with each other by typing messages into their computer.[223] The messages are then displayed on the screen, and any user who is logged in at the particular chat room can see the messages.[224] In *United States v. Charbonneau*,[225] the court held there was no reasonable expectation of privacy in communications conducted in a private chat room. In this case, a police officer went on-line to America Online ("AOL") chat rooms to investigate the distribution of child pornography.[226] After logging on to a given chat room, the officer would observe the conversation and "record" it.[227] Users of the chat room would create an e-mail list based on the users signed on to the chat room and then mail pornographic pictures to the users on the list.[228] The officer observed the defendant sending such pornography and then sought a warrant to identify the individual behind the user name.[229] A warrant was executed on the defendant's home where police retrieved child pornography.[230]

The defendant challenged the use of evidence gathered by the officer while in the on-line chat room on the basis of an expectation of privacy.[231] The court, relying heavily on *Maxwell*,[232] held that there was no expectation of privacy in an on-line chat room because the defendant assumed the risk that he was speaking to an undercover agent.[233] The rationale is hard to dispute. A public chat room is much like a public conversation in a mall or restaurant.

In a case involving the surreptitious transmission of a conversation between an undercover agent and the defendant, the Supreme Court held that the use of a transmission device did not make this a case of wiretapping.[234] The Court

---

storage facility, a warrant would be required for access to an unopened e-mail. Under the statute as constructed, if the e-mail were stored in a remote computing service, access might be gained through something less than a warrant. *See* 18 U.S.C § 2703(b)(1)(B) (2000).

[222] *See Maxwell*, 45 M.J. at 419.

[223] *See* Stephan K. Bayens, *The Search and Seizure of Computers: Are We Sacrificing Personal Privacy for the Advancement of Technology?*, 48 DRAKE L. REV. 239, 249 (1999) (explaining how a chat room works).

[224] *See id.*

[225] 979 F. Supp. 1177, 1179 (S.D. Ohio 1997).

[226] *See id.*

[227] *See id.*

[228] *See id.*

[229] *See id.*

[230] *See id.* at 1180.

[231] *See id.* at 1183.

[232] 45 M.J. 406. The lengthy quotation of *Maxwell* by the court implies that, although the precedent of a military court is not binding on a federal district court, the opinion was respected and in fact adopted. See U.S. v. Charbonneau, 979 F. Supp. at 1184.

[233] *See* 979 F. Supp. at 1185.

[234] *See* On Lee v. United States, 343 U.S. 747, 753-54 (1952); *see also* Lopez v. United States, 373 U.S. 427, 438-39 (1963) (permitting admission of a tape-recorded conversation surreptitiously made by a government agent where the defendant knew he was speaking to a government agent). Note that these decisions were prior to the passage of Title III in 1968.

compared this case to one in which a party stood outside a window and eavesdropped on the conversation.[235] This decision is analogous to the chat room situation. In both instances, the defendant unknowingly converses with a government agent, and the conversation is recorded. A possible distinction is that, in face to face conversations, the defendant has the opportunity to assess the credibility of the person to whom he is speaking; in the on-line environment, this is impossible.[236] Despite this, it is likely *Miller* would control this situation since information exchanged in the chat room is volunteered to a third party, destroying any expectation of privacy.

> One might have a subjective expectation of privacy in an e-mail or chat room conversation, but objectively people know they are, or can be, monitored and thus their expectation of privacy is not objectively reasonable. This was, in part, the rationale applied in *Smith v. Maryland*, which held that people have no expectation of privacy in the telephone numbers they dial because they know the phone company is keeping track of those numbers.

While it is one thing to know that the phone company keeps track of the numbers one dials for billing purposes or that an ISP stores copies of one's e-mails on its server, it is another thing entirely to realize that what one says on the phone or communicates on-line is being recorded or tracked by law enforcement.[237]

ii. Communications Content vs. Non-content

Communications content is "information concerning the substance, purport, or meaning" of a communication.[238] Non-content information is any information that does not fit that definition. Non-content based communications are not thought to implicate the Fourth Amendment.[239] Communications content comes under the protection of the Fourth Amendment and intercepting it thus requires a Title III warrant.[240]

However, these decisions are not thought to have been displaced by the passage of Title III. *See* Goldsmith, *supra* note 25, at 47.

[235] *See* On Lee v. U.S., 343 U.S. at 753-54.

[236] *See* Hoffa v. United States, 385 U.S. 293, 303 (1966) (holding that people engaging in face-to-face conversation assume the risk of being overheard or that the person to whom they are speaking is an undercover agent); Goldsmith, *supra* note 25, at 46-47 (noting that passage of Title III was not thought to displace this doctrine).

[237] *See* Walker v. Darby, 911 F.2d 1573, 1579 (11th Cir. 1990) (agreeing, in dicta, that there is a difference between a reasonable expectation of privacy and a reasonable expectation of non-interception).

[238] *See* 18 U.S.C. § 2510(8) (2000).

[239] *See* Freiwald, *supra* note 10, at 965. Note that the author uses the term "communications attributes" to refer to non-content based communications. *Id.* at 951.

[240] *See id.* at 965.

In *Brown v. Waddell*,[241] police obtained a warrant for a "clone pager"[242] to allow the monitoring, in real time, of pages sent to both of Brown's digital display pagers.[243] The defendant claimed the clone pager was simply a pen register intercepting only phone numbers.[244] However, the court found that the clone pager was not a pen register in part because it was capable of receiving more than just a phone number.[245] The court said that a true pen register would be capable of capturing only telephone numbers.[246]

The court in *Brown* effectively stated that it is possible to transmit communications content by way of digits alone, and that intercepting such a communication requires a probable cause warrant. However, in *United States v. Meriwether*, the court held that monitoring a digital display pager was not an interception within the meaning of Title III.[247] In this case police had arrested a suspect and confiscated his pager in the "on" position.[248] Police then monitored the pages coming into the pager and recorded the numeric messages, which contained more than just phone numbers.[249] The court found this was not an interception in part because an interception historically applied only to "transmissions," which the court interpreted as messages still in transit from sender to receiver.[250] Therefore, when the officer viewed the pager message he was "retrieving" a completed transmission and thus not intercepting.[251]

The *Meriwether* court went on to state that the defendant had no expectation of privacy in the numbers he sent to the pager because he could not have known it was actually in the possession of the person he thought he was paging.[252] This observation is akin to arguing that if one addresses and mails a

---

[241] 50 F.3d 285 (4th Cir. 1995).

[242] *See id.* at 287 (explaining how a clone pager works).

[243] *See* S. REP. NO. 99-541 at 9-10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3563-64 (distinguishing a digital display pager as one capable of displaying numbers (generally 15 or more) and/or letters).

[244] *See* Brown v. Wadell, 50 F.3d at 289.

[245] *See id.* at 294.

[246] *See id.* This dicta runs counter to Freiwald's contention that computerized forms of pen registers could allow police to access transactional information beyond phone numbers. *See* Freiwald, *supra* note 10, at 988-89.

[247] *See* United States v. Meriwether, 917 F.2d 955, 960 (6th Cir. 1990).

[248] *See id.* at 957.

[249] *See id.* The defendant in this case was one of the persons who called the pager in the possession of the police. *See id*. Police then called him back pretending to be the arrestee and agreed to a drug sale with the defendant. *See id.*

[250] *See id.* at 960.

[251] *See id.* The court also agreed with the district court that, since the initial search warrant specified seizure of a personal telephone book, the pager, and the numbers it subsequently displayed were within the scope of the warrant. *See id*. at 958. The court refers to a digital display pager as "nothing more than a contemporary receptacle for telephone numbers." *Id*.

[252] *See id.* at 959. Note that the defendant in this case was an individual who sent a page

letter to another, he or she has no expectation of privacy in that letter because the person at the receiving address might not be the one he or she intended to receive the letter. *Meriwether* runs counter to a number of other cases finding that gathering digital display pager messages does in fact constitute an interception.[253] If one assumes that accessing a display pager message is an interception, and that the message transmitted constitutes communications content, such activity would arguably have to fall under Title III. The importance of the difference between communications content and non-content to the statutory scheme therefore is crucial. Interception of a "message" from a tone-only pager would not require a warrant;[254] but intercepting a true message from a digital display pager would require a warrant.[255]

An argument that transactional information is more like communications content than non-content might succeed if courts are willing to recognize that even digits sent to a pager can constitute communications content. Similarly, there also would be a colorable argument that an Internet history log is also communications content.

iii. Another Possible Challenge?

Neither a reinterpretation of the expectation of privacy doctrine nor a characterization of transactional information as communications content is likely to be a winning argument for heightened protection. There is, however, another possible argument. If an applicable warrant does not comply with the necessary statutory requirements, that warrant is invalid and the evidence gathered under it should be suppressed as the so-called "fruit of the poison tree."[256] One case, though only in dicta, illustrates how suppression of transactional information obtained pursuant to an invalid warrant could be suppressed.[257]

In *McVeigh v. Cohen*, the defendant was under investigation by Navy authorities on suspicion of being a homosexual.[258] Investigators in this case had contacted an ISP and asked for the identity of a subscriber whom they suspected was the defendant, based on the user name the investigators had obtained from a tip.[259] The court, in a motion for a preliminary injunction by the appellant, found that the Navy had not complied with the ECPA in

---

to the party in custody. *See id.* at 957.

[253] *See, e.g.*, United States v. Sills, 2000 U.S. Dist. LEXIS 5570 (S.D.N.Y. 2000); Jackson v. State, 636 So.2d 1372 (Fla.App. 2 Dist. 1994); Mauldin v. State, 874 S.W.2d 692 (Tex.App.—Tyler 1993).

[254] *See* S. REP. NO. 99-541 at 15 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3569.

[255] *See id.*

[256] Nardone v. United States, 308 U.S. 338, 341 (1939) (stating that failure to comply with statutory requirements must lead to suppression of the evidence as "fruit of the poisonous tree").

[257] *See* McVeigh v. Cohen, 983 F. Supp. 215, 220 (D.D.C. 1998).

[258] *See id.* at 217.

[259] *See id.*

obtaining the subscriber information.[260] The court opined that "it is elementary that information obtained improperly can be suppressed where an individual's rights have been violated."[261]

While the court's strict application of the statute may have been in part due to the court's clear distaste for military policy regarding homosexuals,[262] the *McVeigh* decision demonstrates that the fact that the ECPA does not explicitly require suppression does not mean a court cannot do so on its own. Further, the court found that suppression should be granted for the type of subscriber information involved in *Hambrick*, let alone the far more personal and revealing sort of information involved in *Allen.*

While *McVeigh* is a hopeful sign that courts might choose to recognize some privacy right in transactional information, the weight of authority is against it. Arguably the *McVeigh* court was correct in its assertion that if Congress took the time to write a statute describing the requirements for access to transactional information they meant for it to be followed. Certainly, an exclusionary clause within the ECPA would more strongly encourage statutory compliance. However, a more moderate modification to the statute could both encourage compliance by investigators and give courts a statutory basis for suppressing evidence obtained in violation of the statute.

PART IV. PROPOSAL: ADDITION OF A NOTICE REQUIREMENT.

The key distinction between the access requirements for data stored with a remote computing service and those for access to transactional information is the lack of a notice requirement.[263] While the lack of a notice requirement serves to distinguish the two categories of information, it fails to protect adequately transactional information like Internet transaction logs. Lack of notice may be reasonable in terms of access to demographic information such as name and address, but an Internet transaction log has a much different character. As Congress has stated, an Internet transaction log is much more like communications content than non-content.[264] Therefore, Congress should modify Title III to place transactional information of a content nature under the same protection already accorded information stored with a remote computing service.[265]

A. Policy Justifications

One can distinguish between transactional information in general and information in the form of documents or e-mails stored with a remote computing service. The latter involves communication of a message while the

---

[260] *See id.* at 219-20.

[261] *Id.* at 220.

[262] *See id.* at 220-21.

[263] *See supra* notes 161-69 and accompanying text.

[264] *See* H.R. REP. NO. 103-827, at 31 (1994).

[265] *See supra* notes 161-65 and accompanying text.

former includes things like name, address and Web surfing habits. However, if the demographic sort of information is excluded from transactional information and one considers only the more content-rich forms of transactional information like Internet logs, the gap between the two begins to narrow.

Both are capable of conveying information about an individual that is not easily discernible such as personal interests, habits or future plans. Suppose an investigator knows that the target of an investigation took a trip some time ago. If he or she wants to ascertain the location of that trip, he or she might try to search the individual's ISP's servers for e-mail messages or documents related to the trip, or simply serve the local travel agency with a court order compelling it to disclose what sort of ticket it sold to the individual. In either case, the investigator is able to determine where the individual traveled. In the latter instance, the investigator can do so without allowing the individual knowing he or she is being investigated. Perhaps police should not be able to acquire the same information by way of a lesser standard simply because of how the information is acquired. Applying a notice requirement to searches for transactional information would also mean that the investigator would have to meet the additional requirements for delayed notice if he or she wanted to keep the investigation secret.[266]

B. Practically Speaking

The application of the notice requirement to transactional information would not radically alter the statutory scheme. A notice requirement simply would protect subscribers from the sorts of "fishing expeditions" made possible by the statute's currently low standard for access to transactional information.[267] In this way it would function like an exclusionary clause encouraging compliance with the statutory requirements. Investigators, however, could still avoid the notice requirement. They could get a probable cause warrant,[268] apply for an order to have backup copies of the information made,[269] or apply to have the notice delayed.[270]

A notice requirement thus would not represent a lot of additional protection, but it would insure some measure of compliance with the statutory requirements. The courts have demonstrated their reticence to suppress transactional information because the statute does not authorize suppression.[271] A notice requirement would give the courts some justification for demanding compliance. By addressing challenges to the search before it takes place, a notice requirement would protect privacy. In addition, the judicial process would benefit both through legitimizing the statute and injecting some fairness

---

[266] *See* 18 U.S.C. § 2705(a)(2) (2000) (stating the requirements for delayed notice).

[267] *See* FISHMAN & MCKENNA, *supra* note 102, § 26:15(c).

[268] *See* 18 U.S.C. § 2703(b)(1)(A).

[269] *See id.* § 2704(a).

[270] *See id.* § 2705.

[271] *See* United States v. Allen, 53 M.J. 402, 409 (2000); United States v. Hambrick, 55 F. Supp. 2d 504, 507-08 (W.D. Va. 1999).

into the judicial process. Further, a notice requirement could help to avoid the development of problematic case law such as that reflected within *Hambrick.*

The statute's fourteen day limitation on customer challenges ensures that investigators will not be seriously burdened by the process.[272] Even where delayed notice is authorized, the statute still appears to allow for challenges. However, at that stage, the challenge is more like a motion to suppress in that the search has already been conducted.[273] Nonetheless, this is an opportunity for the target of a search to insure that law enforcement conducts a legitimate inquiry and operates within the limitations of the statute.

V. CONCLUSION

The wiretapping statutory scheme is a sensible articulation of the relative importance of privacy within the various types of communication. While there are arguments for treating transactional information differently, they have yet to be adopted in court. The absence of an exclusionary remedy with respect to transactional information has not only served as a justification for according little privacy protection to transactional information but has resulted in the admission of evidence gathered on the basis of flawed warrants. Applying the notice requirement already in the statute to transactional information of a non-demographic nature will enhance privacy protection by affording the targets of searches the means to challenge the legitimacy of such a search.

---

[272] *See* 18 U.S.C. § 2704(b).

[273] *See id.* (stating only that challenge must be made within fourteen days after notice is given without reference to when the search took place).