Stanford Technology Law Review

Almost Private: Pen Registers, Packet Sniffers, and Privacy at the Margin

DAVID MCPHIE*

CITE AS: 2005 STAN. TECH. L. REV. 1
http:// stlr.stanford.edu/STLR/Articles/05_STLR_1

> "It may be that it is the obnoxious thing in its mildest and least repulsive form; but illegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. . . . [W]e decline to go beyond [established Fourth Amendment law] by even a fraction of an inch."[1]

¶1 "Servers don't gossip," proclaims a recent bus-side advertising campaign.[2] The ad is for an online job search service; the promotional hook is that, when it comes to particularly sensitive and private matters, one is clearly better off trusting a machine than a human.

¶2 The trouble is that when it comes to computerized, networked communications, no one is yet quite sure whether to buy that line or not. This uncertainty goes to the heart of the enormous public debate spawned by the development of the Internet, with its dual promises of perfect anonymity and perfect tracking.[3] To borrow from an old joke, with the advent of the Internet age, society has reached the end of all of its privacy problems—but the question is, *which* end?

¶3 The question of the scope of privacy in communications becomes especially urgent whenever it is the government that is doing the listening. Indeed, the issue becomes one of constitutional moment because it implicates Fourth Amendment guarantees against "unreasonable searches and seizures." A pair of Supreme Court cases illustrates well the acute ambiguities in the law. The 1967 case *Katz v. United States* holds that the Fourth Amendment bars the government from listening in on private phone conversations without complying with a hefty set of procedural requirements, including a showing of probable cause of illegality before a duly authorized magistrate.[4] On the other hand, *Smith v. Maryland*, decided just twelve years later, holds that the government may freely collect phone numbers dialed from a home telephone (using a "pen register" device) for any or no reason, no authorization required, and all without triggering any real Fourth Amendment analysis.[5]

¶4 Now, in a practical sense these cases are not ambiguous at all, as they set down a pair of clear rules highly amenable to straightforward application. Thus, the ambiguity lies not in their application,

---

* J.D., Harvard Law School, June 2003.

[1] Silverman v. United States, 365 U.S. 505, 512 (1961).

[2] Advertisement, for CareerSearch.com (seen by the author on a city bus in Boston).

[3] *See, e.g.*, Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) ("[T]he new information age is turning out to be as much an age of information *about* readers as an age of information *for* readers."); Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201 (2000) (suggesting the application of copyright-protecting technologies developed for the Internet to systems providing better privacy in patient records); Jonathan P. Cody, *Protecting Privacy over the Internet: Has the Time Come to Abandon Self-Regulation?*, 48 CATH. U. L. REV. 1183, 1184 (1999) (contending that "collection and use of personal identifiable information have never been cheaper or easier than in the online environment.").

[4] 389 U.S. 347 (1967).

[5] 442 U.S. 735 (1979).

but in our evaluation of their sum effect on privacy in telephonic communications as a whole. Given *Katz* and *Smith*, do we enjoy protection of privacy in our telephone conversations at the constitutional level? On its face, the answer seems to be yes. But questions remain. Justice Stewart's dissent in *Smith* compellingly argued that few of us "would be happy to have broadcast to the world a list of the . . . numbers they have called . . . not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[6] But most people do not seem terribly bothered by the lack of Fourth Amendment protection in the telephone numbers they call, indicating that they view the loss of privacy there as marginal at best.

¶5 This paper challenges that view, arguing that it is precisely at the margin that privacy matters most. This is especially true when yesterday's laws are applied to today's technologies, since the legal lines that get drawn at these margins rarely map in an expected fashion. The constitutional rule of *Smith* and pen registers, for example, does not translate easily to the realm of Internet communications and "packet sniffer" devices. But the problem is not simply one of stale language. The original statutory rules governing privacy in communications, embodied in Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[7] have been revisited on numerous occasions (most recently in the USA Patriot Act of 2001[8]) to reconsider and amend the existing structures, terms, and definitions in light of current technological developments. Does the net protection of privacy really stay more or less the same with each statutory amendment (as Congress usually claims is the case)? Or might a more cautious observer detect subtle changes in the law—movements at the margin?

¶6 This paper takes up this question through a reevaluation of the laws that regulate government use of pen registers and "packet sniffers" (the Internet counterpart to the pen register, roughly speaking).[9] The analysis proceeds in three parts. Part I reviews the basic history and development of the statutory and constitutional law governing privacy in communications. Part II takes a closer look at Title III's use of the concept of "contents" as the touchstone of its privacy scheme, and analyzes the difficulties inherent in that scheme. Finally, Part III tackles the Fourth Amendment question, ultimately arguing that the *Smith* decision is constitutionally suspect. The ultimate solutions prescribed for the current privacy law woes—sharper statutory language, modest increases in substantive statutory privacy rights, and recognition of constitutional privacy protections in "non-content"—might appear small in scope. Of course, that is precisely the point: even small adjustments of invaluable rights matter a good deal.

1. BACKGROUND

¶7 In 1967, the Supreme Court held in a pair of landmark cases (*Berger* and *Katz*) that the use of wiretap evidence in either a state or a federal criminal prosecution was violative of the Fourth Amendment when that evidence was obtained without warrant or other prior judicial authorization.[10] In the face of the uncertainty generated by these decisions, Congress stepped in to create a uniform legislative scheme governing wiretapping (Title III of the aforementioned Omnibus Crime Control Act) that purported to conform to the necessary constitutional constraints. Title III laid down a set of strict standards and procedures required of the government in its use of wiretaps. Any "interception" ("aural acquisition" in the original language[11]) of the "contents" of communications obtained without judicial approval of Title III conformity was made punishable by fine and/or

---

[6] *Id.* at 748 (Stewart, J., dissenting).

[7] Pub. L. No. 90-357, §§ 2510-2520, 82 Stat. 197, 211-225 (1968) (current version at 18 U.S.C. §§ 2510-2520 (2003)).

[8] Pub. L. No. 107-56, 115 Stat. 272 (codified in scattered sections of 8, 15, 18, 22, 31, 42, 49 & 50 U.S.C.).

[9] Denis Howe, The Free On-line Dictionary of Computing, *at* http://wombat.doc.ic.ac.uk/foldoc/ (defining "packet sniffer" as a "network monitoring tool that captures data packets and decodes them using built-in knowledge of common protocols. Sniffers are used to debug and monitor networking problems.").

[10] Berger v. New York, 388 U.S. 41 (1967); Katz v. United States, 389 U.S. 347.

[11] 18 U.S.C. § 2510(4) (1964 & Supp. 1970) (amended 1986).

prison,[12] and the fruits of such an interception were, and are, to be excluded at trial.[13] Title III's original language defined "contents" as "any information concerning the identity of the parties to such communication" or "the existence, substance, purport, or meaning of that communication . . . ."[14]

¶8 Title III did not explicitly mention the use of pen registers at the time when it was first passed, though the Senate Report suggested that the statute was not intended to prevent the use of such devices.[15] Almost ten years after Title III had been signed into law, the Supreme Court in *United States v. New York Telephone Company* relied on this legislative history and the statutory language in holding that pen registers did not intercept the "contents" of communications, and so did not fall within the scope of Title III.[16] The Court decided *Smith v. Maryland* shortly thereafter, finding that collection of information provided by pen registers did not raise constitutional problems, either.[17] The *Smith* majority cited *New York Telephone* for the proposition that pen registers were incapable of collecting the contents of telephone conversations, and noted that, in any event, there could be no "legitimate expectation of privacy" in data like a phone number which had been voluntarily turned over to a third party (in this case, the telephone company's switching equipment).[18] Thus, "[a]lthough petitioner's conduct may have been calculated to keep the *contents* of his conversation private, his conduct was not and could not have been calculated to preserve the privacy of the number he dialed."[19]

¶9 Congress revisited Title III in the Electronic Communications Privacy Act of 1986 (ECPA).[20] One of the primary purposes of the Act was to extend Title III's protections of "wire and oral communications" so as to encompass electronic communications, as well.[21] The Act also included for the first time provisions governing the use of pen register devices, imposing the requirement that government officials first certify before an authorized magistrate that "the information likely to be obtained [through the use of a device] is relevant to an ongoing criminal investigation . . . ."[22] The Act thus made explicit in the statute that which *New York Telephone* had inferred from the earlier version: that the use of pen registers did not fall within the scope of Title III.[23]

¶10 In an apparent effort to make clear the distinction between Title III and the pen register regulation schemes, Congress modified Title III's definition of "contents" so as to eliminate from its

---

[12] 18 U.S.C. § 2511 (2004).

[13] 18 U.S.C. § 2515 (2004).

[14] 18 U.S.C. § 2510(8) (1964 & Supp. 1970) (amended 1986). The Senate Report notes that the term "contents" is meant to include "all aspects of the communication itself. No aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded. The privacy of the communication to be protected is intended to be comprehensive." S. REP. NO. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2179.

[15] *Id.* at 2178 ("The proposed legislation is not designed to prevent the tracing of phone calls. The use of a 'pen register,' for example, would be permissible.").

[16] 434 U.S. 159 (1977). The Court argued that pen registers could not be understood as intercepting the "contents" of communication, as that term was defined under Title III, since "[n]either the purport of any communication between the caller and recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers." *Id.* at 167. Moreover, the court recognized that, as a technical matter, pen registers were incapable of "aurally acquiring" the "purport" of any communication, since pen registers "do not accomplish the 'aural acquisition' of anything." *Id.* Thus, use of such devices was considered untouched by Title III.

[17] Smith v. Maryland, 442 U.S. 735 (1979).

[18] *Id.* at 743-44.

[19] *Id.* at 743.

[20] Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified in scattered sections of 18 U.S.C.).

[21] 18 U.S.C. § 2511 (2004). The definition of "intercept" was also broadened so as to encompass "aural *or other* acquisition" of contents. 18 U.S.C. § 2510(4) (2004) (emphasis added).

[22] 18 U.S.C. § 3122(b)(2).

[23] 18 U.S.C. § 2511(2)(h)(i). While the Act provided definitions for "pen register" and "trap and trace device," § 3126(3), (4), as well as penalties for installation or use of such devices without a court order, §§ 3121(a), (c), the legislation did not appear to provide for the possibility that such devices could be used to collect the content of communications. The legislative history may be read as suggesting that such uses were presumed illegitimate. *See* Electronic Communications Privacy Act of 1986, S. Rep. No. 99-541,1986 U.S.C.C.A.N. 3555 (1986). Of course, collection of content without a warrant would be unconstitutional under Fourth Amendment under *Katz*, 389 U.S. 347 (1967).

scope the "identity of the parties" and the mere "existence" of communication.[24] The Senate Report noted, in an implicit reference to *New York Telephone* and *Smith*, that "[t]he Supreme Court has clearly indicated that the use of pen registers does not violate either [Title III] or the [F]ourth [A]mendment. Subsection 101(a)(5) of this legislation [amending the definition of "contents"] makes that policy clear."[25] The Communications Assistance for Law Enforcement Act of 1994 (CALEA) further clarified this distinction by adding to the statute the requirement that an entity authorized to use a pen register "shall use technology reasonably available to it that restricts the recording . . . of electronic . . . impulses to the dialing and signaling information utilized in call processing."[26]

¶11 While the ECPA and CALEA made it clear that the legal restrictions on wiretapping applied to electronic communications as well, they cast the pen register statute in terms that appeared to presume application only to telephonic technologies.[27] While some judges and magistrates proved willing to approve petitions for pen register orders monitoring electronic communications,[28] not all ruled that the statute could be applied in this manner.[29] Some proposals for clarification thus started stirring about Congress at the turn of the century.[30]

¶12 The terrorist attacks of September 11, 2001 brought about a sudden and urgent call for a serious review of electronic surveillance laws (among others) that might be strengthened for the purpose of fighting terrorism.[31] The USA Patriot Act generalized the pen register definition that had been carried forward from ECPA, broadening it to include "the dialing, routing, addressing, and signaling information utilized in the processing and transmitting of wire or electronic communications . . . ."[32] The amendment further made clear that data collected should not "include the contents of any wire or electronic communications," explicitly incorporating for the first time into the pen register statute the Title III definition of "contents."[33]

2. REEVALUATING THE STATUTORY SCHEME

¶13 The development of the statutory scheme governing the use of pen register devices undoubtedly represents a laudable effort on the part of a legislature attempting to juggle privacy concerns, law enforcement needs, and a desire for specific language that is nevertheless capable of encompassing technological progress, all while satisfying constitutional constraints. Especially commendable is the ECPA's imposition of a pre-surveillance requirement of clearance before a tribunal ("likelihood of

---

[24] The definition, which has been unchanged since the passage of the ECPA, now reads as follows: "'[C]ontents', when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (2004).

[25] *See* S. Rep. 99-541, 1986 U.S.C.C.A.N. 3555, 3567.

[26] Communications Assistance for Law Enforcement Act § 207(b), Pub. L. No. 103-414, 108 Stat. 4279, 4292 (1994) (codified (amended) at 18 U.S.C. § 3121).

[27] For example, until 2001, the definition of "pen register" still basically followed the language of ECPA, describing "a device or process which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached. . . ." 18 U.S.C. § 3127(3) (2000) (amended 2001). *See also* § 3127(4) (2000) (defining "trap and trace device" in telephone-specific terms). Note that this paper does not dwell on the possible differences in analysis that are due pen registers (which record outgoing calls) and trap and trace devices (which record incoming calls). Such an omission is not intended to imply that they ought to be considered equivalent for legal purposes.

[28] Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U.L. REV. 607, 634 n.125 (2003). Kerr's article is an excellent one, and touches on many of the same topics that this paper does.

[29] *Id.*, at 635 n.134.

[30] *See, e.g.*, S. 2067 § 105, 105th Cong. (1998) ("The E-Privacy Act"); S. 934 106th Cong. (1999) ("The E-Rights Act"); S. 2430 § 7, 106th Cong. (2000) ("The Internet Security Act"). *See* Statement of Senator Patrick Leahy, The Uniting and Strengthening of America Act ("USA ACT"), October 11, 2001, *at* http://leahy.senate.gov/press/200110/101101a.html (on file with Stanford Technology Law Review).

[31] The amendments to the pen register statute effected by the USA Patriot Act of 2001 were, however, at least facially modest, and largely reflective of changes that had been advocated before the attacks. Kerr, *supra* note 26, at 636. *See also supra* note 28. Of course, most of the Patriot Act involved subjects having nothing to do with pen registers, but only that aspect of the Act is considered in this paper.

[32] 18 U.S.C. § 3121(c) (2004).

[33] *Id.*

relevance"), which provides some degree of privacy protection in pen register data notwithstanding the lack of constitutional protection after *Smith*.[34]

¶14 Unfortunately, the protections offered by Title III and the pen register scheme are in many respects undermined by the defects and ambiguities inherent in the statute. The principal difficulty flows from the use of the notion of "contents" to distinguish between pen register surveillance (which is subject to minimal restrictions) and wiretapping (which is subject to heavy restrictions). This "content test," while promising ease of application, ultimately oversimplifies the critical privacy issues at play, and fails to fairly and effectively evaluate the legitimacy of warrantless surveillance of communications.

¶15 These problems are made manifest in at least three ways. First, how can content be reliably sorted out in contexts where content does not bear clear indicia of its status? Second, what is the scope of the term "content" as it relates to "addressing and signaling information"? Third, in what cases might pen register data obtained in the first instance directly yield, by implication and analysis, secondary information in a manner that could be considered an unreasonable invasion of privacy? These questions are taken up in turn.

A. Filtering content

¶16 A rule that turns on distinguishing content from non-content must presume that it is possible, as a technological matter, to separate the two, so that non-content may be isolated and collected under a pen register order without disturbing the content matter whose disclosure would require a wiretap order. In fact, this may have been a fair enough presumption at the time that pen registers were first used; dialing information, whether communicated via the voltage pulse of a rotary phone or the dual-tone frequencies of a touch-tone phone, is quite different in character from the electronic encoding of the human voice that makes up the bulk of a telephone call.[35] In other words, it is highly improbable that the sounds that humans make into the mouthpiece of a telephone receiver would ever be translated into electronic signals resembling a voltage pulse or a pair of specific dual-tone frequencies.[36] Thus, insofar as a pen register is built so as only to detect and interpret voltage pulses and/or specific dual-tone frequencies (and nothing else), it can be virtually assured that the pen register will only measure these particular non-content signals.[37] Furthermore, the ability to filter by temporal placement makes the filtering task even more straightforward. That is, because dialing information is communicated at the beginning of a call, presumably the pen register can be set to "listen" only to signals transferred between the dial tone and the initiation of the ringing of the destination phone.[38] In short, it initially appears that any filtering problem is utterly trivial, if such a problem even exists at all.

---

[34] 18 U.S.C. § 3122(b)(2) (2004).

[35] *See* JAMES MARTIN, TELECOMMUNICATIONS AND THE COMPUTER 409-11 (2d ed. 1976) (describing pulse and touchtone dialing signals). For example, the combination of a 1,209 Hz tone and a 697 Hz tone will trigger the recording of the number "1" on the pen register. *Id.* at 411.

[36] *But see* ROGER L. FREEMAN, FUNDAMENTALS OF COMMUNICATIONS 158 (1999) (describing the problem of "talk-down": "the premature activation or deactivation of supervisory equipment by an inadvertent sequence of voice tones through the normal use of the channel"). Of course, not all such premature activation of supervisory equipment was "inadvertent." *See* TLC, Hackers' Hall of Fame, *at* http://tlc.discovery.com/convergence/hackers/bio/bio_03.html (last accessed November 15, 2004) (relating how John Draper discovered that he could "make free phone calls using a plastic prize whistle he found in a cereal box").

[37] United States v. Focarile, 340 F. Supp. 1033, 1040 (D. Md. 1972) (holding that a touch tone decoder measuring only electrical "impulses, frequencies, and voltages," not "aural impulses," did not record content of telephone conversations). *See also* Application of the United States in the Matter of an in Order Authorizing the Use of a Pen Register or Similar Mechanical Device, 538 F.2d 956, 959-60 (2d Cir. 1970) (noting that pen registers do not capture content).

[38] Electronic Frontier Foundation, Statement Before the Subcommittee on the Constitution of the

Committee on the Judiciary, United States House of Representatives, The Fourth Amendment and Carnivore, *at* http://www.eff.org/Privacy/Surveillance/Carnivore/20000728_eff_house_carnivore.html (July 28, 2000) (on file with Stanford Technology Law Review) ("The system first accepts the call routing information (dialed number, number and accounting information of the phone used to make the call, etc.), secondly establishes a connection, and only then opens the line to the content side of the call. The routing information remains wholly separate and severable from the call content, allowing law enforcement easy access to the one but not to the other.").

¶17 However, later developments in both the use of telephones and in the technologies involved have complicated the entire line-drawing exercise. First of all, it is an increasingly common practice to employ automated systems that use dialed digits to acquire more substantive information from callers. Thus, while numbers dialed at the beginning of a call clearly represent addressing information, the numbers dialed after the initial connection is made are less easily categorized. For such numbers, not only is there no longer the temporal indication of non-content, but the constitutive presumption (that any signal that looks like one of a specific set of dual-tone frequencies must be non-content) has been eroded by the use of those same frequencies to represent content. Of course, these so-called "post-cut-through dialed digits" may sometimes in fact represent phone numbers or other non-content, as in the case where the caller first dials a long distance calling card number before entering the number of the true intended recipient of the call.[39] On the other hand, some post-cut-through digits are clearly meant to express substantive content, like account numbers.[40] Surely such information could well constitute part of the "substance, purport, or meaning" of a communication, thus falling under the statutory "content" rule.

¶18 While it would appear that law enforcement has indeed "always had the capability to obtain dialed digits, post-cut-through as well as pre-cut-through, in the [traditional telephone] environment,"[41] it remains to be determined whether they *ought* to be able to collect post-cut-through digits under a pen register order in those cases where the pen register cannot be utilized in a way that will automatically filter out digits that represent content.[42] Of course, the same sort of classification confusion could easily present practical/technological difficulties in reverse, as well.[43]

¶19 How do these issues play out in the context of electronic communications? In some respects, the filtering task may actually present less of a difficulty for a packet sniffer. For example, the analog to the "post-cut-through dialed digit" issue seems less problematic in the Internet context, since in practice, when addressing data is found in a content space (for now, say, outside of the TCP/IP headers), that data is put in a standardized format that would be easy to identify with the use of a packet sniffer.[44]

¶20 Nevertheless, it is often argued that the filtering problem is actually exacerbated in the Internet context, due to certain differences in the way that the telephone network and the Internet work. The Electronic Frontier Foundation (EFF) made just such an argument before a congressional subcommittee evaluating the constitutional issues presented by the government's use of packet sniffing devices. In the telephone context, they argued, routing data and content are processed on "a discrete and continuous segment of the telephone system," making it possible to "allow[] law

---

[39] U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 456 (D.C. Cir. 2000).

[40] "[Callers to] automated banking services enter account numbers. When calling voicemail systems, they enter passwords. . . . And when calling pharmacies to renew prescriptions, they enter prescription numbers." *Id.*, at 462.

[41] Department of Justice and Federal Bureau of Investigation, Remand Reply Comments Before the FCC In the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, Dec. 8, 2000, at 13, *available at* http://www.askcalea.net/docs/001208.pdf (on file with Stanford Technology Law Review).

[42] *See U.S. Telecom*, 227 F.3d at 462 (stating that there is "no way to distinguish between digits dialed to route calls and those dialed to communicate information"). Although the government has contended that it may legally collect such digits so long as it employs "technology reasonably available to it" to avoid processing content digits, at least one recent court case has declined to affirm such a position, hinting that "it may be that a Title III warrant is required to receive all post-cut-through digits." *Id.*

[43] Consider the caller who speaks the digits of an extension number to a system capable of voice recognition in order to get routed through to the desired destination. Surely the content value of a phone number should not turn on whether the number was spoken or dialed. Telecommunications Industry Association, Comments Before the FCC in the Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, May 20, 1998, at 45, *available at* http://www.tiaonline.org/policy/calea/comments52098.pdf (on file with Stanford Technology Law Review).

[44] The Session Initiation Protocol (SIP)—a protocol designed for use in systems offering Internet telephony—offers a simple example of this. When a user initiates a request to speak with another user located at another IP address, the packet extending that invitation contains information that (1) identifies it as containing SIP data, (*e.g.*, TCP over port 5060, *see* Internet Engineering Task Force, RFC 2543, March 1999, *available at* http://www.ietf.org/rfc/rfc2543.txt (on file with Stanford Technology Law Review)) and (2) a destination IP address expressed in a certain characteristic format that would be easy to pick out (e.g., "To: <sip:54385@172.104.32.64>"). Cisco Systems, VoIP Traversal of NAT and Firewall 7, *at* http://voip-itec.tamu.edu/files/reference/voip-nat.pdf (last visited Jan. 24, 2005) (on file with Stanford Technology Law Review). Thus, one could imagine a packet sniffer that would, when operating in pen register mode, record not only IP addresses contained in the IP header (where IP addresses are wont to be found), but also those that appeared in any packets containing SIP data.

enforcement easy access to the one but not to the other."[45] The Internet, by contrast, is "is a packet-switched network, meaning that when information is sent over the Net, it is broken into small packets, routed piecemeal over the Net [that is, not on its own discrete channel][46] and then reassembled at its final destination." Since "[r]outing information, as well as content, are both contained in each individual packet," therefore law enforcement "potentially" has access to both.[47] According to EFF, such access would be both completely unprecedented and a cause for great alarm.

¶21 Much of the description given in the EFF's account is accurate but the ultimate conclusions do not seem to follow. Routing data in Internet packets is placed in a well-defined "header" at the beginning of the packet, and thus it enjoys the same temporal indicia of non-content that exists for phone numbers that are communicated at the very beginning of a telephone call.[48] In both cases the initial routing data is handled separately from the data that follows. True, in the Internet context that stripping away of functional data must be performed on every single packet, whereas for most phone calls it happens but once. But why should that make a difference in terms of privacy?

¶22 It seems that the main argument has something to do with "potential" access, with the assumption that the packet sniffers give a "bad cop" operating under a pen register order much greater opportunity to sneak a peak at information outside the scope of the order. This is certainly a legitimate concern, but it is by no means evident that an equal temptation does not exist with respect to the bad cop performing pen register surveillance. As noted earlier, modern pen registers have the ability to detect "post-cut-through dialed digits," which must mean that the device is still connected and listening to the line even after the initial connection is made. The FBI describes the manner in which pen registers are operated in this way: the government "receives access to all signals transmitted over the subscriber's line . . . *including call content* as well as dialing and signaling information. . . . [T]he signals are sent to a device that is configured to record . . . signaling information . . . without recording or disclosing the call content."[49]

¶23 Thus it would appear that the pen register, once installed, is always listening, but is simply configured to only understand, interpret, and record dialed numbers (and so ends up hearing very little). This is, of course, precisely how a packet sniffer running in a "pen register" mode is designed to operate: detect only authorized data, and let the rest pass by unnoticed. Both devices find little difficulty in separating out addressing data that precedes (temporally) the bulk of the content. This is not to suggest that the potential availability of content to government officials intent on breaking the law is not a problem—that much is undoubtedly true in the Internet context.[50] But the problem is one that appears to plague the use of pen registers and packet sniffers alike.[51]

---

[45] Electronic Frontier Foundation, *supra* note 38.

[46] It is hard to imagine why this makes a difference in practice. After all, millions of people use the Internet every day without worrying about the fact that it gets broken up and sent "piecemeal" over the very same routers that everyone else is using to send data. This is not to say that one might not find such a setup unsettling on some level, but even then, is that not indicative of the fact that a highly distributed environment like the Internet is a less private place to begin with?

[47] Electronic Frontier Foundation, *supra* note 38.

[48] U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 464 (D.C. Cir. 2000).

[49] Dep't of Justice and Fed. Bureau of Investigation, Comments Before the FCC Regarding Further Notice of Proposed Rulemaking In The Matter of Communications Assistance for Law Enforcement Act, CC Docket No. 97-213, Dec. 14, 1998 at 78, *available at* http://www.askcalea.net/docs/981214.pdf

(on file with Stanford Technology Law Review) (emphasis added).

[50] It would be appropriate, for example, to use encryption or codes (under strict control of superior officers) to prevent unauthorized use of packet sniffing software in the field. But in an independent study of the government's "Carnivore" packet sniffing device, it was revealed that "[a]ll users are logged on as 'administrator' and no audit trail of actions is maintained." *See* IITRI, Independent Review of the Carnivore System, Final Report (2000), *at* http://www.usdoj.gov/jmd/publications/carniv_final.pdf (on file with Stanford Technology Law Review). Surely, such a "feature" should be remedied.

[51] Note that the filtering problem could be avoided entirely if the Internet community would simply adopt the "evil bit" protocol. *See* Internet Engineering Task Force, RFC 3514 (2003), *at* http://www.ietf.org/rfc/rfc3514.txt (on file with Stanford Technology Law Review) ("Firewalls, packet filters, intrusion detection systems, and the like often have difficulty distinguishing between packets that have malicious intent and those that are merely unusual. The problem is that making such determinations is hard. To solve this problem, we define a security flag, known as the 'evil' bit, in the IPv4 header.").

B. Defining content

¶24 The second difficulty with the content test is in determining the exact bounds of the term "contents." This question is distinguishable from the first, because it is concerned, not with identifying those attributes that are consistently associated with content, but rather with the more basic issue of what should substantively constitute "content." Of course, as discussed earlier, the term does in fact have a statutory definition: "any information concerning the substance, purport, or meaning of . . . [a] communication."[52] But the Patriot Act amendment to the pen register statute elaborates and complicates the scope of this definition by negative implication, mandating that pen register monitoring should be restricted to "dialing, routing, addressing, and signaling information utilized in the processing and transmitting of . . . communications *so as not to include the contents*. . . ."[53]

¶25 Thankfully, there is a core of cases that are easily categorized by these parameters. Most often the "substance, purport, or meaning" of a communication is inherent in the understanding of the language expressed: the gist of spoken words or text conveyed. That is obviously "content." At the other extreme, certain sorts of data (such as a telephone number dialed to initiate a call) are just as easily categorized as "dialing, routing, addressing, and signaling information"—information that presumably may be collected without including the "contents of any . . . communication[]."[54]

¶26 However, the exact relationship between the positive and negative definitions of "content" (substance and meaning versus addressing or signaling data) is unclear, and made worse by the fact that Congress has given no express definition for the latter.[55] At least three possibilities present themselves. First, "content" might include *all* data that is not "addressing and signaling information," no more and no less. Second, it might be that there is overlap in the categories, such that some addressing and signaling information could be considered content as well.[56] Third, there could actually exist some forms of data that do not fall within *either* category. Consider, in this respect, the fact that the *length* of telephone calls made from a particular line can be recorded with the use of a pen register.[57] Such data would be unlikely to be considered "content," as that term has usually been interpreted. But it is also hard to categorize call length as "addressing or signaling information." If "content" and "addressing or signaling information" are comprehensive and mutually exclusive categories, perhaps call length ought to be considered content, and hence not collectable under a pen register order. [58]

¶27 This categorization problem is only multiplied in the Internet context. Internet packets contain a large quantity of discrete and potentially revealing pieces of data, and for each type of data, its availability for collection under a pen register order depends upon this interplay of the "content" and "addressing and signaling information" requirements. Variations in the interpretation of these terms yield radically different pictures of what the government can get its hands on without a Title III warrant.

¶28 For example, suppose one takes the first interpretation above (that the categories are precisely complementary) along with a broad reading of "addressing and signaling information." The HyperText Transfer Protocol (HTTP) header (used to request and transmit web pages) contains several fields of information that could be swept under such a broad reading. For example, if the packet is requesting a web page, the exact name and location of the of the page is given in the HTTP header in a form such as "GET /docs/privacy.html HTTP/1.1." This is clearly addressing and

---

[52] 18 U.S.C. § 2510(8) (2002).

[53] 18 U.S.C. § 3121(c) (2001) (emphasis added).

[54] *Id.*

[55] Kerr, *supra* note 28, at 638 (noting Sen. Leahy's criticism of the vagueness of the "addressing and signaling" terms).

[56] Note that if this second interpretation is correct, then it would mean that there could be some sorts of addressing and signaling information that the government could not collect with a simple pen register order; in other words, "content" seems to trump "addressing and signaling information" under the text of the statute.

[57] United States v. Ambrosio, 898 F. Supp. 177, 180 (S.D.N.Y. 1995); United States v. Wajda, 810 F.2d 754 (8th Cir. 1987).

[58] 18 U.S.C. § 3121(c) (2001).

signaling information, in that it represents the web address or location of the desired resource, and signals to the web server how to direct the request. Similarly, the "Referer" [sic] field, which reveals the identity of the referring web page (that is, the page visited immediately before the one now requested), could plausibly be called addressing or routing information, under a broad definition of the terms, in that it reveals from where the client is coming in cyberspace (even though the referring information is not technically necessary to direct the client to the next page). Finally, Internet "cookies" are also transmitted to the server within the HTTP header, and might contain information that indicates to a server that the client should be routed or redirected to a particular location (perhaps the client's favorite starting page). If all addressing and signaling information is non-content, then all of this data is arguably available for collection under a mere pen register order.

¶29 Now posit the second interpretation of the statute, which allows for overlap in the categories. To the extent that any of the above could be considered content as well as addressing and signaling information, it cannot be collected without a wiretap order. After all, URLs may easily contain content-like information, such as the terms entered by a visitor to a search engine (e.g., a search for "privacy law" might yield the URL "http://www.google.com/search?q=privacy+law").[59] Similarly, cookies may also contain information such as account numbers or PINs, which are likely to be considered content.[60] Thus, the question of whether this sensitive information would be collectable under a pen register order appears to depend on a seemingly arbitrary choice between two plausible statutory interpretations.[61]

¶30 Consider now a *narrow* reading of "addressing and signaling information" under the first scenario, which would result in a broad understanding of the term "content." For example, TCP headers contain a "port number" which, roughly speaking, enables simultaneous use of many different applications (a web browser, an email client, etc.) on a computer with a single connection to the Internet. The port number is not exactly "signaling information utilized in the processing *and transmitting [over the Internet]* of . . . electronic communications,"[62] since the port number is ignored for the most part until it reaches the destination computer.[63] Thus, under the first interpretation, collection of port numbers would be disallowed.[64] But under the third interpretation (which allows for a gap between the categories), port numbers might well fall into neither category, and thus their collection would be neither approved nor disapproved by the statute: more confusion due to an ambiguous statutory text.

¶31 Consider one final and extreme example of the collision between content and addressing information: information hiding or "steganography." Steganography refers to the practice of communicating data by manipulating in unexpected ways communications over a known channel. For example, one commentator has documented cases of prisoners of war communication to each other by using the dots and dashes of handwritten letters to spell out Morse code messages.[65] Such a

---

[59] American Civil Liberties Union, Surveillance Under the USA PATRIOT Act , *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12263&c=206 (last visited Jan. 24, 2005) (on file with Stanford Technology Law Review).

[60] *Cf.* U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 462 (D.C. Cir. 2000). Zipcar.com is an example of a web page that embeds such information in its cookies.

[61] Distinguishing between content and non-content URLs or cookies via some automated mechanism, unfortunately, is a tricky matter, thus sending the relevant inquiry back to the filtering complication discussed earlier. Of course, for starters, one might require filtering out any HTTP "GET" data from the URL, which consists of the characters following the question mark in the URL. This does not solve the problem, however, since titles suggestive of content are often incorporated into URLs, for example, if the web page is entitled bombmaking.html.

[62] 18 U.S.C. § 3121(c) (2001) (emphasis added).

[63] Some firewalls or "traffic shapers" utilized in the interior of the Internet do pay attention to port numbers. For example, some employers and universities block the TCP ports associated with file-sharing applications (such as Napster) in an attempt to stop use of such software (and thus conserve bandwidth). This has led to a practice among some file-sharing applications of "port scanning" to circumvent such protections, leading one to wonder (perhaps tangentially) if a Digital Millennium Copyright Act issue is brewing there. *See* 17 U.S.C. § 1201(a) (1999).

[64] On the other hand, the port number might be considered a sort of signal through which an incoming packet (say, with port 80) can say to the operating system, "Send me to the web browser" (that is, the application traditionally associated with port 80).

[65] Mark Owens, A Discussion of Covert Channels and Steganography, March 19, 2002, *at* http://www.sans.org/rr/covertchannels/steg.php (on file with Stanford Technology Law Review).

message on its face would appear to a warden (or anyone delivering the letter) to be a normal English text (the known channel) with the Morse code (the covert channel) going undetected.[66] The rub here is that steganographic techniques can be used to hide substantive content anywhere, including in header data primarily used for addressing and signaling. For example, one writer describes a method of "TCP/IP Stego" that would "secret[] data within the header of a TCP/IP packet" by manipulating the (usually arbitrary) "32-bit [TCP] sequence number."[67] Routing data has now become substance, purport, meaning: content.

¶32 Now, it is no doubt highly unlikely that criminal defendants will start arguing that pen register evidence should be excluded at trial because it can be shown to contain steganographic content. Nor does it appear that the government has proven willing to take any interpretation of the statute that would arrive at some of the more radical consequences suggested above. For example, with respect to the government's official "DCS 1000" packet sniffing software (formerly known as "Carnivore"), it would appear from what is known about the way it is designed to be used, that the government has not by far taken the most pro-surveillance interpretation they might have.[68] The DCS 1000 collects IP addresses, packet length, port numbers, the "To" and "From" fields from the email header, but not URLs or cookies.[69] The point, however, is not what the government *does*, but what a slippery statutory text can plausibly be read as *allowing* it to do (say, at a time of crisis, when rationales of "expediency" set in). When that becomes the test, it becomes clear that the statutory language has simply too much play in the joints. Rather than leaving the courts to grapple with the scope of these terms, Congress should accept accountability, and step in to draw clearer lines.

C. Implications of non-content

¶33 The third difficulty with the content test is its seeming obliviousness to the fact that inferences of content can often be quickly and easily drawn from non-content data.[70] For example, in the case of a phone call to a number featuring a fixed, recorded message, capture and testing of the phone number undeniably leads to revelation of the full content of the call. Certain 1-900 numbers might similarly be suggestive (in both senses of the word) of content. Knowledge of the length of a call may also carry with it certain implications, e.g., the hour-long phone call to the pizza place suggests that the caller was not just ordering dinner.

¶34 Phone numbers may reveal additional non-content information that nonetheless might be considered private. One of the most obvious examples of this in the traditional (non-mobile) telephone context is physical location of the caller. While a phone number represents a logical communications address rather than an actual physical location, some translation from the first to the second can be accomplished easily, depending on the interceptor's access to auxiliary information. The area code portion of a phone number, for example, gives an immediate, general indication of location, determinable through the use of a map or table in the front of many phone books. Furthermore, the phone company, which owns the physical lines through which regular phone service is transmitted, is able to relay more precise information to the government, if needed. Indeed,

---

[66] In a more recent example, the U.S. government argued in a habeas proceeding for an alleged al Qaeda "enemy combatant," that there was good reason to deny the prisoner access to counsel because "al Qaeda operatives are trained to use third parties as intermediaries to pass messages to fellow terrorists, even if 'the intermediaries may be unaware that they are being so used.'" Padilla ex rel. Newman v. Bush, 233 F. Supp. 2d 564, 603 (S.D.N.Y. 2002), *rev'd*, Rumsfeld v. Padilla, __ U.S. ___ (2004). *Cf.* Kevin Maney, *Bin Laden's messages could be hiding in plain sight,* USATODAY.COM, Dec. 19, 2001, *at* http://www.usatoday.com/tech/columnist/2001/12/19/maney.htm (on file with Stanford Technology Law Review). Such a practice would be a prime example of communication through a covert channel.

[67] Owens, *supra* note 65.

[68] *See* IITRI, *supra* note 50 (describing operation of DCS 1000).

[69] *Id.* at 3-21. Note that for the FTP, SMTP, and POP3 protocols, certain (easily identifiable) packets containing only transactional data (for example, authentication of the email account owner) are recorded in their entirety.

[70] The Supreme Court itself has noted that "bits and pieces of data may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself," and that "[what] may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context." CIA v. Sims, 471 U.S. 159, 178 (1985) (internal quotes and citations omitted).

the FCC has noted that law enforcement agencies are "routinely" able to "obtain location information . . . from the telephone number."[71]

¶35 Of course, it would be ludicrous to suggest that the government should not be able to draw *any* damning inferences from the data they collect; that would defeat the entire purpose of this sort of investigative law enforcement. The point here is that it is overly simplistic to think that serious privacy issues can turn on questions of whether the information is content or not, and especially when certain kinds of "non-content" (however defined) may almost immediately suggest deeper layers of information implicating more precious notions of privacy.

¶36 The Internet context presents a host of examples of decidedly non-content data whose warrantless disclosure to the government still seems to give too much away. Consider the following list, which simply proceeds down the header stack of an Internet packet:

¶37 *Ethernet header*. One of the values transmitted in the Ethernet header of every packet transmitted or received by a networked computer is a globally unique ID called an "Ethernet address." Each Ethernet address is associated with a single LAN card, a physical component of the personal computer (PC) that provides networking functionality (in other words, the place on the PC that the cord from the Ethernet jack plugs into).[72] Of course, usually the mere invocation of the phrase "globally unique ID" is enough to raise the ire of privacy pundits (recall the flap about the unique IDs on Pentium III chips).[73] So why is it that no one has spoken out against the use of unique Ethernet addresses? The fact is that due to the way the Ethernet headers are used, a machine's Ethernet address is communicated only to immediately neighboring computers (usually the ISP) and not to anyone else—unless, of course, a packet sniffer is listening in.[74] Having access to the Ethernet address essentially tells the government from which physical computer the packets came. In the case of a laptop (or a personal digital assistant, etc.) with wireless access (say, across a campus), it is conceivable that this would mean the ability to track the physical location of the computer (and hence, most likely, its owner).[75]

¶38 *IP header*. The IP header contains IP addresses (both source and destination), which are the packet header data most often analogized (and aptly so) to telephone numbers. What information can be gleaned from these IP addresses? The numbers can often by translated into a more human friendly form ("host names") through a simple process known as "reverse domain name server (DNS) lookup." Host names provide a good deal more information than IP addresses, since they usually contain the name of the ISP through which the packet was sent (both for the source and destination). The ISP might be an employer or a school, which would be suggestive of affiliation with

---

[71] In re Communications Assistance for Law Enforcement Act, Third Report and Order, 14 F.C.C.R. 16,794, 16,816 (1999); *see also id.* at 16,814 ("[I]n the case of wireline communications the fixed location of the subscriber's terminal means that the telephone number of the terminal identifies the location of the call).

[72] Modems do not have any such address. (Then again, dial-up is a dying breed.)

[73] *See* Letter from Barry Steinhardt, Associate Director, ACLU, et al., to Craig R. Barrett, President & CEO, Intel Corp. (Jan. 28, 1999), *at* http://www.cdt.org/privacy/ issues/pentium3/990128intel.letter.shtml (also cosigned by representatives from the Center for Democracy & Technology, Consumer Action, Privacy Rights Clearinghouse, and Private Citizen, Inc.) (on file with the Stanford Technology Law Review).

[74] Nor are Ethernet addresses necessarily as private as one might think. Microsoft Office 97 used to use the Ethernet address as part of a unique identifier for all Word and Excel documents written on the computer to which the Ethernet address corresponded. Richard M. Smith, *Windows 98 Knows Who You Are*, BYTE.COM, March 12, 1999, *at* http://makeashorterlink.com/?Q13412694 (on file with Stanford Technology Law Review). Windows 98, as part of its online registration with Microsoft, was configured to send a "hardware ID" containing the Ethernet address (notably, without telling the user). *Id.* Furthermore, there has been some discussion about use of Ethernet addresses as unique identifiers for use with the next generation of the Internet Protocol, IPv6. Electronic Privacy Information Center, EPIC Alert (Oct. 12, 1999), *at* http://www.epic.org/alert/EPIC_Alert_6.16.html (on file with Stanford Technology Law Review). One solution that has been proposed to get around the privacy problem is to essentially have two kinds of addresses: a permanent, unique one for use with trusted peers, and temporary ones for more fleeting transactions. *See* Internet Engineering Task Force, RFC 3041 (Jan. 2001), *at* ftp://ftp.isi.edu/in-notes/rfc3041.txt (on file with Stanford Technology Law Review). Though these controversies are a few years old (rendering them ancient in Internet time), there is no way to know what addresses are still out there, and to what purposes they might be put. For example, a letter written by a government whistleblower (drafted in Word on an older computer at home) could be traced to its author through knowledge of the Ethernet address of the computer at home (available via a simple pen register order).

[75] Although it would seem that, in order to do so, the government would have to get an order covering several different local area networks over the area of movement.

those entities, as well as location.[76] Commercial ISP host names are also suggestive of location; small ISPs may be located in a limited geographic area, and large ISPs may have hostnames that reflect geographic location.[77]

¶39 The "total length" field of the IP header also lends itself to potentially incriminating inferences, since an exact byte count, especially of a large file, may serve as a sort of unique fingerprint of sorts. That is, if the government has a classified document (say, in PDF format) that is exactly 4,264,187 bytes long and suspect a particular unauthorized person might have a copy, then data from a pen register collection that the suspect transferred a 4,264,187-byte file to a remote computer is powerful corroborating evidence against that suspect.

¶40 *TCP header*. As has been noted, TCP headers contain TCP port numbers, which often correspond to particular applications. In other words, if pen registers see a packet sent to a particular IP address on TCP port 80, it is highly likely that it represents a request for a web page. At that point, of course, the IP address may be entered into the "location" field of a web browser, and it is possible to get an idea of what page or set of pages the monitored subject might have been looking at (unless, as is sometimes the case with smaller hosting services, the IP address is associated with a variety of unaffiliated web sites).

¶41 Sometimes, knowledge that a particular application is being used is suggestive in and of itself. For example, some universities and employers purposely block ports that are usually associated with file-sharing and instant-messaging programs, for a variety of reasons (desire to conserve bandwidth or increase productivity, fear of liability, etc.).[78] The widespread use of Napster, for example, prompted many network administrators to block or deprioritize traffic on TCP ports 6699 and 8888. Some students have told tales of getting called in to explain spikes in network usage over the port usually associated with the peer-to-peer (P2P) software Gnutella, only to explain that they were downloading free software for their Linux boxes.[79]

¶42 Of course, in general, the further down the header stack one travels, the more likely one is to encounter data that meets the statutory criteria of "content," thus directly earning the precise privacy protection denied in the examples given above.[80] And it is perfectly fitting that this content-rich data (e.g., the actual text of an email) should be granted such protection, as is generally conceded by those on all sides of the privacy debate. But this takes nothing away from the privacy value of the other kinds of data that are less clearly "content." Drawing the comparison is misleading; simply calling a bit of data non-content may sometimes mean very little in terms of privacy, measured by the level of intrusion into personal information that one might rationally want to keep secret. Perhaps some of

---

[76] For example, the user at the host name "roam123-213.student.harvard.edu" is likely located in Cambridge, MA. In fact, in the case of Harvard at least, more precise information connecting host names with location is publicly available online. *See* http://www.people.fas.harvard.edu/~lipoff/miscellaneous/files/friends (last visited Nov. 11, 2004) (on file with Stanford Technology Law Review). The host name given as an example in the text can be thus be pinned down to one of a couple of small dorm buildings.

[77] Alternatively, even when local host names do not bear such information on their face, location can sometimes be gleaned through the use of a "traceroute" utility (a version of which comes standard with most modern operating systems) to discover hosts in the immediate vicinity of the unknown host. These nearby hosts may have more location-suggestive names. Note that some ISPs actually publicly post maps that help in deciphering host names. *See, e.g.*, AOL Transit Data Network Map, *at* http://www.atdn.net/network_map.shtml (last visited Nov. 11, 2004) (on file with Stanford Technology Law Review).

[78] Billy Evans, Peer-to-Peer Networking (Oct. 29, 2001), *at* http://www.sans.org/rr/threats/peer2.php (on file with Stanford Technology Law Review).

[79] *See, e.g.* , Slashdot, University of Utah Promises DMCA Crackdown (Mar. 15, 2003), *at* http://yro.slashdot.org/article.pl?sid=03/03/16/0427214&mode=thread&tid=146 (on file with Stanford Technology Law Review) ("Our IT department noticed that our machine was originating a very large volume of outgoing traffic. They ran NMAP, and saw '6346/tcp filtered gnutella' and said 'Oh, they're running Gnutella.' They pulled our plug, without even bothering to try and contact the machine's administrator or the [computer] club's advisor first .□□ It turned out that someone was legitimately downloading a legitimate copy of the non-commercial QNX [ISO, a very large file] from our legitimate public FTP site."). Should users of certain kinds of software often used for illegal purposes simply expect to have to account for their actions on occasion? Similar questions could be asked concerning operating systems (revealed in the HTTP headers, one layer down from TCP): are Linux folks more likely to be engaged in illegal hacking of government computers? Is it then reasonable to engage in "operating system profiling"?

[80] But additional examples do exist. For instance, the DCS 1000 supposedly reads only the "To" and "From" fields of email headers, but independent testing showed that it recorded all the other fields, replacing their contents with Xs. *See* IITRI, *supra* note 50, at 3-15. What information might the length of a content field (for example, the "Subject" line) reveal?

these invasions of privacy are worth the good they do for law enforcement purposes, and perhaps others are not.[81] But as part of that discussion, it is vital to engage in the sort of analysis attempted here: at the end of the day, what is the government able to figure out about people for whom they do not even have probable cause to suspect as guilty of a crime?

¶43 This more nuanced analysis might suggest that simply tightening up statutory language might not be enough to preserve the sort of protections of privacy that American citizens find desirable. One remedy would be to encourage Congress to revisit the actual definition of "contents" so as to protect more of what is required to maintain commonly accepted notions of entitlements to privacy. Another option would be to increase the burden of obtaining a pen register order to begin with. Orin Kerr, for example, has suggested that an "articulable facts" standard might be appropriate.[82] Perhaps an even higher standard would be in order. At the very least, it seems likely that many voters seriously weighing privacy and law enforcement concerns against each other would draw the lines differently from where they are now (inexactly) drawn, on the side of increased privacy protection.

3. RECONSIDERING *SMITH V. MARYLAND*

¶44 The question of what the Constitution requires in terms of privacy in Internet communications reflects a much different inquiry than the essentially policy-based examination undertaken in Part II. One approach to such an inquiry would focus on the question of to what extent the Supreme Court's decision regarding pen registers in *Smith* governs the use of packet sniffers on the Internet to monitor comparable addressing data. This Part considers that inquiry, but is primarily concerned with a more central question. As Eugene Volokh has recently noted, amidst the current debate surrounding the Patriot Act and the proper application of pen register laws to the Internet, few have "argued that *Smith* was itself wrong and that the bad precedent shouldn't be extended." [83] The point is a valid one. In fact, an analysis of Smith both in the legal context in which it was decided, as well as under current law, ultimately reveals a series of serious shortcomings.

A. New York Telephone reconsidered

¶45 The answer to the deeper question Volokh proposes must begin not with *Smith* itself but an examination of the legal context in which *Smith* was decided. As detailed in Part I, the Court had held two years earlier in *New York Telephone* that pen registers did not fall within the original (as-of-then unamended) language of Title III. Although the Fourth Amendment question was not reached in *New York Telephone*, the statutory analysis contained several bad assumptions and errors that later infiltrated the constitutional analysis of *Smith*, as well.

¶46 First, note that the original provisions of Title III prohibited the intercepting of "contents," which included "any information concerning the identity of the parties to such communication. . . ."[84] Surely a phone number collected by a pen register is "content" under this definition, since it reveals "information concerning the identity" of the party called! The *New York Telephone* court seems to have actually understood this basic property of phone numbers at one point, since it noted at the opening of its opinion that the district court order authorizing the use of the pen register explicitly granted that authorization until "knowledge of the numbers dialed led to the *identity* of the associates and confederates of those believed to be conducting the illegal operation." [85] Yet the *New York Telephone*

---

[81] Of course, this is not to say that unconstitutional searches would become acceptable if their benefit to law enforcement were sufficiently high. But the Fourth Amendment sets only a floor of protection, not a ceiling. In terms of statutory protection, then, the policy "balancing" inquiry is perfectly legitimate.

[82] Kerr, *supra* note 28, at 639.

[83] Eugene Volokh, *The Mechanisms of the Slippery Slope*, 116 HARV. L. REV. 1026, 1078 (2003) (astutely asking why we "take the propriety of pen registers for granted"). Note, however, that at least one court has found *Smith* distinguishable in the context of the Internet, on the ground that this network data reveals details more "intimate" than phone numbers alone. Doe v. Ashcroft, 334 F. Supp. 2d 471, 510 (S.D.N.Y. 2004).

[84] 18 U.S.C. § 2510(8) (1964 & Supp. 1970).

[85] United States v. N.Y. Tel. Co., 434 U.S. 159, 162 (1977) (emphasis added).

court completely and inexplicably failed to realize that the ramification of such a finding was that the phone number content could not lawfully be collected without satisfaction of the requirements of Title III.[86]

¶47 Second, *New York Telephone* held that pen registers cannot "intercept" contents because they "do not accomplish the aural acquisition of anything."[87] "Aural acquisition," was, of course, the statutory definition of "intercept" at that time, but what does it mean? The word "aural" is used to describe something relating to the ear or the sense of hearing.[88] How should this word apply when contents are recorded by a machine to be listened to by humans at some later time? Since "aural" is an adjective, perhaps the simplest and most faithful reading of "aural acquisition" would be to place the focus on the nature of the modified subject "acquisition"—think about it as a "hearing acquisition."[89] That is, any device capable of detecting, measuring, interpreting, or recording an audible signal can be thought of as hearing or listening to that signal, and thereby acquiring content from it.[90] Unfortunately, most judicial opinions, like *New York Telephone*, find that pen registers "do not hear sound," but rather "decode outgoing telephone numbers by responding to changes in electrical voltage."[91] Of course, if "responding to changes in electrical voltage" is not "aural acquisition," then the use of a tape recorder seems on its face not to be "aural acquisition," either. But such a reading of the statute is absurd. Pen registers "hear" sound just as well as these other devices; they are just more particular about which kinds of sounds to record, and which to ignore.

¶48 Finally, what of the legislative history explicitly contending that pen registers were outside the scope of Title III? One particular portion of the Senate Report is cited by practically every court considering the question of pen registers and the scope of Title III as first passed by Congress:

> An examination of telephone company records by law enforcement agents in the regular course of their duties would be lawful because it would not be an "interception." (*United States v. Russo*). The proposed legislation is not designed to prevent the tracing of phone calls. The use of a "pen register," for example, would be permissible. But see *United States v. Dote*. The proposed legislation is intended to protect the privacy of the communication itself and not the means of communication.[92]

¶49 The language here appears to be unmistakable evidence that at least someone on or affiliated with the Senate Judiciary Committee thought that the provisions of Title III would not implicate pen registers. But consider that language in light of another passage that appears just a few paragraphs later in the Senate Report:

> Paragraph (8) defines "contents" . . . to include all aspects of the communication itself. No

---

[86] *Id.* at 167. Compare the Massachusetts Supreme Court's analysis of the identical language in the state wiretapping statute, District Attorney for Plymouth Dist. v. New England Tel. & Tel. Co., 399 N.E.2d 866, 869 (Mass. 1980) ("[T]he recording of the telephone number of the line from which a call was attempted is 'information concerning the identity of' a party to a communication"). The Massachusetts Supreme Court distinguished the case from *New York Telephone* by pointing out that the federal statute prohibited "aural acquisition of contents" while the state statute simply restricted acquisition generally. *Id.*, at 869-70. But, of course, the dialing information (the identity "content") captured by a pen register is not recorded aurally, so the cases cannot be plausibly distinguished in that manner.

[87] *N.Y. Tel. Co.*, 434 U.S. at 167.

[88] Steve Jackson Games, Inc. v. United States Secret Serv., 36 F.3d 457, 461 (5th Cir. 1994) (citing dictionary definition); United States v. Falcone, 505 F.2d 478, 482 n.19 (3rd Cir. 1974) ("The Oxford English Dictionary defines "aural" as: (1) Of or pertaining to the organ of hearing; (2) Received or perceived by the ear.").

[89] For example, a voice recognition device that converted an eavesdropped conversation into printed text would surely be an "aural acquisition of . . . contents" even if the end product were designed to be read, not heard. Such a conclusion would be fully consistent with the language of Title III, which protects "content" no matter the form in which it is ultimately recorded. 18 U.S.C. § 2510(4) (2004).

[90] That the collection of touchtone frequencies would be an aural acquisition seems sensible enough, but what about the voltage pulse signals generated by a rotary-style phone? After all, those pulse signals are intended to represent logical on-off values, not audible frequencies or pitches. Does it make any sense to say that a pen register "listens" to such signals? Such a conception may not be as absurd as it might first seem. The pulse signal, if connected to a speaker, *does* generate a series of audible clicks that are interpretable by ear. *See, e.g.*, United States v. Cox, 449 F.2d 679, 688 (10th Cir. 1971) (recounting police agents' successful attempt to determine from a wiretap recording the phone number dialed by "counting the clicks"). If police officers can aurally acquire the content of a rotary pulse signal, then why not a pen register?

[91] *N.Y. Tel.*, 434 U.S. at 167.

[92] S. REP. NO. 90-1097, *supra* note 14, at 2179.

> aspect, including the identity of the parties, the substance of the communication between them, or the fact of the communication itself, is excluded. *The privacy of the communication is intended to be comprehensive.*[93]

¶50 This second passage suggests that the privacy protections of Title III are meant to be read broadly, and that things like data regarding the "identity of the parties" and "the fact of the communication itself" are to be considered part of "the communication itself" (as opposed to mere "means of communication"). At the very least, there is an apparent inconsistency in the two legislative history provisions that demands reconciliation before an argument can be made by simply citing one or the other.[94]

¶51 More important, however, is the conflict between the first Senate Report provision cited above and the actual language of Title III (the latter of which, presumably, ought to control). That plain text reveals that "information concerning . . . identity" was unmistakably part of the "contents" of which interception was prohibited. That should have ruled out the unrestricted use of pen registers, regardless of what an ambiguous legislative history had to say on the matter.

B. Implications for Smith

¶52 In one sense, the three errors listed above were completely resolved with the passage of the ECPA in 1986. First, the ECPA amended the definition of "contents" so as to exclude existence of communication and the identities of the parties to a communication.[95] Second, it redefined "intercept" as "aural *or other* acquisition," effectively writing the troublesome word "aural" out of the statute.[96] Finally, it explicitly added a statutory provision exempting pen registers from the strictures of the wiretap statute, thus avoiding the need for any resort to legislative history on the matter.[97] Yet while the faulty statutory analysis in *New York Telephone* has been subsequently overruled by statute, the legacy of the mistakes it made are perpetuated by way of the *Smith* case, which finally resolved the constitutional question that the *New York Telephone* court (ironically enough) never even reached.[98]

¶53 This legacy is manifested in at least two ways. First, the statutory "contents test" articulated in Title III and first elaborated in *New York Telephone* was inappropriately imported into the constitutional analysis of *Smith*. The *Smith* majority opens its argument by noting that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[99] After drawing attention to the word "contents" (by putting it italics), [100] the majority proceeds to quote from *New York Telephone*'s analysis of the statutory definition of "contents," which lists off the elements (identity, existence, etc.) and argues that they do not apply to pen registers. In so doing, the *Smith* majority appears to incorporate into its decision both the Title III definition of contents as well as *New York Telephone*'s (mis)application of that definition to pen registers, thus elevating the clumsily crafted content test to a constitutional level.

¶54 Justice Stewart's dissent picks up on this wholesale borrowing from *New York Telephone* and chastises the majority for it: "It is true, as the Court pointed out in *United States v. New York Tel. Co.*,

---

[93] *Id.* at 2179 (emphasis added).

[94] Some have commented on the unfortunate fact that many such legislative history analyses are ultimately inconclusive: "wasted effort [and] expensive research and analysis that have no payoff." *See* William N. Eskridge, Jr., *Textualism, the Unknown Ideal?*, 96 MICH. L. REV. 1509, 1541 (1998).

[95] 18 U.S.C. § 2510(8) (2002).

[96] 18 U.S.C. § 2510(4) (2002).

[97] 18 U.S.C. § 3122(b)(2) (2004).

[98] Indeed, there is a curious circularity in the reasoning of this series of developments. Consider: (1) pen regist ers cannot acquire "contents" as defined in Title III, so pen register use is okay under Title III (*N.Y. Tel.*); (2) since *N.Y. Tel.* says pen registers can't acquire "contents," and the 4th Amendment only protects contents, then pen register use is okay under the 4th Amendment (*Smith*); and (3) since pen register use is okay under Title III and 4th Amendment, change definition of Title III "contents" so as to include only information that a pen register cannot acquire (ECPA).

[99] Smith v. Maryland, 442 U.S. 735, 741 (1979).

[100] The word "contents" is highlighted in italics in one other portion of the majority opinion, *see id.* at 743, again suggesting the pivotal weight the majority puts on the term in announcing its decision.

that under Title III . . . pen registers are not considered 'interceptions' because 'they do not acquire the 'contents' of communications,' as that term is defined by Congress. We are concerned in this case, however, not with the technical definitions of a statute, but with the requirements of the Constitution."[101] In other words, if there is something about the "contents" of communication that is inherently worthy of privacy protection under the Fourth Amendment, then there is no reason to think that the constitutional scope of the idea of "contents" should necessarily be defined by Title III (or the Supreme Court's strained interpretation of Title III, for that matter). After all, Justice Stewart argued, "[t]he numbers dialed from a private telephone—although certainly more prosaic that the conversation itself—are not without 'content.'"[102] Why? Because those numbers "easily could reveal the identities of the persons and places called, and thus reveal the most intimate details of a person's life."[103] (Never mind that such "identities" were supposed to be protected in the first place under the plain language of Title III.)

¶55 The second way in which *Smith* places undeserved reliance on *New York Telephone* is in the acceptance of the latter's holdings regarding the limited technological capabilities of pen register devices. *Smith* quotes *New York Telephone* for the proposition that a pen register "does not overhear oral communications and does not indicate whether calls are actually completed,"[104] that such devices "disclose only the telephone numbers that have been dialed,"[105] and that "[n]either the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers."[106] *Smith* accepts these characterizations without considering the current technological developments of the time (most notably the touch-tone phone) that might render such statements inaccurate. Indeed, the *Focarile* case (which predates *New York Telephone*) notes that the "pen register" device used in that case—"a TR-12 touch tone decoder"—was capable of recording not only outgoing telephone call numbers, but also the "fact the . . . phone was in use."[107] The court notes the capability without further comment, despite Title III's prohibition (not yet removed by the ECPA) against collection of information revealing the "existence . . . of communication."[108]

¶56 Today, courts consider as pen registers "devices that record the time, date and duration of both incoming and outgoing calls, devices that record, on tape rather than paper, not only the telephone numbers of the calls placed on a telephone, but other digits dialed, such as personal ID numbers and numbers used in maneuvering through voice-mail systems, and even devices that can record the contents of conversations, as long as that capacity is not used."[109] And such a list does not even begin to include the packet sniffer varieties of pen registers (devices completely unimagined by the Supreme Court of the 1970s, except in the name blithely borrowed from their telephonic cousins), and the full range of data elements such devices can capture. By failing to consider the possible current and future capabilities of "pen register" devices, the *New York Telephone* court left a loophole in the law—one that the *Smith* court blindly adopted as well.

---

[101] *Id.* at 748 n. 1 (Stewart, J., dissenting).

[102] *Id.* at 748 (Stewart, J., dissenting).

[103] *Id.* (Stewart, J., dissenting).

[104] *Id.* at 736 n.1.

[105] *Id.* at 741.

[106] *Id.*

[107] United States v. Focarile, 340 F. Supp. 1033, 1040 (D. Md. 1972) .

[108] *Id.* The court went on to point out (again, as noted earlier) that the device could be easily equipped with a "transducer such as a headphone or loud-speaker" capable of converting the monitored electrical impulses into audible, spoken text.

[109] Electronic Frontier Foundation, EFF Analysis of SA 1562, Subtitle B, *at* http://www.eff.org/Censorship/Terrorism_militias/20010919_eff_sa1562_analysis.html (Sep. 19, 2001) (analyzing a precursor bill to the USA Patriot Act) (on file with Stanford Technology Law Review).

C. Katz and contents

¶57 As discussed earlier, the talk of "contents" in *Smith* might be interpreted as a reading of *Katz* that recognizes a direct Fourth Amendment privacy right in certain substantive aspects of communications. In fact, Justice Stevens in his dissent in *Kyllo v. United States* appears to hint at just such an interpretation.[110] He compares the infrared thermal imaging camera at issue in *Kyllo* to a hypothetical "listening device [that] disclosed only the relative volume of sound leaving [a telephone] booth."[111] Justice Stevens contends that such a device "would be constitutional given *Smith v. Maryland*," since such a device would be incapable of "acquir[ing] the *contents* of communications."[112]

¶58 It would seem, however, that such an interpretation simply doesn't make sense when placed in the context of other Fourth Amendment jurisprudence as a whole. After all, many of the "bugged informant" cases involve disclosure of the actual speech and words—the contents—of conversations.[113] Why are such contents not entitled to privacy protection while those belonging to the *Katz* phone booth conversationalist are?

¶59 The sounder interpretation of the contents language in *Smith* is to read it in light of the classic two-part *Katz* test, which the *Smith* majority restates at the opening of its argument: did "the individual, by his conduct . . . exhibit[] an actual (subjective) expectation of privacy," and was that expectation "one that society is prepared to recognize as reasonable"?[114] Applied to the facts of the case, the *Katz* test asks whether the defendant Smith had both a subjective and an (objectively) reasonable expectation of privacy in the phone numbers he dialed. The notion of "contents," then, operates as a handy paraphrasing of the *Katz* rule, since what is generally thought of as "content" is also the sort of matter for which there is usually thought to be a subjective/reasonable expectation of privacy. But this mode of thinking about content is more a quick rule of thumb than anything else, and not intended to overrule the underlying *Katz* analysis. Accordingly, the most analytically significant portion of *Smith* is not the question of whether phone numbers are "content" or not, but rather whether there exists a reasonable expectation of privacy in such phone numbers. In so doing, the Court relies on the well-established rule that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[115] The *Smith* majority reasons that since telephone users "realize that they must 'convey' phone numbers to the telephone company" in order to complete calls, they may be understood as having lost any expectation of privacy in those numbers.[116]

¶60 Thus, to the extent that *Smith* has come to stand for a proposition about "content," rather than legitimate expectations of privacy, it is further evidence that "the *Smith* decision [has] led many people to accept a justification broader than what the opinion itself relied on."[117]

---

[110] Kyllo v. United States, 533 U.S. 27, 41-51 (2001) (Stevens, J., dissenting).

[111] *Id.* at 49-50 (Stevens, J., dissenting).

[112] *Id.* at 50 n.6 (Stevens, J., dissenting). It may be that the use of "contents" here is just one instantiation of Justice Stevens's more general rule that examines whether a device offers the "functional equivalent of actual presence in the area being searched." *Id.* at 47.

[113] Hoffa v. United States, 385 U.S. 293, 302 (1966); Lopez v. United States, 373 U.S. 427 (1963); United States v. White, 401 U.S. 745, 752 (1971) (plurality opinion).

[114] Smith v. Maryland, 442 U.S. 735, 740 (1979) (internal quotes removed).

[115] *Id.* at 743-44.

[116] The difference between the "content" and "legitimate expectations of privacy" readings of *Smith* becomes apparent by looking again at Justice Stevens's hypothetical "volume-meter." Under the "content" interpretation employed in the *Kyllo* dissent, it is enough to say that volume of a conversation does not constitute "content" (presumably under a narrow definition of the term) and so it is unworthy of Fourth Amendment protection. But under the "expectations" interpretation (the most plausible reading of *Smith*), the analysis is entirely different, turning upon the question of whether phone callers have a subjective belief that volume data in their conversations is private. That is a harder question. At the very least, it seems doubtful that callers "voluntarily turn[] over" volume data to the phone company (except in the general sense that all aspects of their calls are turned over to the company). See discussion, *infra*.

[117] Volokh, *supra* note 83, at 1092.

D. Assumption of risk

¶61 Ultimately, the "assumption of risk" rationale of *Smith*—that callers "voluntarily convey[] numerical information to the telephone company" and thereby "assume[] the risk that the company would reveal to police the numbers [they] dial[]"—presents the strongest argument in favor of its result.[118] At least, there is something reasonable about the proposition that the Fourth Amendment cannot provide protection against all dishonored secrets (a consideration that seems almost to sound more in First Amendment than anything else).

¶62 The *Smith* dissent nevertheless poses an important challenge to the risk assumption rule that demands further elaboration: the telephone conversation itself (the electronic representations of human speech), like the phone numbers dialed, must be "electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment."[119] But if the contents of a telephone conversation itself are viewed as being "voluntarily conveyed" to the phone company, then a straightforward application of the risk assumption rule cannot be squared with the holding in *Katz* that "the user of even a public telephone is entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.'"[120]

¶63 The necessary refinement to the risk assumption rule (and the one that deals with the dissent's counterargument) must be that a party entrusted with data can disclose it to the government *only where that party has been authorized by the originator of the data to use the data in some way*. Thus, goes the argument, phone companies can disclose phone numbers to the government, since phone callers may be understood as conveying those numbers to the phone companies themselves, authorizing their use (if only by machine) in routing the caller to his or her destination. But no similar authorization, express or implied, is given to the phone company vis-à-vis the conversation itself; therefore, the phone company is powerless to disclose that information (and the government is powerless to require it) without complying with the constitutional requirements for wiretaps.

¶64 It is hard to imagine any other way in which *Katz* can be reconciled with the risk assumption doctrine. Does this refinement work to explain the result in *Smith*? Almost—but not quite. The local exchange of a phone company (whose data a pen register seeks to record) certainly *receives* all digits of any phone number a caller enters, but does not necessarily use or look at all of those digits. Consider, for example, what happens when a phone call is made to another area code. The machinery of the local telephone exchange simply looks at the area code of the number dialed, recognizes it as a foreign code, and then forwards the number on to the appropriate carrier who will help connect the caller to the desired destination.[121] The last seven digits are never intended for use by the local exchange. Then how, under the *Katz*-risk assumption compromise, can the government expect the phone company to turn over those seven digits without implicating the Fourth Amendment?[122]

¶65 If this refined risk-assumption theory is right, then its implications for the application of *Smith* to the Internet are quite significant. When online service subscribers pass packets along to their ISPs, they do so understanding that the ISP will examine only those certain elements of the packet required to get the packet one hop closer to its destination (essentially Ethernet data and the destination IP address) and nothing more.[123] Once the packet is passed off to another ISP, the first ISP's obligation

---

[118] *Smith*, 442 U.S. at 744. This is not to say that this doctrine has not been heavily criticized. *See, e.g.*, Tracey Maclin, *Symposium: Katz, Kyllo, and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 97 (2002) (claiming the doctrine is "not a convincing legal theory").

[119] *Smith*, 442 U.S. at 746 (Stewart, J., dissenting).

[120] *Id.* at 747 (Stewart, J., dissenting), citing *Katz*, 389 U.S. at 352.

[121] Dep't of Justice & Fed. Bureau of Investigation, *supra* note 41, at 13 ("As we have noted before, when a subscriber dials a conventional inter-LATA long-distance call (e.g., '1-918-123-4567'), the subscriber's LEC uses only the area code ('918') to route the call; it does nothing with the remainder of the phone number ('123-4567') other than pass it along to the subscriber's IXC.").

[122] *Id.* A similar argument was presented during the course of the CALEA rulemaking proceedings before the FCC, and the government attempted to dismiss it by posing the "hypothetical" of being unable to obtain all the digits of a phone number from a single phone company as an example of the "preposterous result" that would be produced by a rule requiring that phone carriers only had to provide to law enforcement that data that they personally "use[d] . . . for call routing purposes." *Id.*

[123] This is admittedly speculation (as most conjectures regarding society's general subjective intents must be). But consider the

with regard to that packet is through. Thus, in the end, the ISP actually uses very little of the data present in the header of each packet it processes. Therefore, under the refined version of the risk assumption rule (that is, arguably the only version of the rule that can be squared with *Katz*), it would appear to be unconstitutional for the government to obtain that otherwise unused header data from the ISP without first obtaining a warrant or other appropriate approval before a magistrate. Such a conclusion represents a small but significant departure from generally accepted Fourth Amendment jurisprudence.

¶66 A few objections might be raised at this point. First, would not such an approach imply that constitutional protections of privacy would depend entirely upon how much data an ISP decides to look at?[124] In fact, the *Smith* case itself considered a hypothetical variant of this possibility, concluding (though without elaborating) that even "if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry," the force of "well-recognized Fourth Amendment freedoms" could not be overridden in such a fashion.[125] On a smaller scale, it should be noted that there is no reason why ISPs cannot be statutorily restrained in the scope of data they are allowed to look at; indeed, the current pen register statute already imposes some limitations on telephone companies and ISPs.[126]

¶67 A second objection might argue that the refined risk assumption rule is mistaken, and in fact only applies where, as in *Katz*, the matter underlying the privacy protection has some independent and inherent privacy-worthiness—a sort of conjunctive conglomeration of the two different interpretations of *Katz* considered earlier. Are the sorts of data protected by the reformulation of Fourth Amendment doctrine proposed here (e.g., URLs, port numbers, packet lengths) really inherently deserving of protection, or are they the sorts of petty details for which (to borrow the words of the *Kyllo* dissent) no one "would even care if anybody noticed"?[127] Of course, the entire point of Part II of this paper was that people do have actual, real, and substantive privacy interests even in data that might appear at first glance to be unimportant.[128]

¶68 Finally, it might be objected that this particular conception of the Fourth Amendment protection in communications does not go far enough. After all, those elements which are unmistakably communicated to and used by phone companies and ISPs (including Ethernet and IP addresses) are, under this analysis, still subject to the traditional rule of *Smith* implying no Fourth Amendment protection whatsoever. The first response is a simple concession that the risk analysis doctrine that has been so consistently applied in the Supreme Court's Fourth Amendment jurisprudence might itself be mistaken.[129] But even if it is not, it is to be remembered that there are no limits to the extent to which Congress can create privacy protections beyond what the Fourth Amendment is deemed to require. Notwithstanding the existence of super-constitutional legislation, there is still wisdom in having a robust constitutional safety net to steel the nation when the occasional fleeting temptation to abandon civil liberties comes along.[130]

---

following: the *Smith* court's finding of a lack of subjective expectation of privacy was based in part on the fact that phone consumers *knew* that phone companies recorded all the phone numbers they dialed, since they received a bill from the phone company with a list of those phone numbers each month. *Smith*, 442 U.S. at 228. In the Internet context, however, consumers of ISPs receive no monthly bill with a long string of URLs (or port numbers, etc.). Therefore, it would seem that *Smith*'s finding of no subjective expectation of privacy cannot be so easily foisted upon the Internet service subscriber. *See* Volokh, *supra* note 81, at 1092 (making a similar argument).

[124] Such a question becomes especially important as certain ISPs (and especially those affiliated with universities and businesses) have expressed an ever-increasing interest in closely monitoring the details of Internet traffic for a variety of reasons, among them the prevention of copyright or sexual harassment liability. *See supra* note 77.

[125] *Smith*, 442 U.S. 740-41.

[126] 18 U.S.C. § 3121(b) (2001).

[127] Kyllo v. United States, 533 U.S. 27, 50 (2001) (Stevens, J., dissenting).

[128] Moreover, there is a nontrivial argument that can be made directly from the reasoning of *Kyllo* for protection when communications take place within the seclusion of the home — even when the peripheral, mechanical trappings of those communications seem to be no more worthy of privacy than the "nonintimate rug on the vestibule floor." *Id.* at 37. "In the home, our cases show, *all* details are intimate details." *Id.*

[129] *See supra* n. 119.

[130] *Cf.* Electronic Privacy Information Center, Public Opinion on Privacy, *at* http://www.epic.org/privacy/survey/ (last

4. CONCLUSION

¶69 Whether or not servers can be accused of being prone to gossip, there is no doubt that they will cooperate with government authorities when those authorities come calling, warrant or not, unless laws protective of privacy have been put in place before the knock at the door. Fortunately, such laws are, in most respects, already in place for U.S. citizens, ensuring a broad scope of constitutional and statutory safeguards that almost provide us with a truly reasonable expectation of privacy. The trouble, of course, with the notion of "almost private" is that it smacks of meaninglessness. "A bathtub is a less private area when the plumber is present even if his back is turned."[131] In other words, sometimes almost-privacy is as bad as no privacy at all.

¶70 What to do at the margin? Congress should revisit its pen register statutes, clarifying its language to eliminate perilous ambiguities, and providing additional substantive protections so as to limit the ease with which the government can obtain sensitive information. The Supreme Court should rethink the reasoning of the *Smith* decision, especially in light of the capabilities of modern surveillance technologies. Finally, as citizens, we should demand clear lines that will unambiguously protect privacy rights, and then (notwithstanding the occasional ephemeral excuse) make sure that the government does not cross those lines . . . not "by even a fraction of an inch."[132]

---

visited Jan. 24, 2005) (on file with Stanford Technology Law Review) (citing polls showing that while voters generally approved of "more invasive police surveillance technologies" immediately following September 11, such support waned sharply in the succeeding months).

[131] United States v. Karo, 468 U.S. 705, 735 (1984) (Stevens, J., concurring in part and dissenting in part).

[132] Silverman v. United States, 365 U.S. 505, 512 (1961).