A BREAK IN THE INTERNET PRIVACY CHAIN: HOW LAW ENFORCEMENT CONNECTS CONTENT TO NON-CONTENT TO DISCOVER AN INTERNET USER'S IDENTITY

Laura J. Tyson[*]

> Subtler and more far-reaching means of invading privacy have become available to the Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.
>
> . . . The progress of science in furnishing the Government with means of espionage is not likely to stop with wire tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.[1]

I. INTRODUCTION

Katie Talbot[2] knew her next-door neighbor was fraudulently collecting state unemployment benefits while he simultaneously worked a job that paid cash under the table. Talbot considered using her state's anonymous whistle-blower Web page to report the fraud, but she was afraid that investigators might be able to learn her identity through her computer's Internet Protocol (IP) address and that her neighbor might somehow discover the source of the report. Talbot knew that Web surfing she did from her home computer could leave on any Web site that she visited a "digital fingerprint,"[3] which someone might later use to uncover her identity.

---

[*] J.D., 2010, Seton Hall University School of Law; B.A., 1987, University of Miami. The author would like to thank Professor Gaia Bernstein for her valuable guidance and advice regarding this Comment, and also members of the *Seton Hall Law Review* Board of Officers, especially Chester R. Ostrowski, Ashley Ochs, and Trevor F. Berrett, for their assistance.

[1] Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting).

[2] Pseudonym used to protect this individual's identity.

[3] Eric R. Diez, Comment, *"One Click, You're Guilty": A Troubling Precedent for Internet Child Pornography and the Fourth Amendment*, 55 CATH. U. L. REV. 759, 786 (2006)

Unlike Talbot, many Internet users are unaware that their Internet activities leave a trail of evidence that law enforcement can use to determine their identity.[4] David Lat—a young lawyer who worked at the United States Attorney's office in Newark, New Jersey—learned the harsh lesson regarding his privacy on the Internet. By day, Lat worked as an assistant federal prosecutor.[5] At night, in the privacy of his New York City apartment, he penned the satirical blog titled "Underneath Their Robes"—a humorous look at the personal lives of federal judges.[6] Lat used the same computer to respond to blog e-mails and personal e-mails, and his decision to do so ultimately cost him his anonymity as the author of the blog.[7] A former law clerk for a judge on the U.S. Court of Appeals for the Ninth Circuit uncovered Lat's true identity as the blogger by comparing the IP address embedded in the header of an e-mail the clerk had received from Lat with the IP address in an e-mail received from the still-unknown blogger.[8] The IP addresses matched, meaning that both e-mails originated from the same computer and that Lat was most likely the author of "Underneath Their Robes."[9] Had the clerk not received an e-mail from Lat, he would likely have been unable to uncover the blogger's identity, as he would have been unable to compare the IP ad-

(using the phrase "digital fingerprints"); *see also* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 126 (2007) (observing that "[d]ue to changes in technology and the realities of modern life, much First Amendment activity now leaves digital fingerprints beyond private zones protected by the Fourth Amendment" and that "Internet surfing in the seclusion of one's own home creates data trails with third parties in distant locations").

[4] *See* Joel Michael Schwarz, *A Case of Identity: A Gaping Hole in the Chain of Evidence of Cyber-Crime*, 9 B.U. J. SCI. & TECH. L. 92, 93 (2003) ("[M]ost people fail to appreciate exactly how personal information on the Internet is captured and used. . . . [A] person creates a record of activity from the moment that person logs on to the Internet, from every Web site that the person visits to every e-mail that the person sends." (citation omitted)).

[5] Jonathan Miller, *He Fought the Law. They Both Won.*, N.Y. TIMES, Jan. 22, 2006, § 14 (N.J. Weekly), at 1.

[6] *Id.*; *see also* Underneath Their Robes, http://underneaththeirrobes.blogs.com (last visited June 14, 2010).

[7] Telephone Interview with David Lat, Founding Editor, Above the Law (Nov. 5, 2008).

[8] Telephone Interview with David Lat, *supra* note 7; E-mail from David Lat, Founding Editor, Above the Law, to Author (Feb. 17, 2009, 09:32 EST) (on file with author).

[9] Telephone Interview with David Lat, *supra* note 7.

dress of the blogger against a known reference, the IP address from Lat's e-mail.[10]

Federal law enforcement agents frequently use an IP address to determine the identity of an Internet user. With only an administrative subpoena, agents can require an Internet Service Provider (ISP) to hand over the name, address, phone numbers, credit card information, and other personal information of a person using a particular IP address.[11] In fact, law enforcement agents routinely use the IP address captured by a Web site to discover the user's identity.[12] Are Internet users bothered by the fact that the government uses the invisible trail of evidence that their computer's IP address leaves on Web sites as a tool to uncover their personal information, including their names, addresses, and phone numbers? And do Internet users maintain a reasonable expectation of privacy in the personal information they give to their ISP? Many federal courts have answered this second question with an unequivocal "no,"[13] which places this privacy

[10] *See* Microsoft Office, Outlook, View E-mail Message Headers, http://office.microsoft.com/en-us/outlook/HA012303001033.aspx#1 (last visited June 14, 2010) (explaining how to view and translate e-mail message headers).

[11] *See* 18 U.S.C. § 2703(c)(2) (2006).

[12] *See, e.g.*, United States v. Polizzi, 549 F. Supp. 2d 308, 326–27 (E.D.N.Y. 2008) (explaining how law enforcement agents obtained access log records from the server hosting a suspect child-pornography Web site, extracted the IP addresses of every computer used to visit the Web site from the log, and then issued a subpoena to the ISP to obtain subscriber information), *vacated*, 564 F.3d 142 (2d Cir. 2009).

[13] *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (holding that the defendant's use of peer-to-peer software, which permitted others on the Internet to access certain folders in his computer, "could expose his subscriber information to outsiders" and that the defendant thus had no Fourth Amendment privacy expectation in subscriber information held by his ISP); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (holding that "e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the [Web sites] they visit because they should know that this information is provided to and used by [ISPs] for the specific purpose of directing the routing of information"); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) ("Individuals generally possess a reasonable expectation of privacy in their home computers. . . . They may not, however, enjoy such an expectation of privacy in transmissions over the Internet or e-mail that have already arrived at the recipient." (citations omitted)); Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (holding that "computer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator" (citations omitted)); United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *11–12 (4th Cir. Aug. 3, 2000) (holding no legitimate expectation of privacy in non-content subscriber information provided to an ISP), *aff'g* 55 F. Supp. 2d 504, 508–09

interest outside the scope of the Fourth Amendment.[14] Moreover, in 2001, Congress enacted laws that further reduced Internet users' privacy by allowing law enforcement to obtain a broader range of information about individual subscribers from an ISP.[15]

In light of the Supreme Court of the United States's decision in *Smith v. Maryland*, courts have recognized that in the context of a Fourth Amendment search, the contents of a communication receive greater privacy protection than non-content information.[16] Accordingly, federal statutes that provide privacy protections for Internet communications generally give the contents of a communication (for example, the body of an e-mail) broader protection than the non-content portion (such as the "To" and "From" addresses found in the header of the e-mail).[17] To require an ISP to disclose the contents of

(W.D. Va. 1999); United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass. 2007) ("The *Smith* line of cases has led federal courts to uniformly conclude that Internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other noncontent data to which service providers must have access."); Freedman v. America Online, Inc., 412 F. Supp. 2d 174, 181 (D. Conn. 2005) ("In the cases in which the issue has been considered, courts have universally found that, for purposes of the Fourth Amendment, a subscriber does not maintain a reasonable expectation of privacy with respect to his subscriber information."); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005) ("The courts that have already addressed this issue . . . uniformly have found that individuals have no Fourth Amendment privacy interest in subscriber information given to an ISP." (citations omitted)); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002) (holding that there is no reasonable expectation of privacy in subscriber information provided to an ISP); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("Defendant's constitutional rights were not violated when [his ISP] divulged his subscriber information to the government. Defendant has not demonstrated an objectively reasonable legitimate expectation of privacy in his subscriber information.").

[14] *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (explaining that the Fourth Amendment protects privacy interests that a person has actually exhibited and that society recognizes as reasonable).

[15] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 210, 115 Stat. 272, 283 (codified as amended in scattered sections of 8, 15, 18, 22, 31, 42, 49, and 50 U.S.C.) (broadening the scope of information available under 18 U.S.C. § 2703(c)(2) to include, among other things, "any temporarily assigned network address").

[16] *See* 442 U.S. 735, 741–42 (1979) (refusing to recognize an expectation of privacy in the phone numbers captured by a pen register because "pen registers do not acquire the *contents* of communications").

[17] *Compare* 18 U.S.C. § 2703(a) (2006) (requiring a warrant for disclosure of the contents of an electronic communication in electronic storage), *with* § 2703(c)(2)

an Internet-based communication, the government must first obtain a search warrant supported by probable cause.[18] When the government merely seeks the *identity* of an Internet user, however, no showing of cause is required—the government must simply serve an administrative subpoena on the ISP.[19] An Internet user's IP address thus provides law enforcement a quick and easy way to learn that user's identity.

Recent court rulings and federal laws have stifled the sense of freedom and anonymity individuals enjoy while using the Internet. Some might think that the quip made by Sun Microsystems CEO Scott McNealy that "you already have zero privacy—get over it"[20] has become a self-fulfilled prophecy and that "Internet privacy" is nothing but an oxymoron. To prevent that from happening, this Comment argues that courts should consider a different approach when responding to questions of the level of privacy an Internet user seeks and deserves. Because the content of a Web site can reveal highly personal information about the individual who visits it, the personally identifiable information attached to an IP address deserves greater privacy protections than federal courts and legislation presently allow. Courts should more closely scrutinize the distinction between the content and non-content portions of an Internet communication rather than rely on antiquated doctrines that do not adequately address all of the possible privacy concerns.

Part II of this Comment provides a brief overview of Internet technology and explains ways that law enforcement has used the Internet to catch criminals. Part III discusses federal sources of privacy protection in Internet use, including both statutory protections and early court decisions. Part IV discusses a New Jersey case, *State v. Reid*, which held that, under the New Jersey Constitution, Internet users have a reasonable expectation of privacy in their subscriber information held by their ISPs.[21] Part V explains why the methods and analo-

(mandating that an ISP disclose its subscriber's personal information, including name, address, phone numbers, and billing information upon the presentation of an administrative subpoena).

[18] *See* § 2703(a), (b)(1)(A).

[19] *See* § 2703(c)(2).

[20] John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, N.Y. TIMES, Mar. 3, 1999, at A1.

[21] 945 A.2d 26, 28, 33–34 (N.J. 2008).

gies used by courts in the past have not always resulted in the best decisions and provides suggestions for courts to follow when dealing with cases involving an Internet user's privacy rights.

II. A QUICK OVERVIEW OF INTERNET TECHNOLOGY

The means by which an IP address is created, assigned to a particular user, and becomes integrated with that user's Internet communications provides an important backdrop for understanding how law enforcement uses an IP address in investigations.[22]

A. Internet Basics

To access the Internet from home, a user must start with two things—an Internet-ready computer and an ISP. The ISP provides the necessary *physical* link between the computer and the Internet by supplying the household with either a cable modem or digital-subscriber-line (DSL) modem.[23] Every Internet modem has a unique serial number called a media-access-control (MAC) address,[24] on which the ISP relies to distinguish one modem from another, such as the modem that connects the house located at 10 Main Street from the modem that connects the house at 12 Main Street.[25] The ISP automatically assigns a unique number—the IP address—to the modem

[22] *See generally* United States v. Forrester, 512 F.3d 500, 505–06 (9th Cir. 2008) (describing how law enforcement used surveillance of defendant's e-mail and Internet activity to uncover evidence of a massive Ecstasy manufacturing lab).

[23] *See In re* Inquiry Concerning High-Speed Access to the Internet over Cable and Other Facilities, 17 F.C.C.R. 4798, 4803 (2002) (explaining that residential high-speed Internet access is provided over coaxial cables "in the form of cable modem service offered by cable [companies], and over copper wires in the form of digital subscriber line (DSL) services offered by local" phone companies); *see also* ANDREW S. TANENBAUM, COMPUTER NETWORKS 58–59 (4th ed. 2003) (describing the function of an ISP).

[24] *See* United States v. Schuster, 467 F.3d 614, 618 n.1 (7th Cir. 2006) ("A 'MAC address,' or media access control address, is a unique number assigned to the hardware of a particular computer or other device."); *see also* IEEE COMPUTER SOC'Y, IEEE STANDARD FOR LOCAL AND METROPOLITAN AREA NETWORKS: OVERVIEW AND ARCHITECTURE 6 (2002); J.D. Biersdorfer, *Making a Network Members-Only*, N.Y. TIMES, June 9, 2005, at C10.

[25] *See* London-Sire Records, Inc. v. Doe 1, 542 F. Supp. 2d 153, 178 n.34 (D. Mass. 2008) ("The MAC address is used by the ISP in routing information through the network and is specific to the user's computer.").

at each of its subscriber's locations.[26] Thus, the ISP uses the IP address to identify different households.

An IP address consists of four numbers separated by periods.[27] For example, one's IP address might be 68.100.108.40. The Internet Assigned Numbers Authority manages all IP addresses and allocates large blocks of IP addresses to Regional Internet Registries, which in turn allocate smaller blocks to ISPs, such as Comcast, Verizon, and Cox.[28] The result is that every modem that connects a household to the Internet receives a unique IP address, and the ISP is the only organization that can translate a particular IP address to a particular household and to the individual responsible for paying the monthly Internet bill.[29]

The Internet Corporation for Assigned Names and Numbers coordinates the assignment of Internet domain names—for example, www.textbooks.com—with the allocation of IP addresses to make sure that each IP address is unique and that all Internet users can access all valid Web addresses.[30]

Within an individual household, computers connect to the modem either by way of an Ethernet cable or via a wireless router. A wireless router provides the user with the flexibility to access the Internet using a laptop computer from any location in the house. Many people leave their wireless networks unsecured, which renders the network open to access by anyone else with a laptop.[31] Although some may do this on purpose, many fail to enable their wireless router's security due to confusion or ignorance about how wireless rou-

[26] *See* Klimas v. Comcast Cable Commc'ns, Inc., 465 F.3d 271, 273 (6th Cir. 2006) (stating that "[a]ny computer from which a person accesses the [I]nternet is assigned an IP address").

[27] United States v. Heckenkamp, 482 F.3d 1142, 1144 n.1 (9th Cir. 2007).

[28] *See* Internet Assigned Numbers Authority, Number Resources, http://www.iana.org/numbers (last visited June 14, 2010).

[29] An IP address by itself does not reveal a subscriber's name, address, or social security number. *Klimas*, 465 F.3d at 276 n.2. An Internet subscriber's personal information can only be determined by matching the IP address up with the data held by the ISP. *Id.*

[30] *See* Internet Corporation for Assigned Names and Numbers, Frequently Asked Questions, http://www.icann.org/en/faq (last visited June 14, 2010).

[31] *See* Timothy B. Lee, Op-Ed, *Hop on My Bandwidth*, N.Y. TIMES, Mar. 16, 2006, at A27.

ters work.[32] Many manufacturers ship wireless routers from the factory with default security modes disabled, which leaves the unsuspecting user's network vulnerable to "piggybacking"—a third party's unauthorized use of an open Internet network.[33] Additionally, many modems have wireless security features disabled by default to provide the user with an easier and quicker configuration.[34] A typical user might purchase the modem, use the "wizard" set-up to facilitate the installation, and then happily begin surfing the Internet, oblivious of the fact that the next-door neighbors can now also surf the Internet, thanks to the open network.[35] That user would likewise be unaware of a piggybacker's use of the network to conduct unlawful activity and might be surprised when confronted by federal agents asking questions about alleged downloads of child pornography.

When a person surfing the Internet clicks to view a particular Web site, that click triggers a flow of data from the computer out to the Internet. The data flow begins when the user either types in the Web site's Uniform Resource Locator (URL)[36] and presses "enter" on the computer keyboard or simply clicks on a link to a Web site. The click translates into a data stream from the computer to the cable or DSL modem supplied by the ISP. From the modem, the communication travels across the physical cable or DSL connection linking the subscriber's house to the ISP's main switching office where, guided by the destination IP address embedded in the original communica-

[32] *See id.* ("Perhaps the biggest problem [with open wireless networks] is that many people leave their networks open from ignorance.").

[33] NETGEAR INC., ROUTER SETUP MANUAL 1-9 (2007), *available at* ftp://downloads.netgear.com/files/WGT624v4_SM_30Apr07.pdf ("Once you have established basic wireless connectivity, you can enable security settings appropriate to your needs."); *see also* Matthew Hottell, *Defaults vs. Rational Choice: The Case of Home-Based Wireless Security*, 3 J.L. & POL'Y INFO. SOC'Y 319, 336 (2007) (concluding that default settings on wireless routers are a driving cause of consumers failing to secure their wireless networks).

[34] *See* Hottell, *supra* note 33, at 326–27 (noting that "[h]ome-based wireless access points are usually . . . left in a default, unsecure configuration" and describing the trouble through which a typical, uninformed consumer would have to go to enable wireless security for each computer in the household); *see also* NETGEAR INC., *supra* note 33, at 1-9.

[35] *See* Michel Marriott, *Hey Neighbor, Stop Piggybacking on My Wireless*, N.Y. TIMES, Mar. 5, 2006, § 1, at 1.

[36] *See* United States v. D'Andrea, 497 F. Supp. 2d 117, 120 n.12 (D. Mass. 2007) (explaining how a URL works).

tion, it reaches its proper destination—the physical server that hosts the Web site's content.

An Internet communication like the one just described has two components, content and non-content, and the distinction between the two is crucial. Content generally includes "any information concerning the substance, purport, or meaning of a communication,"[37] which includes the information found in the body of e-mail messages, e-mail attachments, and Instant Messages, as well as any other substantive information stored on an ISP's server.[38] The non-content portion of an Internet communication—typically called the "header"—includes both the originating and destination IP addresses.[39] Every communication sent across the Internet contains both the source computer's IP address and the destination computer's IP address.[40]

Non-content data helps ensure that the communication arrives at its intended target. For example, if a user points his Internet browser to www.google.com, the header information in the communication assures that the user's desire to see the Google page is fulfilled and that the user is not directed to some other location instead. The user's IP address embedded in the header also assures that, after the Google Web page receives the initial query, its response—the data, graphics, and text it sends back—arrives at the correct physical location. Thus, if Bob in Boise runs a search on Google for "Sonia Sotomayor," the results do not end up on the computer screen belonging to Paul in Pittsburgh. Even if a user does not specifically run a search but merely clicks on a Web page to view it, the Web site can capture the user's IP address.[41] As such, users inadvertently leave digital fingerprints on every Web site they visit.[42]

---

[37] 18 U.S.C. § 2510(8) (2006).

[38] *See* ORIN S. KERR, COMPUTER CRIME LAW 429 (2006) (explaining that content is the substance of the communication delivered); *see also id.* at 449 ("Contents of communications are the substance of the message communicated from sender to receiver.").

[39] *See* TANENBAUM, *supra* note 23, at 434.

[40] KERR, *supra* note 38, at 394.

[41] *See generally* Schwarz, supra note 4, at 97 (describing how Web servers capture visitor's IP addresses).

[42] *See* Solove, *supra* note 3, at 126 ("Internet surfing in the seclusion of one's own home creates data trails [akin to digital fingerprints] with third parties in distant locations.").

B. The Internet as a Conduit for Criminal Activity

The Internet offers a nearly endless array of opportunities for criminals to conduct illegal activities. Some criminals use e-mail as a convenient way to exchange child pornography.[43] Others have used the purported privacy of a chat room to exchange illicit files and data with other members of the chat room.[44] Computer hackers rely on the Internet to locate different Web sites from which to damage or steal data.[45] For each of these scenarios, law enforcement has powerful tools to determine the identity of the criminal. For example, if a law enforcement agent lurking in an Internet chat room observes evidence of illegal conduct, the agent can record the user's screen name and IP address and then contact the ISP to obtain the user's identification.[46] Second, a Web master who notices suspicious conduct from an anonymous user visiting a site can capture the user's IP address and forward it to law enforcement.[47] Third, law enforcement can target a particular Web page and obtain a log of IP addresses from the host.[48] Once law enforcement has that user's IP address, it only needs to issue an administrative subpoena to the ISP to obtain the user's identity.[49]

---

[43] *See, e.g.*, Hause v. Commonwealth, 83 S.W.3d 1, 4 (Ky. Ct. App. 2001) (describing how a defendant e-mailed child pornography to a California Sheriff's Department detective who had lurked in a chat room designated for individuals with an interest in children).

[44] *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1199 (10th Cir. 2008).

[45] *See, e.g.*, United States v. Heckenkamp, 482 F.3d 1142, 1143 (9th Cir. 2007) (describing how a college student in Madison, Wisconsin hacked into a corporate server located in San Diego); State v. Reid, 945 A.2d 26, 27 (N.J. 2008) (describing how a disgruntled employee changed the login password and shipping address of her employer's account information on its vendor's Web sites).

[46] *See, e.g.*, United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); United States v. Hambrick, 55 F. Supp. 2d 504, 505 (W.D. Va. 1999), *aff'd*, 2000 U.S. App. LEXIS 18665 (4th Cir. Aug. 3, 2000) (per curiam).

[47] *See, e.g.*, *Reid*, 945 A.2d at 29. In *Reid*, an Internet-technology (IT) specialist noticed that one of his client's accounts had been modified in a suspicious way. *Id.* The IT specialist notified the client of the suspicious activity and provided him with the IP address of the computer that was used to make the changes. *Id.* The client then gave the IP address to law enforcement personnel. *Id.*

[48] *See, e.g.*, United States v. Polouizzi, 564 F.3d 142, 146 (2d Cir. 2009).

[49] *See* 18 U.S.C. § 2703(c)(2) (2006) (requiring the government to issue an administrative subpoena to an ISP to obtain a subscriber's name, address, and phone number).

The above examples illustrate how law enforcement uses either content- or non-content-based information to learn the identity of a suspect. In the first example, law enforcement uses non-content-based information—the user's IP address—to determine the user's identity. In the third example, law enforcement starts with the content—the Web page visited by the user—and works backwards from there to determine the user's identity. The third example raises the question of whether Internet users can expect privacy in the substance and contents of the Web sites they visit. Internet users might rightfully object to the intrusion on their privacy that occurs when law enforcement collects the log of IP addresses from a particular Web site and, with the help of the ISP, identifies the users who clicked on the Web site. Moreover, Internet users might be surprised at the lack of available sources of privacy protection on which to rely to protect those interests.

III. SOURCES OF INTERNET PRIVACY PROTECTION

Internet users seeking to maintain the privacy of the personally identifiable information held by their ISP may look to several possibly overlapping sources of privacy protection: those inherent in the Fourth Amendment to the U.S. Constitution, those inherent in individual state constitutions, and those that Congress has created and enacted as federal statutes. Federal courts, when deciding the constitutional questions surrounding privacy in Internet use, often turn to and cite the statutory protections. Thus, this Comment will discuss those protections first.

A. Statutory Sources of Internet Privacy Protection: The Stored Communications Act

Congress developed the statutory framework that applies to protect the privacy considerations of electronic communications in the mid-1980s, years before the Internet achieved widespread public use.[50] Congress passed the Stored Communications Act (SCA)[51] in 1986 as part of a broad swath of privacy protections enacted under

[50] *See* TANENBAUM, *supra* note 23, at 57 (explaining that until the early 1990s, the Internet was used primarily by government, academics, and industrial researchers).

[51] 18 U.S.C. §§ 2701–12 (2006).

the Electronic Communications Privacy Act of 1986 (ECPA).[52] Congress enacted the ECPA in an effort to balance the government's need to obtain evidence with the public's desire to maintain the privacy of electronic communications and electronically stored information.[53] According to the Department of Justice, Congress intended that the ECPA would "fill in the gaps" left by the uncertain application of Fourth Amendment protections to Internet communications.[54] When law enforcement attempts to learn the identity of an anonymous Internet user, the ECPA—and, more specifically, the SCA[55]—controls how and when an ISP may disclose that information.

1. Content and Non-Content

The SCA controls both the disclosure of an Internet user's personally identifiable information and the disclosure of the contents of an Internet-based communication, and it treats these two categories quite differently.[56] Thus, to understand the SCA, it is first necessary to understand the differences between content and non-content information as used in the Act. The SCA draws its definitions from § 2510 of the ECPA,[57] which defines "content" as "any information concerning the substance, purport, or meaning" of a communication.[58] Applied in the context of an Internet communication, content includes the information in the body of an e-mail and any files sent as e-mail attachments.[59] Non-content includes a "record or other infor-

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

[53] *See* S. REP. NO. 99-541, at 1 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555 (stating that the ECPA's purpose was to clarify federal privacy protections in light of "dramatic changes in new computer and telecommunications technologies").

[54] U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 82 (2002), *available at* http://www.cybercrime.gov/s&smanual2002.htm.

[55] *See* §§ 2701–12.

[56] *Compare* § 2703(b) (controlling the disclosure of the *contents* of an electronic communication), *with* § 2703(c) (controlling the disclosure of the *records* pertaining to an Internet subscriber).

[57] § 2711(1).

[58] *Id.* § 2510(8).

[59] *See* KERR, *supra* note 38, at 449 ("Contents of communications are the substance of the message communicated from sender to receiver, while non-content information refers to the information used to deliver the communications from send-

mation" pertaining to a subscriber or a customer.[60] The statute does not define what "other information" about a subscriber is considered non-content, but at a minimum, "other information" includes the subscriber's name, address, local and long-distance phone-connection records, records of Internet-session times and durations, length of service (including the start date) and types of service used, telephone or other subscriber number or identity (including any temporarily assigned network address), and the means of payment for the service (including credit card or bank account numbers).[61] Thus, under the SCA, non-content information includes a vast amount of personal information about an Internet subscriber.

2. Voluntary Disclosure of Personal Information

Section 2702 of the SCA controls an ISP's voluntary disclosure of subscriber records.[62] It generally prohibits the voluntary disclosure of customer communications and subscriber records.[63] It specifically prohibits an ISP from voluntarily disclosing an Internet subscriber's record or "other information pertaining to a subscriber or a customer of such service" to a government entity,[64] but it does *not* restrict the disclosure of this information to a private entity.[65] As a matter of policy, however, many ISPs will not voluntarily disclose a subscriber's personal information.[66] Privacy policies vary from one ISP to the

ers to receivers and other network-generated information about the communication.").

[60] § 2703(c)(1).

[61] § 2703(c)(2).

[62] § 2702.

[63] § 2702(a).

[64] § 2702(a)(3).

[65] § 2702(c)(6) (allowing an ISP to divulge subscriber information to "any person other than a governmental entity").

[66] For example, Cox Cable's High Speed Internet Privacy Policy provides,

> We consider any personally identifiable information we receive about you to be confidential, and it is our policy to use it only in providing our websites and our cable television, internet and telephone services—from sales and installation, to operations, administration, advertising, marketing, support, network provision, maintenance, communications with you, billing, collection and in other ways related to our services.

Cox Communications, Privacy Policy, http://ww2.cox.com/aboutus/policies/your-privacy-rights.cox (last visited June 14, 2010).

next.[67] For example, the AOL Instant Messenger (AIM) Web site promises its members that personal information will not be shared with third parties unless the member consents.[68] Section 2702(a)(3) of the SCA merely prohibits an ISP from *voluntarily* disclosing personal information about an Internet subscriber to the government, but the exception to this general prohibition[69]—which essentially gives the government access to the same information whenever it wants[70]—reduces the provision's effective privacy protections. Thus, § 2702 provides Internet subscribers with a minimal threshold of privacy protection which an ISP, if it so chooses, may exceed.

3. Required Disclosure of Personal Information

When the government requires an ISP to disclose the personally identifiable information associated with an Internet user, § 2703(c) of the SCA applies.[71] This subsection allows the government to obtain a vast range of personal information about an Internet user, including the user's name, address, phone number, and billing information.[72] Section 2703(c) further divides "records" into one of two groups: the information available to the government under

---

[67] *See* Warshak v. United States, 532 F.3d 521, 527 (6th Cir. 2008) (describing the variety of ISP agreements and the resulting expectations of privacy that may come from them).

[68] AIM's privacy policy states:

> Your AIM information consists of personally identifiable information collected or received about you . . . . [It] may include registration-related information (such as name, home or work addresses, e-mail addresses, telephone and fax numbers, birth date or gender); transaction-related information (such as credit card or other preferred means of payment, or a history of products purchased through AIM) . . . .
>
> . . . .
>
> . . . Your AIM information will not be shared with third parties unless it is necessary to fulfill a transaction you have requested, or in other circumstances in which you have consented to the sharing of your AIM information.

AIM Privacy Policy, http://www.aim.com/tos/privacy_policy.adp#how (last visited June 14, 2010).

[69] § 2702(c)(1) (stating that an ISP may divulge an Internet subscriber's records or other information pertaining to the subscriber to the government as authorized under § 2703).

[70] *See* 18 U.S.C. § 2703(c)(2).

[71] *See* § 2703(c).

[72] *Id.*

§ 2703(c)(1), captioned a "record or other information pertaining to a subscriber";[73] and the list of information available to the government under § 2703(c)(2), which computer-crime legal scholar Orin Kerr refers to as "basic subscriber information."[74] The phrase "basic subscriber information" may be an understatement, however, as the list of information available to the government under § 2703(c)(2) extends well beyond "basic." Rather, "basic subscriber information" includes the Internet subscriber's name, address, local and long-distance telephone-connection records, length of service and types of service used, IP address, and method of payment for the service, including credit card account numbers or bank account numbers.[75] Thus, to more accurately convey the breadth of information available to the government under § 2703(c)(2), this Comment will refer to the list as "detailed subscriber information."

The SCA does not define the meaning of "record or other information pertaining to a subscriber" and few reported cases have interpreted the phrase.[76] Thus, the difference between information available under these two subsections is not altogether clear. The legislative history simply notes that "the information involved is information about the customer's use of the service[,] not the content of the customer's communications."[77]

Despite the lack of clarity in the differences between the information available to law enforcement under subsection (c)(1) and subsection (c)(2), one thing is clear: law enforcement can much more easily obtain the information available under (c)(2) than it can obtain the information available under (c)(1). Under § 2703(c)(1), law enforcement may require an ISP to disclose a "record or other information pertaining to a subscriber" only if law enforcement meets

---

[73] § 2703(c)(1).

[74] § 2703(c)(2); Orin Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1219 (2004) (describing the list of items available to law enforcement under § 2703(c)(2) as "basic subscriber information").

[75] § 2703(c)(2).

[76] *In re* Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 758 (S.D. Tex. 2005) (pointing out that no reported case has interpreted the phrase "record or other information pertaining to a subscriber or customer of such service").

[77] S. REP. NO. 99-541, at 38 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3592.

one of four requirements.[78] Law enforcement must obtain a warrant according to the requirements of the Federal Rules of Criminal Procedure, obtain a court order, obtain the consent of the subscriber to the disclosure, or submit a formal written request relevant to an investigation of telemarketing fraud.[79] On the other hand, under § 2703(c)(2), law enforcement is only required to present an administrative subpoena to require an ISP to disclose detailed subscriber information.[80] Alternatively, law enforcement may present either a federal or state grand jury or trial subpoena to obtain detailed subscriber information.[81] Finally, whether law enforcement seeks a "record or other information pertaining to a subscriber" or detailed subscriber information, it is not required to give notice to the subscriber that it has or will obtain the information.[82]

The amount of personal information about an Internet user available to the government has not always been so plentiful. In 2001 Congress updated and expanded the SCA when it enacted the USA PATRIOT Act (Patriot Act).[83] Enacted to deter and punish terroristic threats and to enhance law enforcement's investigatory tools, the Patriot Act expanded the scope of information that law enforcement could obtain with a mere administrative subpoena.[84] The amendments under the Patriot Act added "records of session times and durations," and "any temporarily assigned network address" to the list of information available to law enforcement under the detailed subscriber information category found in § 2703(c)(2).[85] In the Internet context, the "temporarily assigned network address" includes the IP address assigned to the subscriber by the ISP for a particular session.[86]

---

[78] § 2703(c)(1).

[79] *Id.*

[80] § 2703(c)(2).

[81] *Id.*

[82] § 2703(c).

[83] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 210, 115 Stat. 272, 283 (codified as amended in scattered sections of 8, 15, 18, 22, 31, 42, 49, and 50 U.S.C.).

[84] *See id.* § 210 .

[85] § 2703(c)(2).

[86] *See, e.g.*, United States v. Li, No. 07-CR-2915, 2008 U.S. Dist. LEXIS 22283, at *7 (S.D. Cal. Mar. 20, 2008) (holding that administrative subpoenas issued by the government to obtain information and login histories, including the date and time of,

Law enforcement uses this information to identify and trace the physical location of an Internet user suspected of engaging in criminal activity.[87] The Patriot Act amendments also allowed law enforcement to obtain the "means and source of payment" used to pay for service, including "any credit card or bank account number."[88] This change decreases the likelihood that a subscriber can hide behind a false name and address. Overall, the amendments made to § 2703 under the Patriot Act broadened the scope of information available to the government.[89] Notably, those amendments were not subject to the Patriot Act's sunset provision.[90]

In summary, when law enforcement seeks to learn the identity of an unknown Internet user and only has the IP address of the computer used to gain access to the Internet, it only needs to serve an administrative subpoena on the ISP to unlock a wealth of information about the user.[91]

B. Before the Internet: Early Fourth Amendment Communications Privacy

The cases that shaped the early development of Fourth Amendment communications privacy protections have had a remarkable impact on the modern decisions relating to an Internet user's privacy interests. What is significant is how the courts decide which privacy interests fall inside or outside the scope of a Fourth Amendment protected search.

The Fourth Amendment provides the right of the people to be "secure in their persons, houses, papers, and effects" and protects against "unreasonable searches and seizures."[92] To determine whether a government intrusion on a privacy interest constitutes a violation of the Fourth Amendment, the interest must satisfy the test outlined in Justice Harlan's concurrence in *Katz v. United States*.[93] An individu-

and IP address used for, each login for a particular user name, were authorized under the SCA).

[87] *See supra* Part II.B.

[88] § 2703(c)(2)(F).

[89] *See* USA PATRIOT Act § 224.

[90] *Id.*

[91] *See* § 2703(c)(2).

[92] U.S. CONST. amend. IV.

[93] 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

al must show a reasonable expectation of privacy in the area into which the government has intruded, and that expectation of privacy must be one that society recognizes as reasonable.[94] In *Katz*, the Court was asked to decide whether the government's use of an electronic listening device placed on a public telephone booth violated the telephone user's reasonable expectation of privacy.[95] After recognizing the vital role that the public telephone played in providing private communications, the Court held that the device violated the petitioner's privacy and thus constituted a Fourth Amendment protected search.[96]

Katz also reinforced the doctrine that information that a person "knowingly exposes to the public" does not merit Fourth Amendment protection.[97] This doctrine controlled the decision in *United States v. Miller*,[98] which in turn influenced subsequent Internet privacy decisions.[99] In *Miller*, the Court held that law enforcement's procurement of a suspect's bank records did not constitute an intrusion into a Fourth Amendment protected interest.[100] Offering three reasons to support its holding, the Court first concluded that the documents (which included checks and other bank records) were not confidential communications but were negotiable instruments used in commercial transactions.[101] Second, the Court noted that the complainant voluntarily conveyed the information to the banks and its employees in the ordinary course of business.[102] Third, the Court reasoned that the complainant could not claim any legitimate expectation of privacy regarding his bank records because Congress had said as much by enacting the Bank Secrecy Act.[103] The Court reiterated

[94] *Id.*

[95] *Id.* at 349 (majority opinion).

[96] *Id.* at 352–53.

[97] *Id.* at 351.

[98] 425 U.S. 435 (1976).

[99] *See, e.g.*, cases cited *infra* note 128.

[100] *Miller*, 425 U.S. at 440.

[101] *Id.* at 442.

[102] *Id.*

[103] *Id.* at 442–43. The Supreme Court previously upheld the constitutionality of the Bank Secrecy Act. *See* Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 69–70 (1974). In *Shultz*, the Court announced that a bank complying with the Bank Secrecy Act "neither searches nor seizes records in which the depositor has a Fourth Amendment right." *Id.* at 54.

that the Fourth Amendment does not prohibit the government from obtaining information that an individual revealed to a third party even if the individual reveals the information to the third party on the assumption that it will be used only for a limited purpose.[104]

In the 1979 case *Smith v. Maryland*, the Supreme Court considered whether a warrantless installation of a pen register at the phone company to record numbers dialed from a private home amounted to a search.[105] The Court first determined that because the pen register had been installed at the phone company, the petitioner could not argue that his property was invaded or that the government intruded upon a "constitutionally protected area."[106] The Court next considered whether an individual has an expectation of privacy in the phone numbers dialed from a home phone.[107] It rejected the petitioner's privacy claim, holding that because telephone users typically know that they must convey information to the phone company and because the phone company records this information for a variety of legitimate business purposes, telephone users could not claim any expectation that the phone numbers they dial would remain secret.[108] In reaching its decision, the Court acknowledged that "subjective expectations cannot be scientifically gauged," but nonetheless it was "too much to believe" that telephone users would expect that the numbers they dial remain a secret.[109]

Significant to the Court's analysis in *Smith* was its distinction between the *contents* of a phone call—the actual spoken communication, which *Katz* recognized as protected—and the non-content portion of the phone call, the number dialed.[110] This distinction between content and non-content has influenced modern cases that decided Internet privacy issues.[111] Thus, both *Miller* and *Smith* are significant for the impact they have had on modern courts attempting to untangle privacy issues stemming from Internet communications.

---

[104] *Miller*, 425 U.S. at 443.

[105] 442 U.S. 735, 736–37 (1979).

[106] *Id.* at 741.

[107] *Id.* at 742.

[108] *Id.* at 742–43.

[109] *Id.* at 743.

[110] *See id.* at 741.

[111] *See, e.g.*, United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *11–12 (4th Cir. Aug. 3, 2000).

C. Early Internet Cases: Fourth Amendment Protections

Beginning in the late 1990s, courts were asked to decide whether Internet users had a reasonable expectation of privacy in their subscriber information held by their ISP. One of the earliest opinions to decide this question was *United States v. Hambrick*,[112] a 1999 decision from the U.S. District Court for the Western District of Virginia. In *Hambrick*, a New Hampshire police officer posing as a fourteen-year-old engaged in an anonymous chat-room discussion with an individual who used the screen name "Blowuinva."[113] The officer suspected that "Blowuinva" intended to entice a minor to leave New Hampshire.[114] After determining that "Blowuinva" was using a computer with IP address 207.69.169.92 assigned by ISP MindSpring,[115] the officer prepared a subpoena (later deemed defective) that ordered MindSpring to release records and personal information on the subscriber to whom it had assigned that IP address.[116] MindSpring complied with the subpoena and provided investigators with Hambrick's name, address, credit card number, e-mail address, and phone numbers.[117] Police used this information to search Hambrick's residence, where they ultimately found incriminating evidence.[118]

Hambrick challenged the evidence that flowed from the defective subpoena and sought to suppress all the information provided by MindSpring.[119] The district court denied Hambrick's motion by first holding that the ECPA (under which the SCA was passed) was not a legislative mandate that an Internet subscriber has a reasonable expectation of privacy in his name, address, social security number, credit card number, and proof of Internet connection.[120] The court also rejected the notion that Hambrick's subjective expectation of

[112] 55 F. Supp. 2d 504 (W.D. Va. 1999), *aff'd*, *Hambrick*, 2000 U.S. App. LEXIS 18665.

[113] *Id.* at 505.

[114] *Id.*

[115] *Id.*

[116] *Id.* at 505–06. The subpoena was invalid because another detective in the same local police department had approved it. *Id.* at 506.

[117] *Id.* at 505.

[118] United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *5 (4th Cir. Aug. 3, 2000).

[119] *Hambrick*, 55 F. Supp. 2d at 505.

[120] *Id.* at 507.

privacy was one that society was willing to recognize as reasonable because he had knowingly revealed his personal information to his ISP, he had chosen a screen name that was linked to his true identity recorded in the ISP's records, and the ISP's employees had access to this information in the ordinary course of business.[121] From this, the court held that no reasonable expectation of privacy existed in the information that the police obtained from the ISP.[122] Because Hambrick had no reasonable expectation of privacy in the information, it was not protected under the Fourth Amendment, and suppression of the information was therefore not an available remedy in the criminal trial.[123]

The U.S. Court of Appeals for the Fourth Circuit affirmed the district court's decision in an unreported opinion.[124] The court relied heavily on *Smith v. Maryland* and *United States v. Miller* and quickly concluded that "the information at issue in this case is not distinguishable from the materials in *Miller* and *Smith*, as the government merely obtained non-content information."[125] The court limited its holding to finding that no Fourth Amendment privacy interest exists in non-content information.[126]

Hambrick was followed by the U.S. Court of Appeals for the Sixth Circuit in *Guest v. Leis*, which also held that Internet users do not have a legitimate expectation of privacy in their subscriber information when they convey that information to a third party such as a system operator of a Bulletin Board System or an ISP.[127] Many subsequent federal decisions followed *Guest* and, as a result, discarded privacy rights for Internet users by relying on the third-party doctrine from *Miller*.[128] For example, in 2008 the U.S. Court of Appeals for the

[121] *Id.* at 508.

[122] *Id.* at 509.

[123] *Id.* at 510.

[124] United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *14 (4th Cir. Aug. 3, 2000) (per curiam).

[125] *Id.* at *12 n.4.

[126] *Id.* at *13–14.

[127] 255 F.3d 325, 336 (6th Cir. 2001)..

[128] *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); United States v. D'Andrea, 497 F. Supp. 2d 117 (D. Mass. 2007); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174 (D. Conn. 2005); United States v. Sherr, 400 F. Supp. 2d 843 (D. Md. 2005).

Tenth Circuit in *United States v. Perrine* considered whether law enforcement violated the Fourth Amendment and the SCA when it obtained an Internet user's subscriber information.[129] In *Perrine*, a civilian showed local police the transcript of a conversation he had with "stevedragonslayer" in a Yahoo! chat room where "stevedragonslayer" had played several videos depicting child pornography.[130] Police obtained a court order pursuant to the SCA ordering Yahoo! to disclose the IP address of the individual using the "stevedragonslayer" screen name.[131] With the IP address provided by Yahoo!, police next determined that Cox Communications had registered the IP address, and police ordered Cox to provide subscriber information for the IP address.[132] From this, police issued a search warrant for Perrine's house, seized his computer, and discovered thousands of images of child pornography on the computer's hard drive.[133]

Perrine challenged the evidence on two grounds: first, that the government failed to show "specific and articulable" facts as required to obtain a court order under the SCA;[134] and second, that the search violated the Fourth Amendment.[135] The court rejected both arguments.[136] It concluded that the affidavits in support of the court order showed specific and articulable facts to show that the information sought was relevant and material to an ongoing criminal investigation.[137] With respect to Perrine's Fourth Amendment claim, the court concluded that because Perrine had voluntarily provided Cox and Yahoo! with his personal information and had enabled peer-to-peer file sharing on his computer, he could have no reasonable expectation of privacy protected by the Fourth Amendment.[138]

---

[129] 518 F.3d at 1201.
[130] *Id.* at 1199.
[131] *Id.*
[132] *Id.*
[133] *Id.*
[134] *Id.* at 1202.
[135] *Perrine*, 518 F.3d at 1204.
[136] *Id.* at 1202–04.
[137] *Id.*
[138] *Id.* at 1204.

IV. THE NEW JERSEY CASE OF *STATE V. REID*

In the wake of countless federal court decisions finding no privacy interests in personal information held by an ISP, the Supreme Court of New Jersey reached the opposite conclusion in its 2008 decision in *State v. Reid*, holding that an Internet user has a reasonable expectation of privacy in subscriber information given to an ISP.[139] Under *Reid*, information improperly obtained by law enforcement from an ISP must be suppressed to deter future police misconduct and to encourage respect for protected rights.[140]

In *Reid*, an IT specialist for a supplier's Web site noticed that someone had logged into one of his customer's accounts, changed the customer's shipping address to a nonexistent address, and then changed the login password to the customer's account.[141] The supplier's Web site captured the hacker's IP address of 68.32.145.220, which was registered to Comcast.[142] The IT specialist informed the customer about the suspected hacker and gave him the IP address.[143] The customer first attempted to obtain subscriber information for the IP address directly from Comcast, but predictably, Comcast declined to respond without a subpoena.[144] The customer next contacted the local police and gave them the IP address.[145] A detective obtained a subpoena *duces tecum* from the local municipal court to command Comcast to turn over information regarding IP address 68.32.145.220.[146] Comcast complied, providing information that implicated defendant Shirley Reid,[147] who was subsequently indicted and

[139] 945 A.2d 26, 28 (N.J. 2008).

[140] *Id.* at 37.

[141] *Id.* at 29.

[142] *Id.* Web sites such as Whois.net can provide the name of the ISP to whom a particular IP address is registered. *See* Whois By IP Address, http://tools.whois.net/whoisbyip/ (last visited June 22, 2010). For example, by typing "68.32.145.220" into the search box on the Whois By IP Address Web page, one can learn that the address is registered to Comcast Cable Communications, Inc. NJ-SOUTH. *Id.*

[143] *Reid*, 945 A.2d at 29.

[144] *Id.*

[145] *Id.*

[146] *Id.*

[147] *Id.* at 29–30.

charged for computer-related theft in violation of a New Jersey statute.[148]

At trial, the court granted Reid's motion to suppress after finding that she had a reasonable expectation of privacy in the personal information held by her ISP and that the resulting search violated Reid's state constitutional right to be free from unreasonable searches because the subpoena issued by the municipal court was defective.[149] The Appellate Division of the New Jersey Superior Court affirmed the trial court's order of suppression, and the State appealed.[150]

After framing the question as whether "Internet subscribers have a reasonable expectation of privacy in their identity while accessing Internet [Web sites]," the Supreme Court of New Jersey held that individuals have a reasonable expectation of privacy in the subscriber information provided to an ISP.[151] After recognizing the importance of computers and the Internet to everyday modern life, the *Reid* court compared ISP records with telephone and bank records, both of which New Jersey had already afforded greater privacy protections than those available under federal law.[152] The court recognized that Internet users provide information to an ISP for the limited purpose of gaining use of the ISP and not for the purpose of allowing the ISP to release their private information to others.[153] To respect an Internet user's privacy, police seeking a user's personally identifiable information from an ISP must obtain a grand jury subpoena based on a relevancy standard, and information obtained in violation of proper procedure must be suppressed.[154] The court affirmed that the fact that the subpoena issued by the municipal court was defective mandated suppression of evidence seized pursuant to it—namely, Reid's subscriber information.[155] The court noted, however, that Comcast's subscriber information existed independently of the faulty process

[148] *Id.* at 30.
[149] *Reid*, 945 A.2d at 30.
[150] *Id.*
[151] *Id.* at 27–28.
[152] *Id.* at 32–33.
[153] *Id.* at 33.
[154] *Id.* at 36–37.
[155] *Reid*, 945 A.2d at 37.

the police followed and that the tainted police conduct did not affect that information.[156] Thus, under those circumstances, the State could attempt to reacquire the information with a proper grand jury subpoena limited to seeking the user information for the IP address at issue.[157]

V. PROBLEMS AND SOLUTIONS TO INTERNET PRIVACY LAW

Reid represents a decision where everyone won. Defendant Reid won because the court recognized her interest in maintaining as private the information linked to her IP address.[158] The State won because it could reacquire through proper means the information it sought and it could continue to prosecute Reid.[159] New Jersey residents also won because they can continue to use the Internet with confidence that law enforcement cannot arbitrarily demand their personal information from an ISP, and if law enforcement violates this privacy right in obtaining such personal information, the information obtained may be subject to exclusion in a criminal trial.[160] Thus, *Reid* provided a realistic approach that embraced modern considerations of privacy interests in Internet use. Past federal decisions have not shown the same level of insight and balancing of interests as *Reid*.

Society's increasing reliance on the Internet for everyday activities is obvious.[161] Statistics place the number of Internet users in the United States at 231 million, or approximately seventy-five percent of the population.[162] Recognizing the importance the Internet holds in everyday life, the Supreme Court of New Jersey acknowledged that

---

[156] *Id.*

[157] *Id.* at 38.

[158] *See id.* at 33–34.

[159] *See id.* at 38.

[160] *See id.* at 37.

[161] *See Reid*, 945 A.2d at 33 ("[I]t is hard to overstate how important computers and the Internet have become to everyday, modern life.").

[162] *See* Cent. Intelligence Agency, The World Factbook, https://www.cia.gov/library/publications/the-world-factbook/geos/us.html (last visited June 22, 2010) (estimating the population of the United States at 310,232,863 people as of July 2010).

Internet users expect that their "identity will not be discovered through a string of numbers left behind" on a Web site.[163]

One might look at *Reid* and wonder whether the federal courts' approaches to answering Internet-privacy cases by applying the third-party doctrine of *United States v. Miller*[164]—which dealt with banks and bank records—was proper. Was it appropriate to compare the information held by an ISP to the information held and used by a bank? Or did this analogy simply offer federal judges with a quick and easy way to deal with the oftentimes confusing venue of Internet privacy?[165] Those who are comfortable with Internet technology might realize that the legal doctrines and analogies established before the mid-1990s do not neatly lend themselves to issues of Internet privacy. Furthermore, the statutory provisions available to Internet users to protect the users from disclosure of their personal information by an ISP are insufficient relative to the importance of Internet use in today's society.

A. Limited Remedies Available Following an Unlawful Search

Internet users who become the subject of a search of their ISP's records have few remedies should law enforcement illegally obtain this information. First, the traditional remedy of suppression of unlawfully seized evidence under the Fourth Amendment is generally not available.[166] In a criminal trial, the government cannot generally proffer in its case-in-chief evidence obtained in violation of the defendant's Fourth Amendment rights.[167] If, however, the area of governmental intrusion falls outside of the scope of Fourth Amendment

[163] *Reid*, 945 A.2d at 35.

[164] 425 U.S. 435 (1976).

[165] Federal courts have routinely applied the third-party doctrine to hold that an Internet user has no Fourth Amendment privacy expectation in the information linked to her IP address. *See* cases cited *supra* note 13.

[166] *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008); United States v. D'Andrea, 497 F. Supp. 2d 117, 121 (D. Mass. 2007); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 183 (D. Conn. 2005); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005).

[167] *See* Mapp v. Ohio, 367 U.S. 643, 655 (1961) (holding that evidence obtained in violation of the Fourth Amendment may not be used in criminal prosecutions in state courts); Weeks v. United States, 232 U.S. 383, 398 (1914).

protection, the defendant may not challenge the intrusion.[168] Consequently, the defendant cannot seek suppression of the evidence in a criminal trial.[169] With the federal courts' announcement that Internet users' expectations of privacy in the subscriber information held by their ISP is not an area protected by the Fourth Amendment, users cannot seek to have information obtained by law enforcement through unlawful methods suppressed at a criminal trial.

Second, Internet users have no remedies for suppression through the SCA because the few remedies the SCA does offer are limited and provide virtually no protection to a defendant in the criminal courtroom.[170] If law enforcement deviates from the procedures set forth in § 2703, an individual harmed may bring an action against the United States for damages and reasonably incurred litigation costs.[171] This, however, is the exclusive remedy against the government available under the SCA.[172] The SCA does not provide for suppression in a criminal trial of evidence obtained in violation of its provisions,[173] and federal courts have refused to read suppression as a remedy into the SCA.[174]

---

[168] *See generally* Rakas v. Illinois, 439 U.S. 128, 139–41 (1978) (holding that the proper analysis to determine whether a defendant may challenge a search focuses on the extent of the defendant's substantive Fourth Amendment rights rather than on the question of standing).

[169] *See id.* at 134 (holding that "since the exclusionary rule is an attempt to effectuate the guarantees of the Fourth Amendment, . . . it is proper to permit only defendants whose Fourth Amendment rights have been violated to benefit from the rule's protections" (internal citations omitted)).

[170] *See* 18 U.S.C. § 2712(a) (2006).

[171] *See id.*

[172] *See* § 2712(e). Remedies in the form of civil actions are also limited. Section 2703(e) restricts the use of civil actions by a subscriber against an ISP. § 2703(e). It prohibits an aggrieved person from bringing a civil action against an ISP who provided law enforcement with information in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification. *Id.* Section 2707 allows an aggrieved person to bring a civil action for injunctive or declaratory relief, damages, and reasonable attorney's fees and other litigation costs incurred only where the ISP knowingly or intentionally violated the provisions of the SCA. § 2707.

[173] 18 *U.S.C.* § 2708 (2006) ("The remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter.").

[174] *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1202 (10th Cir. 2008); *see also* United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); United States v. Smith, 155 F.3d 1051, 1056 (9th Cir. 1998); Bansal v. Russ, 513 F. Supp. 2d 264, 282–83

With no threat of suppression under the Fourth Amendment and no statutorily mandated suppression, little remains to deter law enforcement from deviating from the requirements of the SCA when it seeks information from an ISP. As a result, those who subscribe to an Internet service are at risk that law enforcement will obtain their personal information without regard to playing by the rules.

B. Shortcomings of the Stored Communications Act

The SCA fails to adequately protect an Internet user's privacy interests because it lacks suitable guidance for the courts to follow when interpreting the statute. For example, it distinguishes between a "record or other information pertaining to a subscriber" under § 2703(c)(1) and the list of items available to law enforcement under § 2703(c)(2) (which includes the subscriber's name, address, phone numbers, IP address, and credit card or bank account information), but the statute fails to explain how these two categories are different.

Furthermore, the SCA distinguishes between content and non-content in an Internet communication,[175] but it does not provide the courts with clear guidance to determine the *difference* between content and non-content in light of changing technology.[176] For example, law enforcement could locate a blog post, which undoubtedly contains content, obtain the IP address of the computer that sent the post, and then require the ISP to provide the missing link—the blogger's name and address. This is how law enforcement links non-content, which is easy to obtain through the SCA, to content, which generally requires a warrant or a court order.[177]

Courts have struggled to understand the SCA. The U.S. Court of Appeals for the Fifth Circuit expressed its frustration that "[u]nderstanding the [SCA] requires understanding and applying its many technical terms as defined by the Act, as well as engaging in painstaking, methodical analysis."[178] The Ninth Circuit expressed similar dissatisfaction, complaining that "the existing statutory

(E.D. Pa. 2007); United States v. Sherr, 400 F. Supp. 2d 843, 848 (D. Md. 2005); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

[175] *See* 18 U.S.C. § 2703 (2006).

[176] *See In re* Pen Register & Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 759 (S.D. Tex. 2005) (suggesting that parts of the SCA are "murky").

[177] *See* § 2703(a), (b)(1)(A).

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

framework is ill-suited to address modern forms of communication."[179] The court concluded that "until Congress brings the laws in line with modern technology," protection of the Internet and Web sites "will remain a confusing and uncertain area of the law."[180]

Scholar Orin Kerr suggests that the SCA provides sufficient protections to Internet users because it places limits on the ability of an ISP to disclose subscriber information, whereas the Fourth Amendment does not.[181] The "limit" imposed on the government before it can obtain personal information on an Internet subscriber, however, is negligible—it merely requires the government to serve an administrative subpoena to the ISP.[182] An administrative subpoena requires no showing of probable cause by law enforcement; the information sought need only be "relevant" to an authorized law enforcement inquiry.[183] Should law enforcement fail to meet this minimal requirement, very little is available in the way of remedies to the party whose privacy interests were violated.[184] Furthermore, Congress has not updated the SCA quickly enough to reflect modern Internet use, and thus, the SCA has failed to keep pace with the rapid development of Internet communications. For example, although § 2703 has been amended several times since its inception, most of the amendments have *reduced* subscriber privacy protections and made it *easier* for law enforcement to obtain subscriber information from an ISP.[185] In 1986 the drafters of the SCA surely could not have envisioned the de-

[179] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002).

[180] *Id.*

[181] Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 45 HASTINGS L.J. 805, 816 (2003) (claiming that the privacy protections offered by the ECPA exceed those offered by constitutional standards).

[182] *See* § 2703(c)(2).

[183] *Id.* § 3486(a)(1)(C)(i). Section 3486 controls the issuance of administrative subpoenas for the investigation of a federal offense involving the sexual exploitation or abuse of children. § 3486(a)(1)(A)(i)(II). A subpoena issued to an ISP in the context of the SCA must not extend beyond the information listed under § 2703(c)(2), which this Comment refers to as "detailed subscriber information." *See* § 3486(a)(1)(C)(i).

[184] *See supra* Part V.A.

[185] *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No.107-56, §§ 209(2), 210, 212(b)(1), 220(a)(1), (b), 115 Stat. 283, 285, 291, 292 (codified as amended in scattered sections of 8, 15, 18, 22, 31, 42, 49, and 50 U.S.C.).

velopment of open wireless networks on nearly every suburban street corner and the cell phones equipped with full Internet access that are commonplace today. The opportunities and means for individuals to communicate via the Internet will only continue to grow.

Some scholars, perhaps in an effort to simplify the explanation of the difference between the content and the non-content portions of an Internet communication, compare an Internet communication to a letter sent via the postal service.[186] The content portion of the communication is akin to the letter located inside the envelope, and the non-content portion of the communication—the header—is akin to the destination address and return address found on the outside of the envelope.[187] This analogy is flawed. First, many Internet users are likely *unaware* that their IP address is embedded in every mouse click that they make across the Internet. And second, most Internet users could not likely disable their IP address from appearing as part of an Internet communication. Yet almost everyone knows how to drop an anonymous letter with no return address into a mailbox.

Rather than providing Internet users with broad privacy protection, the SCA has done the opposite. It has evolved into a powerful tool on which law enforcement relies to gain access to an Internet user's personal information.[188] It has given law enforcement broad liberties to search Internet-based communications by defining electronic privacy narrowly and by reducing the required showing by the government to obtain information from an ISP.[189]

---

[186] *See* Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 611–16 (2003) ("[E]very communications network features two types of information: the contents of communications, and the addressing and routing information that the networks use to deliver the contents of communications. The former is 'content information,' and the latter is 'envelope information.' The essential distinction between content and envelope information remains constant across different technologies, from postal mail to e-mail.").

[187] *See id.* at 611 ("The envelope information is the information derived from the outside of the envelope, including the mailing and return addresses, the stamp and postmark, and the size and weight of the envelope when sealed.").

[188] *See* JAMES A. ADAMS, NAT'L INST. FOR TRIAL ADVOCACY, COMMENTARY, 18 U.S.C.S. prec. § 2701 (LexisNexis 2008) ("In addition to attempting to breach the shield of computer privacy by a search for stored electronic information on individual computers or through Internet Service Providers, the Government is now using computers as a sword to obtain, compare and store information about individuals.").

[189] *See* United States v. Polizzi, 549 F. Supp. 2d 308, 388 (E.D.N.Y. 2008), *vacated*, 564 F.3d 142 (2d Cir. 2009).

C. Problems with Past Precedent

Early decisions that addressed whether Internet users have a reasonable expectation of privacy in the subscriber information held by their ISPs may have been flawed for two reasons. First, the judges who decided some of the earliest cases—which ended up providing precedent for subsequent decisions—may have had an insufficient working knowledge of Internet technology necessary to reach an informed decision. Second, the courts relied on doctrines that were ill suited to answer the question of whether Internet users maintained an expectation of privacy in the information held by their ISPs. Those early court decisions thus provided inadequate constraints on unwanted governmental prying.

1. Wrestling with the Technology

The judges who decided some of the earliest Internet privacy cases may have lacked a solid understanding of the technology necessary to make an informed decision. Many judges generally did not have experience with Internet technology, and thus, cases involving Internet issues were likely more difficult to decide.[190] Courts that did not understand fully the technology on which they were asked to rule may have created unworkable rules.[191]

Many courts admitted their shortcomings in the area of new technology. In 1999 the district court judge in *Hambrick* acknowledged the "difficult" task of analyzing "previously unadjudicated situations in the world of cyberspace."[192] The Appellate Division of the New Jersey Superior Court self-consciously stumbled on the technology in its *Reid* decision by concluding that because the defendant used an "anonymous ISP address," she "manifested an intention to keep her identity publicly anonymous. She could have used her own name or some other ISP address that would have readily revealed her

---

[190] *See* Orin Kerr, *Internet Accounts and Probable Cause to Search a Home*, THE VOLOKH CONSPIRACY, Aug. 18, 2005, http://volokh.com/posts/1124409198.shtml.

[191] *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 879 (2004).

[192] United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 2000 U.S. App. LEXIS 18665 (4th Cir. Aug. 3, 2000) (per curiam).

identity, but she did not."[193] The court appeared to confuse the ISP-assigned IP address with a user-selected screen name.

Some judges are not shy about admitting their lack of experience in handling technically challenging Internet cases. They even "pride themselves on their lack of technological skills and wear it like a badge of honor."[194] One judge cited "an acknowledged dearth of technological savvy on the part of the undersigned" as a reason to refrain from elaborating on the possible definitions of "contents" in the context of the Pen Register Statute.[195] Many of the lawyers who tried early Internet cases may not have helped either because, as Orin Kerr claims, they were no more prepared to handle the technically complex Internet cases than the judges were to hear them.[196]

Kerr argues that legislatures are in a better position than the courts to provide privacy protection for areas affected by new technologies.[197] According to Kerr, whereas cases involving "stable" technologies (such as automobiles) tend to be regulated by the courts under the Fourth Amendment, cases involving new "technologies tend to be regulated by statute."[198] Why is this so? Do federal courts consciously avoid deciding technology issues and defer the development of technology-based privacy law to the legislature? While it may be difficult to answer that question, one fact remains: as a result of

---

[193] State v. Reid, 914 A.2d 310, 317 (N.J. Super. Ct. App. Div. 2007), *aff'd, modified, and remanded*, 945 A.2d 26 (N.J. 2008). This fact was noted with some amusement by a Wired Network Blogger who aptly noted that defendant Reid did not "'choose' anonymity since she made no attempt to mask her 'ISP address[.'] Maybe she ignorantly thought she was anonymous, but she certainly wasn't." Ryan Singel, *Jerseyites Have Right to Protect "ISP Address,"* WIRED.COM, Jan. 23, 2007, http://blog.wired.com/27bstroke6/2007/01/jerseyites_have.html.

[194] Donald E. Shelton, *Teaching Technology to Judges*, 40 JUDGES J. 42, 42 (2001).

[195] *In re* U.S. for an Order Authorizing the Use of a Pen Register & Trap on [xxx] Internet Service Account/User Name [xxxxxxxx@xxx.com], 396 F. Supp. 2d 45, 49 (D. Mass. 2005) ("There may be other examples of instances in which 'dialing, routing, addressing and signaling information,' reveals the 'contents' of communications as 'contents' is defined. Due to time constraints . . . and an acknowledged dearth of technological savvy on the part of the undersigned, the Court will not at this time try to identify and discuss them.").

[196] *See* KERR, *supra* note 38, at 423 ("[C]omputer technologies are new, and relatively few lawyers are sufficiently knowledgeable about them to raise creative challenges to government practices.").

[197] *See* Kerr, *supra* note 191, at 888.

[198] *Id.*

recent federal court decisions, large portions of Internet privacy protections have been carved out from the protections of the Fourth Amendment, and this leaves Internet users who desire greater privacy protections at the mercy of Congress. Furthermore, the courts cannot avoid interpreting the sometimes confusing and overwhelmingly technical statutes that touch Internet-privacy issues. Thus, Kerr's suggestion that "courts should be wary of imposing broad privacy protections against the government's use of new technologies"[199] is not necessarily the proper solution. The better choice is for courts to become more fluent with Internet technology and how it potentially affects an individual's privacy interests. This responsibility also flows to the attorneys who are trying cases and who have the opportunity to educate the bench via briefs and oral arguments.

2. Criticisms of *Katz* and *Miller*

The foundation of Internet privacy jurisprudence—*Katz* and *Miller*—has left modern Internet users on a weak footing when it comes to protecting privacy interests. One widely recognized problem with Justice Harlan's *Katz* test is that the second prong of the test—which requires a showing that the privacy interest sought is one that society recognizes as reasonable—may never be met in a particular area if the government or the Supreme Court were to announce that society no longer has any privacy interest in that area.[200] For example, homeowners generally enjoy an expectation of privacy in the contents of their garages. In this hypothetical, Congress could, in an interest to crack down on the growing problem of car thefts, enact a new statute that allows federal agents to search private garages at any time. Under the new statute, homeowners would quickly adjust to the idea that their garages were no longer private, and thus, the second prong of the *Katz* test would never be met if a homeowner challenged a search of a private garage.[201] Justice Scalia referred to the *Katz* test as "self-indulgent" because, "unsurprisingly, those actual (subjective) expectations of privacy that society is prepared to recog-

[199] *Id.*

[200] *See* Smith v. Maryland, 442 U.S. 735, 741 n.5 (1979) (noting that "where an individual's subjective expectations had been 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms," those subjective expectations cannot play a meaningful role in determining the scope of Fourth Amendment protection).

[201] Justice Blackman used a hypothetical similar to this in *Smith*. *Id.*

nize as reasonable bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable."[202] The same could be true of the expectations of privacy that Congress considers reasonable. Simply an applicable statute can suggest whether an expectation of privacy in a particular area is reasonable.[203] Thus, Congress can inform the courts that an individual has no reasonable expectation of privacy in a particular area by enacting a statute that indicates as much.[204]

Over twenty years after *Miller* was decided, courts rekindled the *Miller* rule to hold that the government's use of an IP address to obtain an Internet subscriber's personal information from the subscriber's ISP did not amount to a "search" and thus received no Fourth Amendment protection.[205] Federal courts have stubbornly refused to discard the third-party doctrine from *Miller* when evaluating Internet privacy cases and by doing so have announced that an ISP is just like a bank.[206] But in *Miller*, part of the Court's reasoning derived from the fact that Congress *had already eliminated* a bank user's expectation of privacy when it enacted the Bank Secrecy Act.[207] The Bank Secrecy Act required banks to maintain records and provide to law enforcement certain reports that would "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings."[208] Thus, when the *Miller* Court considered the question of the constitutionality of the Bank Secrecy Act, Justice Douglas aptly predicted in his dissent that "[i]t would be highly useful to governmental espionage to have like reports from all our bookstores, all our hardware and retail

[202] Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (internal quotes and citation omitted).

[203] *See* United States v. Polizzi, 549 F. Supp. 2d 308, 388 (E.D.N.Y. 2008) (explaining that applicable statutes can suggest whether an expectation of privacy is reasonable), *vacated*, 564 F.3d 142 (2d Cir. 2009).

[204] *See id.* ("[T]he ECPA grants the government broad liberty to search online materials by defining electronic privacy narrowly.").

[205] *See, e.g.*, Guest v. Leis, 255 F.3d 325 (6th Cir. 2001); United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *12 (4th Cir. Aug. 3, 2000).

[206] *See, e.g.*, cases cited *supra* note 128.

[207] *See* United States v. Miller, 425 U.S. 435, 442 (1976).

[208] Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 26 (1974) (quoting 12 U.S.C. §§ 1829b(a)(2), 1951 (1970); 31 U.S.C. § 1051 (1970) (current version at 31 U.S.C. § 5311 (2006))).

stores, all our drugstores. These records too might be 'useful' in criminal investigations."[209]

Many states have diverged from *Miller* and concluded that, on the basis of their state constitutions, bank customers have an expectation that their bank records will remain private.[210] One court referred to the doctrines developed by the federal courts as "extraordinarily restrictive" and having the "effect, if not the purpose, of placing a large percentage of illegal [searches] beyond the scrutiny of the courts."[211] The Supreme Court of New Jersey recognized that "the advent of modern technology, coupled with the ubiquity of commercial banking, underscores both the ability of prying government eyes to obtain bank records and the need to protect ordinary citizens' financial privacy in ways that promote fairness."[212]

For these same reasons, courts should refrain from applying the third-party doctrine from *Miller* when law enforcement seeks subscriber information from an ISP based on an IP address. While it is true that Internet subscribers do knowingly expose personally identifiable information to their ISPs, the same is not true for their IP ad-

---

[209] *Id.* at 84–85 (Douglas, J., dissenting).

[210] *See, e.g.*, Burrows v. Superior Court, 529 P.2d 590, 594 (Cal. 1974) (holding that a bank customer's reasonable expectation is that, absent compulsion by legal process, the matters he reveals to the bank will be used by the bank only for internal banking purposes); Charnes v. Digiacomo, 612 P.2d 1117, 1122 (Colo. 1980) (holding that taxpayer bank depositor has a reasonable expectation of privacy in the bank records of his financial transactions); Winfield v. Div. of Pari-Mutuel Wagering, Dep't of Bus. Regulation, 477 So. 2d 544, 548 (Fla. 1985) (recognizing an individual's legitimate expectation of privacy in financial-institution records); State v. Thompson, 745 P.2d 1087, 1096 (Idaho Ct. App. 1987) (noting that "services of banks, like those of telephone companies, are indispensable in today's business environment" and that "the disclosure of information to telephone companies or banks ought not to be treated as an abdication of a privacy interest"); People v. Jackson, 452 N.E.2d 85, 88–89 (Ill. App. Ct. 1983) (rejecting *Miller* and noting that "[s]ince it is virtually impossible to participate in the economic life of contemporary society without maintaining an account with a bank, opening a bank account is not entirely volitional and should not be seen as conduct which constitutes a waiver of an expectation of privacy"); State v. McAllister, 875 A.2d 866, 875 (N.J. 2005) (same); Commonwealth v. DeJohn, 403 A.2d 1283, 1291 (Pa. 1979) (holding that bank customers have a legitimate expectation of privacy in records pertaining to their affairs kept at the bank); State v. Thompson, 810 P.2d 415 (Utah 1991) (same); State v. Popenhagen, 749 N.W.2d 611, 632 (Wis. 2008) (holding that suppression of defendant's bank records is an appropriate remedy when the bank records were obtained in violation of a state statute).

[211] *Thompson*, 810 P.2d at 420 (Zimmerman, J., concurring).

[212] *McAllister*, 875 A.2d at 875.

dresses. An Internet subscriber cannot "knowingly expose to the public" something of which the subscriber is unaware. The ISP (not the subscriber) generates and assigns the IP address, and the subscriber has no control over the process.[213] The IP address associated with an Internet subscriber is like an envelope with no return address—inherently anonymous.[214] This is why the third-party doctrine does not provide a workable framework for Internet cases. As one court stated,

> The long history of the third-party doctrine—removing constitutional protection to information disclosed to a third party on the ground that the third party has the technical ability to disclose the information to the government—may not be compatible with the typical expectations of the general populace, notwithstanding its sophistication and computer savviness.[215]

Unlike the expectations for communications sent via postal mail, which are still sorted manually at the local post office and hand delivered by a carrier, the typical expectations of the general populace using the Internet today do not include the expectation that a live human handles each communication individually. And unlike a typical face-to-face transaction that occurs at a local bank when customers walk in to cash a paycheck, make a deposit, or simply inquire as to their account balance, Internet subscribers likely believe that their electronic communications do not involve any contact with a human but are instead controlled by switches, routers, and other computers. Even Google assures Gmail users that "no humans" are involved in its generation of targeted advertisements, which are based on keywords located in the body of a Gmail message.[216] When an Internet user

[213] Advanced Internet users seeking privacy have figured out ways to mask their IP address by use of "anonymizing" software or third-party proxy servers such as PrivateProxy. *See* PrivateProxy, http://www.privateproxysoftware.com/anonymous_proxy_personal.html (last visited June 14, 2010) ("Every time you connect to the Internet, you leave an electronic trail. This trail leads back to your door. Protect yourself by using an anonymous proxy to change your IP address. By using Private Proxy, you can surf anonymously on the Internet. The trail will lead to us and not you!").

[214] *See* United States v. Polizzi, 549 F. Supp. 2d 308, 390 (E.D.N.Y. 2008) ("IP 'addresses' are generally considered envelope—not content—information."), *vacated*, 564 F.3d 142 (2d Cir. 2009).

[215] *Id.* at 397.

[216] *See* Google Privacy FAQ, http://www.google.com/privacy_faq.html#toc-gmail-ads (last visited June 14, 2009) (Google uses "software to scan for keywords in users' emails which we can then use to match ads. When a user opens an email message,

"communicates" with a Web site, the *only* human involved is the one who types on the keyboard or clicks with the mouse. For these reasons, the third-party doctrine from *Miller* should not apply to Internet communications.

3. Inadequate Constraints on Government Prying

A court's conclusion that no reasonable expectation of privacy exists in a particular area has dire consequences, not just for the defendant in a criminal trial but also for the rest of society. As more government activity falls outside of the scope of Fourth Amendment protection, society suffers through a reduction of security and liberties. Justice Marshall predicted that "unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide."[217] Scholar Daniel S. Solove suggested that harmful consequences would result from "[i]nadequately constrained government information-gathering."[218] Those harms include a "slow creep toward a totalitarian state," a chill in democratic activities, and interference with the right of self-determination.[219] In the context of Internet use, federal court opinions fail to recognize that most people expect to use the Internet without the fear that law enforcement may arbitrarily track their usage.

Once a privacy interest falls outside of the protection of the Fourth Amendment, violations of that interest are no longer subject to the exclusionary rule.[220] Without an exclusionary rule, the incentive for law enforcement to adhere to proper methods of obtaining information is nearly eliminated. Law enforcement may very well take matters into its own hands, and yet the criminal defendant will have no standing to challenge the government's improper conduct.[221]

computers scan the text and then instantaneously display relevant information. . . . The whole process is automated and involves no humans.").

[217] Smith v. Maryland, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting).

[218] Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1084 (2002).

[219] *Id.* at 1084–85.

[220] *See* Weeks v. United States, 232 U.S. 383, 395–96 (1914).

[221] *See* United States v. Salvucci, 448 U.S. 83, 95 (1980) (holding that an illegal search conducted by law enforcement through use of a defective warrant may only be challenged by a person with a legitimate expectation of privacy in the invaded place); United States v. Payner, 447 U.S. 727, 731–32 (1980) (finding no Fourth Amend-

The result is not just harmful to the defendant in the particular case but to society as a whole. New Jersey's decision in *State v. Reid* recognized that the exclusionary rule helps deter police misconduct and encourages respect for protected rights.[222] Because the statutory regimes enacted by Congress to fill the void left by the inapplicability of the Fourth Amendment are "woefully inadequate,"[223] modern Internet users are left with very little protection against unwanted government prying.

D. Solutions for the Future: Rethink "Content" Under the SCA

As suggested above, courts deciding Internet privacy cases should aim to better understand the technology and avoid reflexively applying last century's third-party doctrine. Additionally, courts should consider more closely the delicate link between content and identity before allowing that link to be broken with a mere administrative subpoena.

The SCA requires that if law enforcement already has the name and personal information of an Internet subscriber and now wishes to obtain the contents of that subscriber's Internet-based communication, it must provide a search warrant pursuant to the Federal Rules of Criminal Procedure or an equivalent state search warrant.[224] But when law enforcement starts with the contents of a communication made by an anonymous Internet user and wishes to link that content to a subscriber record to obtain the user's identity, it only needs to prepare an administrative subpoena.[225] In the first scenario, the link between content and identity is protected by the requirement of a search warrant supported by probable cause, but in the second scenario, it is not. The solution to this dichotomy is to rethink the meaning of "content" under the SCA.

---

ment standing to challenge illegal search where defendant's bank records were illegally obtained by law enforcement upon breaking into a hotel room).

[222] State v. Reid, 945 A.2d 26, 37 (N.J. 2008).

[223] Solove, *supra* note 218, at 1138.

[224] *See* 18 U.S.C. § 2702(a)–(b) (2006) (requiring the government to obtain a search warrant prior to the disclosure of the contents of an electronic communication).

[225] § 2703(c)(2).

The Ninth Circuit has held that an "electronic communication" includes the transfer of data when an individual accesses a Web site.[226] The court considered the sequence of events and transmissions that occur between a subscriber and a Web site when the subscriber requests a particular Web site to load.[227] The court recognized that a Web site functions as an electronic communication because once the subscriber requests data from the Web site, the server transmits specific documents to the subscriber's computer.[228] The Web site owner transfers information (i.e., "contents" of the Web site) to the subscriber via one of the methods listed in the ECPA's definition of "electronic communication."[229]

If the act of clicking on a Web site is an electronic communication, what portion of that communication is "content?" Under the SCA, "contents" includes any information concerning the substance, purport, or meaning of a communication.[230] An Internet user who logs in to her Earthlink e-mail account and sends a message to a friend that says "meet at 5 p.m. to collect the package" expects that the contents of this e-mail message ("meet at 5 p.m. to collect the package") will remain private. Likewise, when she uses Google to locate Web sites on "local home foreclosures" and clicks on the first item in the search results list but does nothing more than view the text and images from the Web page that appears on her monitor, she expects that her identity will not be revealed from simply viewing the page.

In both cases above, content-based information is involved. Most would recognize the content in the first example as the message "meet at 5 p.m. to collect the package." In the second example, the click on the search result created a communication between the subscriber and the Web site, with the text, images, and graphics flowing from the Web site back to the subscriber's computer making up the "substance, purport or meaning" of that communication. The contents of a Web site viewed by a subscriber can reveal extraordinarily private information about that individual that goes well beyond the

[226] Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002).

[227] *Id.*

[228] *Id.*

[229] *Id.*; *see also* § 2510(12) (defining "electronic communication").

[230] § 2510(8).

subscriber's name, address, or phone number. For example, law enforcement may make inferences after learning that a subscriber visited Web sites such as http://www.wikihow.com/Know-if-You-are-Pregnant; http://www.herpes.com/; or http://www.domesticviolence.org/questions-about-leaving/.

In *United States v. Forrester*, the Ninth Circuit recognized that the line between "content" and "non-content" in an Internet-based communication may not be as clear cut as *Smith* and *Katz* describe it to be.[231] The court was asked to consider the constitutionality of the government's real-time surveillance of a subscriber's Internet activity, which included monitoring the IP addresses of the Web sites the subscriber visited.[232] Comparing the real-time collection of IP addresses with the use of a pen register to collect phone numbers in *Smith v. Maryland*, the court held that the government's surveillance did not constitute a Fourth Amendment search because IP addresses only constitute addressing information and do not reveal any more about the underlying contents of a communication than does a phone number.[233] After claiming that *Smith* and *Katz* drew a "clear line" between unprotected addressing information and protected content, the court seemed to concede that the line is not so clear when it comes to Internet-based communications.[234] The court noted that a surveillance method that allowed the government to determine not only the IP address of a Web site but also the URL of a particular page within a Web site might be more "constitutionally" problematic because the URL identifies a particular document within the site and "thus reveals much more information about the person's Internet activity."[235] But *Forrester*'s distinction between the level of content that appears on the home page of a Web site compared to the content that could appear within a particular URL of the Web site is misplaced. While a URL does point to a specific page within an overall Web site, the home page of a Web site could just as easily contain a

[231] 512 F.3d 500, 510 n.6 (9th Cir. 2008).
[232] *Id.* at 505, 509–11.
[233] *Id.* at 510.
[234] *See id.*
[235] *Id.* at 510 n.6.

particular document that "reveals much more information about the person's Internet activity."[236]

In *Forrester*, the court recognized the potential privacy issue of connecting a known subscriber to particular content. Yet law enforcement frequently connects a subscriber to content but from the other direction. Law enforcement *starts* with the content by first identifying a particular Web page. It next obtains the IP address of the computer that was used to access that page, and finally it obtains from the ISP the subscriber information to whom the IP address is registered.[237]

Should the minimum required level of suspicion by law enforcement vary according to whether law enforcement needs to connect content to a subscriber or a subscriber to content? If the act of a subscriber viewing a particular Web site constitutes an electronic communication[238] and that communication includes content—the specific text, audio, graphic, or video files associated with the particular Web site—should not the government be required to obtain a warrant supported by probable cause (as opposed to a mere administrative subpoena) before it can connect the content of the communication to the subscriber? Anything less fails to protect an Internet subscriber's desire to retain privacy and anonymity in the Web sites the subscriber viewed. Thus, the government should be required to obtain a warrant or court order when it seeks the personally identifiable information on an Internet subscriber.

VI. CONCLUSION

No one can deny the important role that the Internet plays in everyday life. People rely on the Internet to communicate with business colleagues and life-long friends, pay bills, purchase books, learn about recent news events, and stay in touch with family members. And society expects privacy in using the Internet regardless of wheth-

[236] *Id.*

[237] *See, e.g.*, United States v. Polizzi, 549 F. Supp. 2d 308, 386–87 (E.D.N.Y. 2008) (describing how law enforcement first identified a particular Web site, obtained the access log records listing the IP addresses of 1900 different users who had logged onto the Web site, identified the ISPs to whom the IP addresses were registered, and finally administratively subpoenaed the ISPs to disclose the identities of the subscribers), *vacated*, 564 F.3d 142 (2d Cir. 2009).

[238] *See* Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (9th Cir. 2002).

er federal courts are willing to recognize such a privacy interest. The content of a Web site can reveal highly personal information about the individual who visits it, and the personally identifiable information attached to an IP address deserves greater privacy protections than federal courts and legislation presently allow. Courts should recognize that the first generation of Internet privacy decisions relied on antiquated doctrines and that these decisions might not help a modern court resolve privacy questions. Furthermore, the SCA does not provide a suitable substitute for Fourth Amendment protections because modern Internet use has outgrown the SCA's useful application.

New Jersey's decision in *State v. Reid* moved Internet privacy a step in the right direction. By recognizing that Internet users maintain an expectation of privacy in the subscriber information held by their ISPs, New Jersey reinstated Internet privacy without unduly frustrating law enforcement's goals of catching criminals. Federal courts ought to extract themselves from the rigid framework of the third-party doctrine and consider New Jersey's approach to protecting Internet users' interest in the privacy of their subscriber information held by their ISPs.