THE THIRD PARTY DOCTRINE REDUX: INTERNET SEARCH RECORDS AND THE CASE FOR A "CRAZY QUILT" OF FOURTH AMENDMENT PROTECTION

Matthew D. Lawless[1]

ABSTRACT

The dark secrets brought to light by America Online's recent exposure of 658,000 of its users' search records reveal both a societal expectation of privacy in Internet searches, and an increased likelihood that such information will be used as evidence in criminal proceedings. In the absence of a statutory suppression remedy, the only bar to those records becoming Exhibits A-Z is a Fourth Amendment that, while purporting to protect expectations of privacy society would deem reasonable, utterly fails to consider what society has said about Internet searches. Increasingly, this means that courts will be faced with a choice: uphold the third party doctrine to the letter of *Smith v. Maryland*—or protect those expectations of privacy, legal as well as technological, that society is prepared to recognize as reasonable. This Comment aims to facilitate judicial adoption of the latter by showcasing the antipodal treatment of Internet search records under the third party doctrine as against the "operational realities test," and providing support for a rights-based re-reading of the doctrine that would restore constitutional consistency.

[1] J.D. Candidate, Indiana University School of Law—Bloomington, 2008; M.A., Texas Tech University, 2005; B.A., Michigan State University, 2001. Thanks to Professors Fred Cate, Joshua Fairfield, and Susan Brenner, and my colleagues Mark Oram and Aaron Stucky, for comments and encouragement. All errors, as they say, are mine.

INTRODUCTION

[¶1] You may have heard this story about a young Florida couple.[2] They celebrated their wedding anniversary by taking a romantic walk along the beach. As they were walking, the husband suddenly felt his wife get tense; he noticed a man approaching them, wearing a cap and brandishing a pistol. The man seemed agitated and demanded money. Shots were fired. And the husband briefly lost consciousness. When he awoke, the husband discovered he had taken four shots to his upper body and his left hand. He found his wife face down, floating in the surf, dead of a bullet wound to the face. The weapon and the assailant were gone.

[¶2] In 2002, that was how Justin Barber described the events of the night his wife April was killed. On June, 24, 2006, a Florida jury told a much different story—it found Justin guilty of April's murder. Barber's motive, it turns out, echoes many a made-for-TV movie: he had a rocky marriage and had recently acquired a $2 million life insurance policy on his wife.[3] But the evidence against him was more *Minority Report* than trite TV plotline. Six months before April's death, Barber foreshadowed one of the gunshot wounds he would take on the night of the murder by using Google to search for "trauma cases gunshot right chest."[4] On the basis of this evidence, the jury found that Justin planned to shoot himself in order to make the crime look like a robbery, and that he used the Internet to research how to survive.[5]

[¶3] Justin Barber is not alone in expecting his Internet searches to remain private. In August 2006, in what the blogosphere dubbed a "Data Valdez,"[6] America Online published three

---

[2] *See* Dennis Murphy, *Murder in the moonlight*, MSNBC INTERACTIVE, (Sept 8, 2006), *at* http://www.msnbc.msn.com/id/14738060/.
[3] Harriet Ryan, *Fla. man convicted of killing his wife during faked mugging, now faces death*, COURT TV NEWS, (June 26, 2006), *at* http://www.courttv.com/trials/barber/062406_verdict_ctv.html.
[4] Murphy, *supra* note 1.
[5] Ryan, *supra* note 3.
[6] Derek Slater, *AOL's Data Valdez Violates Users' Privacy*, ELECTRONIC FRONTIER FOUNDATION, (August 07, 2006), *at* http://www.eff.org/deeplinks/archives/004865.php; *see also* AOL's Massive Data Leak, ELECTRONIC FRONTIER FOUNDATION, *at* http://www.eff.org/Privacy/AOL/ (last visited April 15, 2007).

months worth of search queries by 658,000 of its users.[7] These searches, while so far presenting no tragic endings, have brought to light plenty of dark secrets reminiscent of Barber's infamous Google query. Among the searches revealed were these: "how to tell your family you're a victim of incest," "how to kill your wife," "suicide by natural gas," "child porno," and "my baby's father physically abuses me."[8] These queries, published anonymously by AOL, are presently being identified with individuals across the country.[9] Thus, it is only a matter of time before one of those individuals (or someone else) has their Internet search records used as evidence of a crime.

[¶4] Against the backdrop of this increased use of Internet search records as criminal evidence, there is a corresponding void in privacy law: there is no applicable statutory suppression remedy. As non-contemporaneous electronic communications, Internet search records are governed by Title II of the Electronic Communications Privacy Act, a provision referred to as the Stored Communications Act (SCA).[10] That act, unlike its counterpart in Title I (the Wiretap Act), does not provide a suppression remedy for violations.[11] Without such a statutory remedy, the only bar to Internet search records being used as criminal evidence—whether they were obtained by wrongful exposure by AOL,[12] pursuant to a defective warrant or

---

[7] Jeremy Kirk, *Update: AOL reportedly released search data*, INFOWORLD, (August 07, 2006), *at* http://www.infoworld.com/article/06/08/07/HNaolsearchdata_1.html.
[8] Michael Barbaro & Tom Zeller Jr., *A Face Is Exposed for AOL Searcher No. 4417749*, N.Y. TIMES, August 9, 2006, at A1.
[9] *Id.*
[10] 18 U.S.C. §§ 2701-12.
[11] *Compare* 18 U.S.C. § 2515 *with* 18 U.S.C. § 2707; *see generally* Monica R. Shah, *The Case for a Statutory Suppression Remedy to Regulate Illegal Private Party Searches in Cyberspace*, 105 COLUM. L. REV. 250, 272 (2005) (arguing that a statutory exclusionary remedy is warranted for stored communications); *see also* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 807 (2003) (discussing a suppression remedy for contemporaneous communications); *see also* McVeigh v. Cohen, 983 F. Supp. 215, 220 (D.D.C. 1998) (reading a suppression remedy into the statute: "While the government makes much of the fact that § 2703 (c)(1)(B) does not provide a cause of action against the government, it is elementary that information obtained improperly can be suppressed where an individual's rights have been violated.").
[12] *See* Kirk, *supra* note 7.

subpoena,[13] or by otherwise exceeding the scope of law enforcement's authority[14]—is the Fourth Amendment.

[¶5] This reliance on constitutional law punctuates a present doctrinal tension. While the Fourth Amendment purports to protect the expectations of privacy society would deem reasonable, its preeminent test for assessing those expectations—the "third party" doctrine—fails to consider what society has said about Internet searches. Historically, societal expectations of privacy have been intertwined with both property and location; thus, having information in third-party hands coincided with a lack of an expectation of privacy, absent theft or other lack of consent.[15] But now, search information is given to third parties with every expectation of privacy: this expectation is codified in the Stored Communications Act[16]; revealed by AOL's leak of its customers' sensitive queries[17]; recognized by the Southern District of California in *Gonzalez v. Google*[18]; and reflected in the privacy policies between service providers (such as Google) and their users.[19] Thus, in order to give effect to search engine users' expectations, a retooling of the doctrine is required.

[¶6] The need for this doctrinal shift is highlighted by the constitutional treatment of Internet search records under the third party doctrine as compared to the "operational realities"

---

[13] *See, e.g.*, United States v. Hambrick, 55 F. Supp. 2d 504, 509 (D. Va. 1999) (ISP subscriber information, which also typically falls under the Stored Communications Act, was admitted despite a defective subpoena because there was no "reasonable expectation of privacy" in the information).
[14] *See, e.g.*, United States v. Maxwell, 45 M.J. 406, 416 (C.A.A.F. 1996) (finding the seizure of electronic files, in this case e-mail, far exceeded the plain language of the warrant).
[15] *See generally* Olmstead v. United States, 277 U.S. 438 (1928); United States v. Miller, 425 U.S. 435 (1976).
[16] 18 U.S.C. § 2706.
[17] *See* Kirk, *supra* note 7.
[18] Gonzales v. Google, Inc., 234 F.R.D. 674, 681 (N.D.C.A. 2006) (noting that Internet search records contain sensitive and identifiable information including names, social security numbers, and credit card numbers).
[19] *See, e.g.*, Google Privacy Policy, *at* http://www.google.com/privacypolicy.html, (last modified October 14, 2005) ("We will not collect or use sensitive information for purposes other than those described in this Policy and/or in the specific service notices, unless we have obtained your prior consent" and "We may share with third parties certain pieces of aggregated, non-personal information, such as the number of users who searched for a particular term, for example, or how many users clicked on a particular advertisement. Such information does not identify you individually.").

test. Because Internet searches are conducted from both work and from home, online search queries are simultaneously regulated by both of the Fourth Amendment privacy tests. The problem is, unlike with e-mail—which has received some constitutional privacy protection under both the third party doctrine and the "operational realities" test—the application of those tests to Internet search records produces results that turn the Fourth Amendment's core tenet of protecting expectations of privacy "society is prepared to recognize as 'reasonable'" on its head.[20] As it stands, the law would deny Fourth Amendment protection to Internet searches conducted at home, but might allow for Fourth Amendment protection of government employee Internet searches conducted at work. In other words, contrary to popular belief, the law labels expectations of privacy in Internet searches conducted from home a priori "unreasonable," while holding that the expectations of privacy in the same searches conducted at a government workplace may well be "reasonable."

[¶7] This Comment argues that the consistency between the Supreme Court tests and the Fourth Amendment aim of protecting reasonable expectations of privacy should be restored by reconsidering the third party doctrine's binary view of privacy. Part I outlines the historical context of Fourth Amendment information privacy law, and provides the framework for the Supreme Court's third party doctrine and "operational realities" test. Part II highlights the inconsistency between the third party doctrine treatment of Internet search records and societal expectations of privacy by showing the constitutional protection (or lack thereof) under each of the judicial tests. Part III argues that the Court's "operational realities" test is better suited to evaluating reasonable expectations of privacy, and it contends that the third party doctrine should be understood in operational realities terms by shifting the focus of the doctrine's knowledge element toward a *right* (a harmony of policy and practice) rather than a *capacity* to view

[20] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

information. It first anchors this understanding in the original third party doctrine cases; then explains how the content/envelope distinction supports that view; and finally, it explores the application of the rights-based approach in recent judicial decisions. Part IV concludes that while this non-traditional view of the third party doctrine may create a "crazy quilt" of Fourth Amendment protection, such a patchwork approach is necessary to preserve the Court's commitment to protecting societal expectations of privacy in Internet search records.

I. THE FOURTH AMENDMENT APPROACH TO INFORMATION PRIVACY

[¶8] The Fourth Amendment declares the right of people to be "secure in their persons, houses, papers, and effects" against unreasonable searches and seizures in the absence of a probable cause warrant.[21] This guarantee has historically provided Fourth Amendment protection coextensive with notions of property.[22] In 1967, the Supreme Court, at least rhetorically, shifted away from that paradigm when it stated in *United States v. Katz* that the "Fourth Amendment protects people not places."[23] In doing so, the court ushered in a new era of constitutional privacy protection that recognizes a Fourth Amendment interest where an individual has a "subjective expectation of privacy that society recognizes as reasonable."[24] To define when expectations of privacy are reasonable, the Supreme Court has since articulated two frameworks known as the "third party doctrine" and the "operational realities" test.[25]

---

[21] U.S. Const. amend. IV.
[22] Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 807 (2004); Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 905 (2004); *see, e.g.*, Olmstead v.United States, 277 U.S. 438, 438 (1928).
[23] *Katz*, 389 U.S. at 352.
[24] Kyllo v. United States, 533 U.S. 27, 33 (2001); *Katz*, 389 U.S. at 361 (Harlan, J. concurring); *see also* Robert S. Steere, *Keeping "Private E-Mail" Private: A Proposal to Modify the Electronic Communications Privacy Act*, 33 VAL. U.L. REV. 231, 241 (1998).
[25] *See, e.g.*, Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 527 (2006); *see also* Stephen E. Henderson, *Nothing New Under the Sun?: A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 517 (2005).

A. The Third Party Doctrine

[¶9] The third party doctrine provides that information "knowingly exposed" to a third party is not subject to Fourth Amendment protection because one "assumes the risk" that the third party will disclose that information to the government.[26] Under this test, constitutional privacy interests in information are both bright and binary. It does not matter if the information is exposed for a limited purpose, or in confidence; it matters only whether the individual should know the information was made available to another party.[27] This section describes the origin of the test, its knowledge requirement, and its exception known as the content/envelope distinction.

1. United States v. Miller and Smith v. Maryland

[¶10] *United States v. Miller* and *Smith v. Maryland* doctrinalized the notion that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party."[28] In *United States v. Miller*, federal law enforcement officials issued subpoenas to two banks to produce a customer's financial records.[29] The defendant contended this constituted a violation of his Fourth Amendment rights.[30] The Court disagreed: it held that the customer lacked a reasonable expectation of privacy in the financial records maintained by his bank, because those records where voluntary conveyed by the customer, and exposed to the bank's employees in the ordinary course of business.[31]

---

[26] *See* Solove, *supra* note 25, at 528; *see also* Philip H. Marcus, *A Fourth Amendment Gag Order – Upholding Third Party Searches at the Expense of First Amendment Freedom of Association Guarantees*, 47 U. PITT. L. REV. 257, 276 (1985).

[27] "Made available" is used loosely here, but this idea will be explored as the knowledge requirement later in this section. United States v. Miller, 425 U.S. 435, 442; *see also* Marcus, *supra* note 26, at 276.

[28] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[29] *Miller*, 425 U.S. at 436.

[30] *Id.* at 437.

[31] *Id.* at 438 ("all of the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business" and "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to government authorities.").

[¶11] *Smith v. Maryland* affirmed that proposition in a slightly different context. In that case, a robbery victim received threatening and obscene telephone calls from a man identifying himself as the robber.[32] Law enforcement officials subsequently used a pen/trap register at the phone company's headquarters to trace the calls dialed by the suspect at his home.[33] The evidence obtained implicated the suspect; charges were brought; and the defendant sought to have the evidence excluded on Fourth Amendment grounds.[34] The Court denied the defendant's motion, holding that individuals lack a reasonable expectation of privacy in the phone numbers they dial because people know they must convey that information to the phone company and thus "cannot harbor any general expectation that the numbers they dial will remain secret."[35]

[¶12] As these cases illustrate, Fourth Amendment privacy protection is denied through the third party doctrine wherever one has knowledge that the information in question is exposed to another party.[36]

2. The Knowledge Requirement

[¶13] The third party doctrine's knowledge requirement is perhaps most famously articulated in *Katz*. There, the Supreme Court admonished, "What a person *knowingly exposes* to the public . . . is not the subject of Fourth Amendment protection."[37] In recent years, a consensus has emerged regarding how this element is to be satisfied. The accepted understanding is that the third party doctrine requires knowledge of the mere technological

[32] *Smith*, 442 U.S. at 737.
[33] *Id.*
[34] *Id.*
[35] *Id.* at 743. In response to the Court's determination in *Smith* that there was no constitutional privacy interest in telephone numbers dialed, Congress recognized that there was a privacy interest in that information by enacting the Pen Register Act, 18 USC 3121(a), which provided a procedural hurdle (though a slight one) to law enforcement's installation and collection of information via a pen trap/register.
[36] *See generally* Sam Kamin, *The Private is Public: The Relevance of Private Actors in Defining the Fourth Amendment*, 46 B.C.L. REV. 83, 99 (2004); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 562 (1990); Randolph S. Sergent, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1181, 1187 (1995).
[37] *Katz*, 389 U.S. at 351.

capacity for exposure—not knowledge of the likelihood or actuality of such exposure—in order to make an expectation of privacy unreasonable.[38] Under such an approach, the focus is on the knowledge of the potential transfer of information, not the recipient's right to view that information.[39]

[¶14] Support for this proposition is found in *Smith*.[40] There, the Supreme Court insisted that it was immaterial that the telephone company did not keep records of its subscribers' telephone calls; the fact that the company might keep such records if it wanted, and that subscribers knew that the company might, was sufficient to make an expectation of privacy unreasonable.[41] In other words, its decision turned not on the whether the company elected to retain such information, but simply on whether the phone company "had facilities for recording" and was "free" to use them.[42]

[¶15] The bottom line of this technological capacity approach is that, with a single exception, no Fourth Amendment protection presently exists for widely adopted electronic communications.[43]

3. The Content/Envelope Distinction

[¶16] The exception to the third party doctrine is known as the "content/envelope" distinction.[44] This distinction enables courts to recognize that while a third party may have

---

[38] *See* Catherine Crump, *Data Retention: Privacy, Anonymity, and Accountability Online*, 56 STAN. L. REV. 191, 203 (2003) (Smith holds "that technological possibility determines what privacy expectations are reasonable."); W. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(B), at 507 (2d ed. 1987) ("Indeed, it is enough for the majority in Smith that the telephone company has the capacity to make a record of such relationships, even though the company has the good sense not to offend its subscribers by making or keeping those records for no reason.").

[39] *Id.*

[40] *Smith*, 442 U.S. at 745.

[41] *Id.*

[42] *Id.* ("The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not, in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record.")

[43] *See* Francisco J. Navarro, *United States v. Bach and the Fourth Amendment in Cyberspace*, 14 ALB. L.J. SCI. & TECH. 245, 251 (2003).

physical control over an individual's information, such control does not make all expectations of privacy unreasonable.[45] Rather, only information that the third party sees (i.e., envelope information) is unprotected, while information that is hidden from the third party (i.e., letter information) is covered by the Constitution. This section outlines the traditional-analogical view of the exception, explains why that understanding is ineffectual (at least for purposes of ascertaining constitutional protection of Internet search records), and presents an alternative view.

a) The Traditional-Analogical View

[¶17] Courts have employed the content/envelope distinction in the electronic communications context by analogizing the modern communication to the information contained either on the inside or outside of a letter. In *Katz*, for example, the Supreme Court referred to the audio information constituting the telephone call as "content." In *Smith*, on the other hand, the Court found that the telephone numbers transmitted by a pen/register device were "envelope" information. This distinction has more recently carried over into Internet Service Provider (ISP) subscriber information cases, where courts have denied Fourth Amendment protection by analogizing that information to the text displayed on the outside of a letter,[46] and to cases involving e-mail, where at least some courts have found the information to be content.[47]

---

[44] *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 (2003); Brian D. Kaiser, *Government Access to Transactional Information and Lack of Subscriber Notice*, 8 B.U.J. SCI. & TECH. L. 648, 676-678 (2002); Navarro, *supra* note 43, at 253.

[45] See Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1286 (2004) (explaining "ECPA largely tracks the distinction made by the Court in Smith v. Maryland, between what Kerr calls 'envelope' and 'content' information. Analogizing to postal mail, Kerr states that 'the content information is the letter itself, stored safely inside its envelope. 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.') (quoting Kerr, *supra* note 44, at 611-616).

[46] *See, e.g.*, United States v. Hambrick, 55 F. Supp. 2d 504, 509 (W.D. Va. 1999).

[47] *See, e.g.*, United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996).

b) Criticisms of a Literal Understanding

[¶18] Despite this judicial acceptance, a literal understanding of the content/envelope distinction is undesirable insofar as it lacks analytical power to predict Fourth Amendment protection of hard to analogize communications such as Internet search records.[48] Specifically, Internet search records bear no characteristics that would make them wholly analogous to either content or envelope information ex ante. While they might be considered equivalent to the telephone numbers collected in *Smith*, or to a telephone call conversation in *Katz*, such analogies can only be made by looking at the privacy interest in the specific search terms ex post.

[¶19] For example, if the Internet query was for "AIDS," the communication might be considered content; and, if the Internet search was for, say, "Pizza Hut," the search might be considered envelope information. Aside from its potential to coexist with a suppression remedy, that analysis is ultimately academic: it is of dubious value to judge the content of a letter in order to determine if it is "content" information rather than "envelope" information because the privacy interest is already violated by making that inquiry.

c) A Messenger/Recipient View

[¶20] A better way to understand the content/envelope distinction is therefore required. One understanding that avoids the aforementioned criticism, and apprehends the case law, is to focus on whom the information is intended for; in other words, a better understanding of the content/envelope distinction is to view it as a distinction between the messenger and the recipient. Under this framework, envelope information exists where the information is disclosed

[48] Moreover, the content-qua-content test is impractical: anything worth the attention of law enforcement would invariably be something a court could find to be envelope information under that test because the harm is already done and the defendant is unsympathetic.

to the deliverer of the message, and content information exists where the information is disclosed to the intended recipient of the message.[49]

[¶21] This recipient/messenger understanding of the content/envelope distinction can be seen in the seminal third party doctrine cases of *Katz*, *Miller* and *Smith*. In *Katz*, the defendant was found to have a reasonable expectation of privacy in his conversation, even though the information was by definition knowingly exposed to a third party (the person on the other end of the telephone line), because it was not the recipient who disclosed that information to the government.[50] Conversely, in *Miller* and *Smith*, the intended recipients of the information were the parties that disclosed the information to the government, thereby eliminating any reasonable expectation of privacy. This view is consistent with the Supreme Court's language that individuals, by revealing their affairs to third parties, assume the risk that the information will be "conveyed **by that person** to law enforcement officials."[51] It is further confirmed by recent Fourth Amendment e-mail cases.

(1) E-Mail as Example

[¶22] The messenger/recipient distinction is clearly exhibited in the context of e-mail. If one sends an e-mail "to" America Online (AOL) for account assistance, AOL would be the recipient of the message; on the other hand, where AOL merely transmits the message and stores it on its server, it is not the recipient of the communication but its messenger.

[¶23] True to this understanding, courts find that individuals can have a reasonable expectation of privacy in their e-mail where someone other than the intended recipient of the communication discloses the message to the government. In one example, *United States v.*

[49] It is the relationship that is key.
[50] *Katz*, 389 U.S. at 352.
[51] Reporters Committee for Freedom of Press v. American Tel. & Tel. Co., 593 F.2d 1030, 1045 (D.C. Cir. 1978) (quoting *Miller*, 425 U.S. at 442-44).

Maxwell,[52] the scope of a search warrant was exceeded by the search of e-mails stored on AOL's server. The court employed the traditional explanation of the content/envelope distinction—that an e-mail message is analogous to a letter—to hold that the author of the e-mails had a reasonable expectation of privacy "until the transmissions are received."[53] In other words, the court found that because it was not the recipient of the message that disclosed the e-mail to the government, but rather AOL as the system administrator (or messenger), the sender could maintain a reasonable expectation of privacy in his message.

[¶24] Another example is provided by *Warshak v. United States*.[54] In that case, the government obtained an order under the Stored Communications Act directing NuVox Communications, an Internet Service Provider ("ISP"), to provide the Federal Bureau of Investigation with customer account information, including "e-mail communications received by the specified accounts that the owner or user of the accounts has already accessed, viewed, or downloaded."[55] The court found that regardless of the fact that personal emails were stored on a commercial ISP's server, and thereby exposed to a third party, the expectation of privacy in those emails was not per se unreasonable or "already . . . frustrated."[56] Again, where it was not the recipient who disclosed the information, the court found that the sender's expectation of privacy had at least the possibility of being reasonable.

---

[52] Maxwell, 45 M.J. at 417-18.

[53] *Id.* at 417-418 The *Maxwell* court explained that as when an individual "seals an envelope and addresses it to another person, the sender can reasonably expect the contents to remain private" so too the sender of e-mail may maintain a reasonable expectation of privacy "until the transmissions are received by another person." *Id.* at 417-18. Similarly, the maker of a telephone call has a reasonable expectation that police officials will not intercept and listen to the conversation; however, the conversation itself is held with the risk that one of the participants may reveal what is said to others. *Id.*at 418.

[54] Warshak v. United States, No. 1:06-cv-357, 2006 U.S. Dist. LEXIS 50076 (S.D. Ohio July 21, 2006).

[55] *Id.* at *3-4. However, the Court stated that while it was "prepared to reconsider its views upon the presentation of further evidence … it [was] not persuaded -- as an initial matter -- that an individual surrenders his reasonable expectation of privacy in his personal emails once he allows those emails (or electronic copies thereof) to be stored on a subscriber account maintained on the server of a commercial ISP." *Id.*at *19.

[56] *Id.* at 16 (quoting United States v. Jacobsen, 466 U.S. 109, 117 (1984)).

[¶25] On the other hand, courts find that individuals hold no reasonable expectation of privacy in their e-mail where the intended recipient of the communication discloses the message to the government.[57] In *United States v. Charbonneau*,[58] the court found no reasonable expectation of privacy to exist where the recipient of the e-mail was an undercover agent.[59] Likewise, in *Commonwealth v. Proetto*,[60] the court held that there was no reasonable expectation of privacy in e-mail messages sent by a man to a 15-year-old girl, where the girl reported the incidents to the police department, and provided the police with electronic copies of the incriminating messages.[61]

[¶26] The third party doctrine, through these basic rules, thus serves as the preeminent test for evaluating the reasonableness of expectations of privacy in information under the Fourth Amendment. Only in the narrow realm of the governmental workplace is there alternative Fourth Amendment treatment through what is known as the "operational realities" test.

B. The "Operational Realities" Test

[¶27] The Fourth Amendment inheres with some disparity in the employment context. In the private sector, courts apply the third party doctrine to assess, and invariably preclude, reasonable expectations of employee privacy.[62] In the public sector, or where private employers act at the behest of government officials in conducting a search of an employee, courts disregard

---

[57] *See, e.g.*, United States v. Jones, 149 F. App'x 954, 960 (11th Cir. 2005); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001); Maxwell, 45 M.J. at 418.
[58] United States v. Charbonneau, 979 F. Supp. 1177 (S.D. Ohio 1997).
[59] *Id.* at 1185.
[60] Commonwealth v. Proetto, 771 A.2d 823 (Pa. Super. Ct. 2001), *aff'd* 837 A.2d 1163 (Pa. 2003).
[61] *Id.* at 826, 831.
[62] *See, e.g.*, Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) (holding that once employee communicated information to his supervisor over a company e-mail system "any reasonable expectation of privacy was lost"); *see also* McLaren v. Microsoft Corp., No. 05-97-00824, 1999 WL 339015, at *4 (Tex. App. May 28, 1999) (finding employee had no reasonable expectation of privacy in e-mail messages transmitted over the network that "were at some point accessible by a third-party"); Garrity v. John Hancock Mut. Life Ins. Co., 2002 WL 974676,at *2 (D. Mass. May 7, 2002) (finding that e-mails sent over company intranet system were not private).

the third party doctrine and instead apply the "operational realities" test.[63] This section explains the origins of that test and its subsequent application to electronic communications.

1. Origin in O'Connor v. Ortega

[¶28] The Supreme Court's landmark "operational realities" decision is *O'Connor v. Ortega*.[64] In that case, a hospital undertook an investigation of one of its doctors, including a search of the doctor's office and a seizure of several items[65]. The doctor brought suit alleging violation of his Fourth Amendment rights after his employment was terminated.[66] In holding that the doctor had a reasonable expectation of privacy in his office, filing cabinet, and desk, the Court explained that reasonable expectations of privacy are judged according to the "operational realities"—the policies and practices—of the governmental employer's workplace.[67]

2. Application to Electronic Communications

[¶29] Since *O'Connor*, the "operational realities" test has been used to evaluate workplace expectations of privacy in electronic communications under the Fourth Amendment. Despite the race to the bottom anticipated by permitting governmental employers to define the reasonableness of employee expectations of privacy, courts have found several such expectations in the workplace to be reasonable. In one example, *United States v. Long*,[68] the United States Court of Appeals for the Armed Forces found that an employee had a reasonable expectation of privacy in her e-mails, which were sent and stored on her employer's computer, because a log-in banner warned only of routine monitoring, and the e-mails were uncovered in the process of monitoring for the specific purpose of exposing misconduct.[69] The court held that under the

[63] O'Connor v. Ortega, 480 U.S. 709, 717 (1987).
[64] *Id.*
[65] *Id.* at 713-14
[66] *Id.*.
[67] *Id.* at 717, 719.
[68] United States v. Long, 64 M.J. 57 (C.A.A.F. 2006).
[69] *Id.* at 64-65.

"operational realities" test the employee reasonably could have expected her e-mails to remain private because the workplace policy assured employees that only routine monitoring would be conducted.[70]

[¶30] Similarly, in *Quon v. Arch Wireless Operating Co.*,[71] the court found workplace practices dispositive of Fourth Amendment protection for text messages.[72] In that case, the defendant had been informed that the City considered the use of pagers to fall within its e-mail policy, and that it would monitor the use of those pagers, including auditing what messages were sent and received by employees at any time.[73] Despite notice of that policy, the court held that an employee had a reasonable expectation of privacy in the contents of his text messages because the "operational reality" was transformed by his supervisor's conscious decision not to enforce the written policy.[74]

[¶31] By considering such negotiated or relational restrictions on the exposure of information, rather than simply considering the technological capacity for exposure, the "operational realities" test provides Fourth Amendment protection where it would be precluded by the third party doctrine. This variance, as highlighted by the use of Internet searches

[70] *Id.*
[71] Quon v. Arch Wireless Operating Co., 445 F. Supp. 2d 1116 (C.D. Cal. 2006).
[72] *Id.* at 1148.
[73] *Id.* at 1124.
[74] In particular, Lt. Duke made it clear to Quon and other employees that he would not audit their pagers so long as they agreed to pay for any overages. *Id.*at 1148; *see also* United States v. Slanina, 283 F.3d 670, 677 (5th Cir. 2002) ("given the absence of a city policy placing Slanina on notice that his computer usage would be monitored and the lack of any indication that other employees had routine access to his computer, we hold that Slanina's expectation of privacy was reasonable"), vacated on other grounds by 537 U.S. 802 (2002), *on appeal after remand* 359 F.3d 356 (5th Cir. 2004) (per curium); Leventhal v. Knapek, 266 F.3d 64, 74 (2nd Cir. 2001) (finding that an employee had a reasonable expectation of privacy in "storing personal items in his office computer" despite employer's policy prohibiting personal use of state equipment, because the employer acknowledged that employees "would not violate state policies by keeping a personal checkbook in an office drawer, even though it would take up space there"); Adams v. City of Battle Creek, 250 F.3d 980, 984 (6th Cir. 2001) (finding no diminished expectation of privacy where a pager monitoring policy had not been enforced).

conducted in both contexts, helps to illustrate the tension between the third party doctrine and the reasonable expectations of privacy principle.[75]

II. ASSESSING INTERNET SEARCH RECORDS UNDER THE CURRENT PARADIGM

[¶32] The use of Internet search records as evidence in criminal proceedings raises important questions for information privacy law, most notably the availability of a suppression remedy under the Fourth Amendment.[76] Because Internet searches are conducted from both work and from home, the availability of such a remedy involves the application of both of the aforementioned Fourth Amendment privacy tests. This section applies those tests to Internet search records, explains the variance in constitutional protection, and illustrates the incompatibility of the third party doctrine with the Fourth Amendment tenet of protecting subjective expectations of privacy that society would find reasonable.

A. No Protection Under the Third Party Doctrine

[¶33] The third party doctrine currently precludes Fourth Amendment protection of Internet search records because users know the information is exposed online, and search strings are unlikely to be considered content. When a user enters a search string, they know—because they can see—that the information has been passed along: they provide a search string, hit Enter, and the Web page displays results based on the entered information. Not only is the information knowingly given to the search engine, it is visibly propagated to third party advertisers.[77] If a user enters "AIDS" she might get an ad for www.results.org, an activist website soliciting

[75] *Cf.* Lopez v. United States, 373 U.S. 427, 449 (1963) (Brennan, J., dissenting) ("The right of privacy would mean little if it were limited to a person's solitary thoughts, and so fostered secretiveness. It must embrace a concept of the liberty of one's communications, and historically it has.")
[76] *See generally* Gonzales v. Google, Inc., 234 F.R.D. 674, 687 (N.D. Cal. 2006) (noting that Internet search records contain identifiable information including names, social security numbers, and credit card numbers, and they often implicate criminal intentions; e.g., "bomb placement white house," or "communist berkeley parade route protest war.")
[77] *See, e.g.*, Google Toolbar, *at* http://toolbar.google.com

donations.[78] If she enters "Pizza Hut" she might get an ad for www.freepizzaworld.com.[79] There is thus little doubt that courts will find the third party doctrine knowledge requirement to be satisfied.

[¶34] The question is whether Internet searches are "content" for purposes of the exception. It seems clear that they are not. If, as this Comment has argued, the content/envelope distinction rests on the intended identity of the third party, Internet searches can be no different than ISP subscriber information cases. In each instance, the recipient of the communication is, at least ostensibly, the service provider. Individuals disclose information to ISPs in order to obtain access to the Internet; and individuals disclose information to search engines in order to locate information on the Web. Consequently, there would be no Fourth Amendment protection for Internet search records under the third party doctrine because any disclosure of that information to the government would be done by a recipient of the communication, not a messenger.

B. Possible Protection Under the "Operational Realities" Test

[¶35] Under the "operational realities" test the result is different. The technology does not foreclose the possibility of Fourth Amendment protection; rather, such protection is determined according to the broader situational context. Thus, in *United States v. Simons*,[80] the court found no privacy interest in an employee's Internet search records where an employer posted a privacy disclaimer regarding computer files.[81] It concluded that remote searches of the defendant's computer did not violate his Fourth Amendment rights because the employer's

[78] *See, e.g.*, http://www.google.com/search?hl=en&q=aids, (last visited April 15, 2007). Also, the fact that these are likely only computer recipients, see Kerr, *supra* note 44, at 609 (discussing computer recipients versus human recipients), heightens the expectation of privacy, a fact wholly ignored by the traditional technological capacity approach of the third party doctrine. *See generally* Bradley v. Google, Inc., No. C 06-05289, 2006 U.S. Dist. LEXIS 94455 (N.D. Cal. Dec. 22, 2006) (discussing third party advertising through Google); *and* Google Inc. v. Am. Blind & Wallpaper Factory, Inc., No. C 03-05340,2005 U.S. Dist. LEXIS 6228 (N.D. Cal. Mar. 30, 2005) (same).
[79] *See, e.g.*, http://www.google.com/search?hl=en&q=pizza+hut&btnG=Search, (last visited April 15, 2007).
[80] United States v. Simons, 206 F.3d 392 (4th Cir. 2000).
[81] *Id.* at 398-99.

policy made any expectation of privacy in the files downloaded from the Internet unreasonable.[82] Similarly, in *Muick v. Glenayre Elecs*,[83] the 2nd Circuit found that an employer's notice that it could inspect employee laptops rendered illegitimate any expectation of privacy the employee may have had in the computer.[84]

[¶36] More recently, the 9th Circuit's reissued opinion in *United States v. Ziegler*,[85] appears to appreciate a Fourth Amendment interest in Internet search records located on an employee's computer.[86] In its original opinion, the court found that the "Frontline policy entitl[ing] its personnel to administrative access to the employees' computers was an "operational realit[y] of [Ziegler's] workplace [that] diminished his legitimate privacy expectations."[87] Now, however, the court recognizes a constitutional interest in Ziegler's computer because the computer was located in a non-public, locked office.[88] It essentially finds that the location of the computer in a private office is more relevant to determining the reasonableness of Ziegler's expectation of privacy in his computer than Frontline's workplace policy permitting its monitoring of employee computers.[89]

[¶37] These cases thus illustrate the basic difference between the "operational realities" test and the third part doctrine—dimensionality. The "operational realities" test provides the possibility of Fourth Amendment protection by looking at the policies and agreements

---

[82] *Id.*
[83] Muick v. Glenayre Elec., 280 F.3d 741, 743 (7th Cir. 2002).
[84] *Id.* ("But Glenayre had announced that it could inspect the laptops that it furnished for the use of its employees, and this destroyed any reasonable expectation of privacy that Muick might have had and so scotches his claim.")
[85] United States v. Ziegler, 474 F.3d 1184, 1186 (9th Cir. 2007) ("A review of Ziegler's 'search engine cache information' also disclosed that he had searched for 'things like 'preteen girls' and 'underage girls.'")
[86] *Id.* at 1189-90.
[87] United States v. Ziegler, 456 F.3d 1138, 1142-43 n.9 (9th Cir. 2006) (quoting United States v. Simons, 206 F.3d 392, 399.
[88] Ziegler, 456 F.3d at 1190 ("Furthermore, Ziegler's expectation of privacy in his office was reasonable on the facts of this case. His office was not shared by co-workers, and kept locked.")
[89] *Ziegler*, 474 F.3d at 1189-93. It should be noted that the court then used that workplace policy to find that Frontline had the authority to consent to a government search, thus complying with (and effectively overriding) Ziegler's Fourth Amendment interest.

concerning the information—as well as, following *O'Connor*, the location of the property holding the information—while the third party doctrine denies protection prior to any such analysis by considering only whether the party should have known the information was potentially exposed to someone else.

C. The Resulting Fourth Amendment Fracture

[¶38] The Fourth Amendment protection of Internet search records is thus currently something of a paradox in privacy law. While the modern understanding of the Fourth Amendment is that it protects expectations of privacy that "society would deem reasonable," two tests the Supreme Court has developed to assess this reasonableness are now positioned to achieve results contrary to general societal expectations of privacy in electronic communications: it is now possible to "expect" more privacy in Internet searches while working at a government office than at home.[90] These differences are particularly salient considering that the home has forever been the bastion of constitutional privacy under the Fourth Amendment, and that government workplaces include military workplaces, where commanders can authorize searches of employees, order them confined, and even bring criminal charges against them.[91]

[¶39] Imagine that Justin Barber used Google to search for "trauma cases gunshot right chest" using his work computer, and that he worked at a government organization that gave employees significant privacy with respect to their use of the Internet. As it stands, the law might provide Barber with a suppression remedy for his Internet search records under *O'Connor*'s "operational realities" test, yet he would almost certainly receive no Fourth

[90] The upshot of these competing constitutional tests is that public employers now have the sole power to cause Internet searches to be excluded as evidence in criminal prosecutions by implementing policies that permit employees to maintain reasonable expectations of privacy in that information; this is not to suggest, however, that they will actually ever do so. *See, e.g.*, *Muick*, 280 F.3d at 743 (explaining "the abuse of access to workplace computers is so common (workers being prone to use them as media of gossip, titillation, and other entertainment and distraction) that reserving a right of inspection is so far from being unreasonable that the failure to do so might well be thought irresponsible.")

[91] *Olmstead*, 277 U.S. at 438; *Long*, 64 M.J. at 57.

Amendment protection if he conducted his Internet search using his home computer because of the third party doctrine.[92] To put this contrast in even sharper relief: the law would presently seem to recognize the privacy of Internet searches at home only in the ironic circumstance of someone performing those searches using their employer's computer.[93]

[¶40] While the government workplace may require a test that captures the unique privacy interest attendant with physical property in a semi-public environment, it is difficult to see how such differential treatment is justified for information transmitted on the Internet.[94] The risk in either case—both at home and at work—is the exposure of remotely stored electronic search information by the third party to law enforcement. Simply because an employer might also use that search information for internal investigations of misconduct, while an Internet search engine will not, the ultimate expectation in each instance is that the information will not fall into police hands—otherwise why have one constitutional test for the public workplace and another for the private one? Given that equanimity of risk, it is unclear as a practical matter why a forced contractual relationship with a government employer justifies the possibility of a reasonable expectation of privacy, while a freely entered contract with a search engine is held to be unreasonable, wholly irrespective of the terms governing the latter relationship.

III. RESTORING CONSTITUTIONAL CONSISTENCY

[¶41] To restore constitutional consistency—such that reasonable expectations of privacy in Internet search records are aligned with judicial outcomes—courts should reconsider the continuing validity of the third party doctrine's binary approach to information privacy. As it is, the third party doctrine gives effect to the criticism often aimed at the "reasonable expectation of

[92] In truth, it would not have mattered in Barber's case because the government obtained a warrant.
[93] Again, this would depend on many operational factors.
[94] Consider that the "operational realities" test was articulated in a case involving physical not informational privacy. See *O'Connor*, 480 U.S. at 709.

privacy" principle, by holding that individuals can only reasonably expect privacy where the Court gives them that privacy.[95] Because the third party doctrine fails to address true societal expectations of privacy (as evident by its failure to protect any information entered into a search engine), it reinforces the privacy norms of a politically and temporally insulated judiciary: once people know their searches are exposed, then—by the time these cases are contested—there will, in truth, be no expectation of privacy.

[¶42] The Supreme Court's more recently advanced "operational realities" test outlines a better constitutional approach to information privacy. By looking at the broad reality of the circumstances—a latitude that is especially significant when the communication is governed by privacy agreements, and might reasonably be viewed as communication with a computer instead of a person—that test provides a way to capture legitimate community expectations of privacy. This section argues that the third party doctrine should be understood in "operational realities" terms.

A. The Case for an "Operational Realities" View of the Third Party Doctrine

[¶43] The third party doctrine can be reconciled with the "operational realities" test by shifting the focus of its knowledge requirement away from technological capacity and toward a right to view information.[96] Such an approach would dispel the Court's present binary view of information privacy under the third party doctrine, and place an increased emphasis on the agreements and relationships between the parties. Thus, if an individual could rely on her

[95] Kyllo v. United States, 533 U.S. 27, 34 (2001) ("The Katz test -- whether the individual has an expectation of privacy that society is prepared to recognize as reasonable -- has often been criticized as circular, and hence subjective and unpredictable."); *see also* 1 WAYNE R.LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.1(d), at 393-394 (3d ed. 1996); Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 (1979).

[96] This approach is similar in kind to those adopted by other advocates of relational understandings of Fourth Amendment information privacy. *See, e.g.*, Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. POL'Y 211, 247 (2006); *See generally*, Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593 (1987).

awareness of a privacy agreement promising that information will not be read or disclosed to others (as individuals do in the "operational realities" cases), there would necessarily be no knowing exposure under a "right to view" interpretation of the third party doctrine's knowledge requirement. The following subsections summarize the support for this view.

1. Reconsidering Katz, Miller, and Smith

[¶44] The "operational realities" approach to the third party doctrine has significant precedential justification. Consider once more the seminal cases of *Katz*, *Miller*, and *Smith*.[97] In *Katz*, the defendant occupied a telephone booth, shut the door, paid the toll, and was thereby "entitled to assume that the words he [uttered] into the mouthpiece [would] not be broadcast to the world."[98] The nature of Katz's entitlement was such that, even though he technologically exposed his conversation to the phone company, he maintained a reasonable expectation of privacy in his conversation because he relied on the knowledge that it was not the phone company's practice to records its users' calls.[99] In other words, it would appear that the Court recognized the operational realities of Katz's phone call when it granted him Fourth Amendment privacy protection.[100]

[¶45] An "operational realities" understanding is similarly observable in *Miller*. In that case, there was no reasonable expectation of privacy where the customer's information was disclosed to the bank, whose practice was to share that information with its employees and use it to provide service to its customers. On these facts, one can conclude that it was not simply the technological capacity for exposure in *Miller*, but the "operational realities" of that exposure—

[97] For an excellent analysis of these cases in a similar vein *see* Brenner & Clarke, *supra* note 90.
[98] *Katz*, 389 U.S. at 352.
[99] *Id.*
[100] In fact, this would seem to make *Katz* bad law under *Smith*. *See* Crump, *supra* note 34, at 203. ("One has only to apply the logic of *Smith* to the scenario in *Katz* to see that this is the case. *Smith* holds that there is no Fourth Amendment protection for dialed phone numbers because the average person should be aware that their phone company is technically capable of accessing this information. If this Court had applied this logic in *Katz*, then surely the content of phone conversations would be similarly unprotected.") (citation omitted.)

the fact that the information was shared with and used by employees—that mattered for purposes of the Fourth Amendment.[101] This emphasis on the consensual use of information by third parties for business purposes, and not simply the fact that information has been exposed, is evident in a long line of cases.[102] The *Miller* Court's language to the contrary—that it makes no constitutional difference whether information is revealed "only for a limited purpose," or with an expectation that one's confidence in a third party "will not be betrayed"[103]—is simply a misapplication of case law involving personal interactions between undercover agents and suspected criminals.[104] As Susan Brenner and Leo Clarke have persuasively argued, there is a constitutionally significant difference between those cases—and that reasoning—and the use and storage of personal, electronic information by businesses.[105]

---

[101] Brenner & Clarke, *supra* note 90, at 214.

[102] *See, e.g.*, United States v. Covello, 410 F.2d 536, 542 (2d Cir. 1969) ("[T]he keeping of toll records is a *necessary part of the ordinary course of the telephone company's business* and is necessary in order that the company may substantiate its charges to its customers. Toll records are kept for all telephone subscribers and are not kept just for subscribers being investigated by officers of the law, or ones suspected of criminal proclivities. The subscriber is fully aware that such records will be made . . . and the records of the telephone company so kept in the ordinary course of the company's business are entitled to the same evidentiary treatment as the records of other businesses.") (emphasis added); United States v. Gallo, 123 F.2d 229, 231 (2d Cir. 1941) ("When a person takes up a telephone he . . . . must be deemed to consent to *whatever record the business convenience* of the company requires.") (emphasis added); *see also* Hambrick, 55 F. Supp. 2d at 505, *aff'd* 225 F.3d 656 (4th Cir. 2000), cert. denied, 531 U.S. 1099 (2001) (where the government served a subpoena on MindSpring, an Internet service provider, requesting "any records pertaining to the billing and/or user records documenting the subject using your services.").

[103] *Miller*, 425 U.S. at 443. ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.")

[104] United States v. White, 401 U.S. 745, 751-52 (1971); Hoffa v. United States, 385 U.S., 293, 302; Lopez v. United States, 373 U.S. 427 (1963).

[105] Brenner & Clarke, *supra* note 90, at 251 ("The reasoning in both Smith and Miller relied on cases such as United States v. Hoffa that dealt with verbal disclosures by one individual to other persons . . . . There is, however, a constitutionally significant factual distinction between Hoffa and Government access to stored digital transaction data. In the former situation, the individual who communicates with another person (i) knows what he has said, (ii) knows that the recipient is not only able, but likely, to evaluate the implications of the information transmitted, and (iii) knows that the recipient may decide, based on that evaluation, to disclose the information to others. The one who shares information with another individual is also likely to appreciate and rely on the limits of human memory and the cognitive constraints sociologists call 'bounded rationality.' The person who shares information also is likely, as a matter of empirical reality, to have some idea of what other information the recipient can combine with the information transmitted.")(citation omitted).

[¶46] The central barrier to an "operational realities" view of the third party doctrine is *Smith v. Maryland*.[106] A traditional reading of *Smith* would deny an "operational realities" understanding of the third party doctrine because the Court concluded that it made no constitutional difference whether the telephone company actually kept records of its customers' calls; it only mattered that the company could.[107] But let's look again at the language used by the Court. It refers to the phone company being "free to" make records of the call information—language that might well encompass not only the phone company's physical capacity to make such records, but also its legal right to do so.[108] The upshot of this observation is twofold. First, after *Smith*, Congress passed the Electronic Communications Privacy Act to restrict the disclosure of customer information by communications companies.[109] Thus now, unlike then, there are significant legal obstacles to disclosure that reflect and reinforce society's expectation of privacy—an expectation that is no doubt better reflected by the democratically-elected members of Congress, through its legislation, than by the Court through its decision.[110] Second, insofar as the Court's language contemplates the legal rights of the phone company to use the customer information, it could be said to adopt an operational realities view of information privacy. While such a reading is ultimately incompatible with the Court's stated rationale, "We

[106] Smith, 442 U.S. at 735.
[107] *Id.*
[108] *Id.* at 745 ("The fortuity of whether or not the phone company in fact elects to make a quasi-permanent record of a particular number dialed does not, in our view, make any constitutional difference. Regardless of the phone company's election, petitioner voluntarily conveyed to it information that it had facilities for recording and that it was free to record.").
[109] Electronic Communications Privacy Act of 2000, Digital Privacy Act of 2000 and Notice of Electronic Monitoring Act: Hearing on H.R. 4987, and H.R. 4908 Before the Subcommittee on the Constitution of the Committee on the Judiciary, House of Representatives, 106th Cong. 82 (2000), ("In 1986, in enacting the ECPA's Title II and Title III provisions, the Congress was aware of the foregoing Supreme Court rulings and sought to 'create' new privacy protection in statute to protect a subscriber's communications addressing and transactional record information."); *See generally* Lieutenant Colonel LeEllen Coacher, *Permitting Systems Protection Monitoring: When the Government Can Look and What It Can See*, 46 A.F. L. Rev. 155, 171 (1999) (noting "the ECPA was designed to confer an expectation of privacy to electronic and wire communications, and it generally prohibits the interception or accession of electronic communication.").
[110] 18 U.S.C. 2511; 18 U.S.C. 2701. Though, of course, the passage of the Bank Secrecy Act failed to substantiate a similar expectation (in the Court's view) in *Miller*.

are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the pattern of protection would be dictated by billing practices of a private corporation,"[111] the continuing validity of that rationale has been called into question by the more recent articulation of the "operational realities" test. To the extent that the Supreme Court's holding in *Smith* rests on that rationale it is arguably overruled by *O'Connor*. By defining reasonable expectations of privacy through the "operational realities" of the government workplace, *O'Connor* directly undercuts the Court's reasoning in *Smith* because it purposefully creates just such a "crazy quilt" within the public workplace.[112]

2. The Content/Envelope Distinction Focuses on Rights Not Capacity

[¶47] A rights-based approach to the third party doctrine is also supported by both the traditional-analogical and messenger views of the content/envelope distinction. Under each framework, the emphasis is on the right rather than the capacity to view information. When a letter is given to the post office for delivery, there is no physical guarantee of privacy. It is technologically possible for mail carriers, other postal workers, and even prying neighbors to readily view the content of anything ultimately deposited in a residential mail box. The only barrier to third party access to such information is a legal one.[113] The same is true for e-mail. While AOL, for example, would clearly have access to all electronic mail it delivers and stores, the mere existence of that access has not eliminated reasonable expectations of privacy in the content of e-mail messages.[114] This is because AOL, like the post office, is bound—legally, not

[111] Smith, 442 U.S. at 744.
[112] O'Connor, 480 U.S. at 709.
[113] *See generally* 18 U.S.C. 1708 (2000) ("Whoever steals ... from or out of any ... mail receptacle ... any letter, postal card, package, bag, or mail ... shall be fined under this title or imprisoned not more than five years, or both.").
[114] *See, e.g.*, *Warshak*, 2006 U.S. Dist. LEXIS at *50076.

physically—to uphold the privacy of the messages it delivers.[115] This rights-based approach to the third party doctrine is illustrated in several recent decisions.

3. Recent Judicial Recognition: Hambrick, Freedman, Maxwell

[¶48] An "operational realities" view of the third party doctrine can be seen in contemporary cases involving electronic communications. One such case is *United States v. Hambrick*.[116] In that case, the court denied the defendant's motion to suppress his Internet subscriber information, in part because the subscriber agreement between the defendant and MindSpring did not proscribe MindSpring from revealing the defendant's personal information to nongovernmental entities.[117] The court found that where there was no prohibition on the dissemination of information to third parties, there could be no reasonable expectation of privacy.[118]

[¶49] Another example is provided by *Freedman v. Am. Online, Inc.*[119] There, the court also considered the agreement between the subscriber and the ISP in assessing the reasonableness of the subscriber's expectation of privacy.[120] It held that the plaintiff had no objectively reasonable expectation of privacy because his contract with AOL permitted AOL to release subscriber information to non-governmental entities, and to governmental entities in limited circumstances.[121] Finally, *United States v. Maxwell* also illustrates this view.[122] In *Maxwell*, the court noted that it was AOL's policy not to read or disclose subscribers' e-mail to

[115] 18 U.S.C. § 2701.
[116] U.S. v. Hambrick, 55 F. Supp. 2d. 504, 508 (W.D. Va. 1999).
[117] *Id.*at 509.
[118] *Id.*.
[119] Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174 (D. Conn. 2005).
[120] *Id.* at 183 ("Where such dissemination of information to nongovernment entities is not prohibited, there can be no reasonable expectation of privacy in that information.") (quoting Hambrick, 55 F. Supp. at 509).
[121] *Id.* (noting that AOL's privacy policy with Plaintiff permitted AOL to reveal Plaintiff's subscriber information "where needed for delivering a product or service" and "to comply with valid legal process such as a search warrant, subpoena or court order, or in special cases such as a physical threat to you or others.").
[122] Maxwell, 45 M.J. at 417.

anyone except authorized users, and that AOL would only disclose the information to third parties if given a court order.[123] On that basis, the court found that the defendant's expectation of privacy was reasonable.[124]

[¶50] If the third party doctrine's knowledge element is treated merely as whether the information is knowingly technologically made available to a third party, it would be dispositive of a lack of Fourth Amendment protection in every one of these cases. There would be no need for the courts to consider the agreements between the service provider and the subscriber; those agreements would simply be irrelevant. But that is not what these courts did. Instead, they considered the operational reality of the privacy agreements between the parties and cited that reality to grant or deny Fourth Amendment protection of the information.

IV. CONCLUSION

[¶51] As the availability of a suppression remedy for Internet search records under the Fourth Amendment becomes increasingly relevant, courts will be faced with a choice: uphold the third party doctrine to the letter of *Smith*—or protect those expectations of privacy, legal as well as technological, that society is prepared to recognize as reasonable. In anticipation that courts may follow in the footsteps of *Freedman*, *Maxwell*, and *Hambrick* and choose the latter, this Comment has aimed to provide a justification for their decisions by marshaling support for an "operational realities" view of the Court's third party doctrine.

[¶52] It is unavoidable that this non-traditional view of the doctrine creates a "crazy quilt" of Fourth Amendment protection, and in so doing raises many questions about the future of Fourth Amendment privacy law: Will consumers negotiate for stronger privacy protection?

---

[123] *Id.* at 417 (holding while "implicit promises or contractual guarantees of privacy by commercial entities do not guarantee a constitutional expectation of privacy, we conclude that under the circumstances here appellant possessed a reasonable expectation of privacy, albeit a limited one, in the e-mail messages that he sent and/or received on AOL.").

[124] *Id.*

Will businesses, including search engines, enter into meaningful privacy agreements? Do other operational realities of such relationships diminish (already?) users' expectations of privacy? And what is to be made of a free market approach that allocates constitutional privacy protection according to individual negotiating power and ability?

[¶53] Whatever the answers to such questions may be, a patchwork approach is necessary if the preeminent Supreme Court test for assessing reasonable expectations of privacy in information is to be aligned with the actual expectations of privacy in Internet search records. Indeed, if actual societal expectations of privacy are what the Fourth Amendment truly protects—and not simply those expectations a nine member panel is willing to uphold—then such an approach to information privacy is perhaps even ideally suited to the task. How better to determine the expectations of privacy "society is prepared to recognize" as reasonable then by letting society do just that?[125]

[125] *Katz*, 389 U.S. at 361 (Harlan, J. concurring).