# ARE GOOGLE SEARCHES PRIVATE? AN ORIGINALIST INTERPRETATION OF THE FOURTH AMENDMENT IN ONLINE COMMUNICATION CASES

*By Jayni Foley*

In the United States, about ninety-seven million adults use the internet at least once per day.[1] On a typical day, thirty-eight percent of all Americans use a search engine to find information, thirty-one percent read news online, and thirty percent browse the internet for entertainment or leisure.[2] During this online activity, users leave "digital footprints" with their internet service provider (ISP) or search engine, revealing their interests, hobbies, or agendas.[3]

Over the past decade, the amount of personal information collected, stored, and shared by private companies has skyrocketed due to the rise of internet communication, decreased cost of data storage, and the emergence of data brokerage companies.[4] Increasingly, the government subpoenas private companies like America Online (AOL), eBay, and Google to access this information in order to fight and prevent crime.[5] However, these subpoenas are increasingly opposed on privacy grounds.[6]

In *Gonzales v. Google, Inc.*, the U.S. District Court for the Northern District of California rejected a federal government request for thousands of search query strings entered by Google search engine users that the

---



1. *See, e.g.*, Pew Internet & Am. Life Project, Daily Internet Activities, http://www.pewinternet.org/trends/Daily_internet_Activities_7.19.06.htm (last visited Mar. 23, 2007) ("According to [the] February-April 2006 survey, 66% of American adult internet users, about 97 million people, use the internet on an average day.").

2. *Id.*

3. *See, e.g.*, Google Privacy Center: Privacy Policy, Google Privacy FAQ, http://www.google.com/intl/en/privacy_faq.html (last visited Nov. 8, 2006) (describing the information recorded and stored in Google's server logs).

4. Nancy Libin, *Perspective: the anxious new dawn of cybersnooping*, CNET NEWS.COM, May 3, 2006, http://news.com.com/The+anxious+new+dawn+of+cybersnooping/2010-1028_3-6067598.html.

5. In 2005, four government agencies—the Department of Justice (DOJ), State Department, Homeland Security Department, and the Social Security Administration—spent roughly $30 million to purchase personal information from data brokers. *Id.*; *see also* Saul Hansell, *Online Trail Can Lead to Court*, N.Y. TIMES, Feb. 4, 2006, at C1.

6. *See* Fred von Lohmann, *Could Future Subpoenas Tie You to "Britney Spears Nude"?*, LAW.COM, Feb. 6, 2006, http://www.law.com/jsp/article.jsp?*id*= 1138961111185.

government claimed it needed to test filtering software for online pornography.[7] This incident exemplified the competing interests involved in government access to information about individuals held by third parties. While most internet users respect the government's need to fight terrorism and child pornography, they do not want to be wrongly flagged as terrorists or pornographers due to mischaracterizations of their digital footprints.[8] How can society prevent privacy intrusions while allowing law enforcement appropriate access to relevant information?

This Note analyzes privacy protections currently in place for internet searches and the interplay between these protections and law enforcement access. Part I provides an overview of the technological and regulatory background for search engines and ISPs. This Note focuses on Google because it is the world's most widely-used search engine.[9] Part II analyzes the constitutional and statutory framework for ISP and search engine privacy, focusing on the erosion of Fourth Amendment protection of information held by "third parties" such as Google. Additionally, it outlines statutory protections currently in place for ISP data under the Electronic Communication Privacy Act (ECPA). Part III examines the *Gonzales v. Google, Inc.* opinion as an example of the interplay among individual, business, and government interests. Part IV proposes that courts should adopt an originalist interpretation of the Fourth Amendment in deciding online communication cases. This interpretation is consistent with a reasonable expectation of privacy in information conveyed to third parties such as Google. Finally, Part V explores ECPA's statutory framework for electronic communications and advocates expanding its protections.

---

7. Gonzales v. Google, Inc., 234 F.R.D. 674, 678, 688 (N.D. Cal. 2006).

8. Doug Henschen, *Q&A: Got Data? Beware Privacy Pitfalls, Big Brother*, INTELLIGENT ENTERPRISES, Mar. 2006, http://www.intelligententerprise.com/showArticle.jhtml?articleID=177105304 (quoting Jim Dempsey of The Center for Democracy & Technology as stating, "I'm happy to fight pornography, but I'm unwilling to be wrongly labeled a pornographer. The issues have to do with inaccuracy, false positives, misinterpretation or misuse of data.").

9. Google's Opposition to the Government's Motion to Compel at 2, Gonzales v. Google, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 5:06-mc-80006-JW) [hereinafter Google Opp.]; Google Corporate Information: Quick Profile, http://www.google.com/corporate/facts.html (last visited Jan. 17, 2006).

# I. BACKGROUND: SEARCH ENGINES AND SUBPOENAS

## A. Technological Background

As of early 2006, about seventy-three percent of Americans use the internet.[10] Millions of internet users look to the web as their "information source of first resort,"[11] and more than seventy-three percent of American college students use the internet to gather information more than they use the library.[12] Google operates the world's most widely-used search engine at www.google.com, receiving about a billion search requests per day.[13] Google, like other search engines, functions by "crawling" the web and organizing content in a searchable web index.[14] When a user types a query, Google's proprietary technology produces a list of hyperlinks organized by relevance and reliability.[15]

Google treats information about its search queries and methods of indexing and returning URLs as confidential.[16] That noted, Google has the technology to list every search query ever sent from a specific IP address.[17] Google's online privacy policy states, "Like most Web sites, our

---

10. MARY MADDEN, PEW INTERNET & AM. LIFE PROJECT, INTERNET PENETRATION AND IMPACT (April 26, 2006), http://www.pewinternet.org/pdfs/PIP_Internet_Impact.pdf.

11. Peter Lyman, Archiving the World Wide Web, http://www.clir.org/pubs/reports/pub106/web.html (last visited Mar. 23, 2007).

12. STEVE JONES, PEW INTERNET & AM. LIFE PROJECT, THE INTERNET GOES TO COLLEGE: HOW STUDENTS ARE LIVING IN THE FUTURE WITH TODAY'S TECHNOLOGY 3 (2002), http://www. pewinternet.org/pdfs/PIP_College_Report.pdf.

13. Google Opp., *supra* note 9, at 2; Google Corporate Information: Quick Profile, http://www.google.com/corporate/facts.html (last visited Jan. 17, 2006). This Note focuses on Google's search engine because it is arguably the most well-known search engine in the United States.

14. Google Corporate Information, Technology Overview, http://www.google.com/corporate/tech.html (last visited Jan. 17, 2006); Searching the Google Directory, Excerpt from GOOGLEPEDIA: THE ULTIMATE GOOGLE RESOURCE, Aug. 28, 2006, http://www.quepublishing.com/articles/article.asp?p=606600&rl=1.

15. *Id.*

16. Google Opp., *supra* note 9, at 2 (citing Declaration of Matt Cutts, ¶ 6, Gonzales v. Google, 234 F.R.D. 674 (N.D. Cal. 2006) [hereinafter Cutts Decl.]).

17. Here is an example of a typical Google log entry where the search is for "cars," followed by a breakdown of its parts:

> 123.45.67.89 - 25/Mar/2003 10:15:32 - http:// www.google.com/search?q=cars- Firefox 1.0.7; Windows NT5.1-740674ce2123e969
> "123.45.67.89" is the IP address assigned to the user by the user's ISP; "25/Mar/2003 10:15:32" is the date and time of the query; "http://www.google.com/search?q=cars" is the requested URL, including the search query; "Firefox 1.0.7; Windows NT 5.1" is the browser and operating system being used; and; "740674ce2123a969" is the

servers automatically record . . . your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser."[18] Google also records which links users click after inputting search queries.[19] Google records this information in order to develop new products and services, display customized content and advertising, and ensure technical functionality.[20] Yahoo!, another leading search engine, has a similar privacy policy.[21]

Despite these companies' claims that they use this information to produce more and better products,[22] privacy advocates and users are concerned that this information may be increasingly targeted by law enforcement as well as private lawyers wielding subpoenas.[23] Google's privacy statement asserts that Google will protect "personal information," expressly defined to users as "information that you provide to us which personally identifies you, such as your name, e-mail address or billing information, or other data which can be reasonably linked to such information by Google."[24] Google states that it shares this information in limited situations, including when Google has a "good faith belief" that disclosure,

---

unique cookie ID assigned to this particular computer the first time it visited Google.

Google Privacy Center, Google Privacy FAQ, http://www.google.com/intl/en/privacy_faq.html (last visited Nov. 8, 2006).

18. *Id.*

19. Google Privacy Center, Google Privacy FAQ, What information does Google receive if I click on a link displayed on Google?, http://www.google.com/intl/en/privacy_faq.html (last visited Nov. 8, 2006); *see also* Google Search Privacy Notice, http://www.google.com/searchhistory/privacy.html (last visited Nov. 8, 2006) (stating that Google's "Personalized Search" feature records information including search queries, results clicked on, and the date and time of searches "in order to improve your search results and display your search history").

20. Google Privacy Center, Google Privacy Policy, Information we collect and how we use it, http://www.google.com/privacypolicy.html (last visited Nov. 13, 2006).

21. Yahoo! Privacy Policy, http://privacy.yahoo.com/privacy/us (last visited Nov. 17, 2006) ("Yahoo! automatically receives and records information on our server logs from your browser, including your IP address, Yahoo! cookie information, and the page you request.").

22. *See supra* notes 20, 21.

23. *See* von Lohmann, *supra* note 6. This Note focuses on government subpoenas only. Private subpoenas are beyond the scope of this Note.

24. Gonzales v. Google, Inc. 234 F.R.D. 674, 684 (N.D. Cal. 2006) (citing Second Declaration of Joel McElvain, Ex. C.); *see also*, Google Privacy Center, Google Privacy Policy, http://www.google.com/pri-vacypolicy.html (last visited Mar. 23, 2007) (stating that "personal information" is protected); Google Privacy Center, Google Privacy FAQ, http://www.google.com/privacy_faq.html (last visited Mar. 23, 2007).

access, use, or preservation of the information is "reasonably necessary" to:

> (a) satisfy any applicable law, regulation, legal process or enforceable governmental request, (b) enforce applicable Terms of Service, including investigation of potential violations thereof, (c) detect, prevent, or otherwise address fraud, security or technical issues, or (d) protect against imminent harm to the rights, property or safety of Google, its users or the public as required or permitted by law.[25]

Google states that it obeys the law and complies with enforceable government requests for information.[26] Therefore, in order to know precisely what kind of information is protected, one must know what kind of information the government can legally access.

The following Section notes the increased use of subpoenas for government access to online communications. Part II then addresses constitutional and statutory protection for electronic communications.

## B. Subpoenas of Search Engines and ISPs

### *1. Increasing Use of Third Party Subpoenas*

In this era of omnipresent technology, companies like Google manage comprehensive networks that can track users' activities. This practice has altered the way law enforcement approaches criminal investigations. Rather than search for discrete pieces of physical information, law enforcement can simply request bundles of information from private companies such as ISPs and search engines.[27] One high-profile example of using Google's records occurred in the Scott Peterson murder case, where prosecutors presented evidence on websites Peterson visited prior to his wife's death.[28]

---

25. Google Privacy Center, Google Privacy Policy, http://www.google.com/privacypolicy.html (last visited Nov. 13, 2006).

26. *Id.*

27. *See* Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6, 14-15 (2003).

28. The websites included maps of the San Francisco Bay, tidal charts, and fishing guides. Harriet Ryan, *Scott Peterson's Lawyer Strives to Throw Doubt on Phone Evidence*, COURTTVNEWS.COM, Aug. 6, 2004, http://www.courttv.com/trials/peterson/082604_ctv.html. These records were subpoenaed for use in a criminal investigation, unlike the civil litigation in question in *Gonzales v. Google, Inc.* This distinction is important: ECPA allows court orders for information when the government shows "specific and articulable facts showing that there are reasonable grounds to believe" the information sought is relevant and material to an ongoing criminal investigation. 18 U.S.C.

The New York Times recently reported that AOL receives more than 1,000 subpoenas each month seeking information about its users.[29] Most large internet and telephone companies now have formal processes in place for "subpoena management."[30] Information generally sought in subpoenas includes users' names, residence, when they were online, and—if a court issued a search warrant—what users have written and read in their e-mail or typed into their web browser.[31]

Subpoenas are convenient methods to obtain information because ISPs and search engines retain massive amounts of data. E-mail programs such as Google's Gmail advertise the benefit of users never having to throw anything away.[32] Rather than limit this data storage, as many privacy advocates advise, both the federal government and state governments are encouraging it.[33] In 2006, Attorneys General of forty-nine states requested that Congress adopt a national data retention requirement to aid law enforcement.[34] Similarly, U.S. Attorney General Alberto Gonzales and FBI Director Robert Mueller have indicated that ISPs should retain customer records for two years.[35]

### 2. *Subpoenas Require Only a Standard of Relevance*

In terms of information privacy, subpoenas afford weak protection; they are normally issued without prior judicial approval and are enforced on a mere showing of relevance.[36] The only limits on issuance of grand jury subpoenas are that they must seek relevant information and not be overbroad.[37] Government subpoenas for third-party information are gener-

---

§ 2703(d) (2006). Further, the Fourth Amendment "probable cause" standard was likely met when these records were subpoenaed.

29. Hansell, *supra* note 5.

30. *Id.*

31. *Id.*

32. *See* About Gmail, http://mail.google.com/mail/help/intl/en/about.html (last visited Oct. 28, 2006) ("over 2,600 megabytes of storage (and growing every day)").

33. As Professor Tim Wu articulated, Starbucks might improve its coffee by recording every conversation that takes place in its café, but Starbucks customers would be appalled at the thought. von Lohmann, *supra* note 6.

34. Declan McCullagh & Anne Broache, *Gonzales: ISPs must keep records on users*, CNET NEWS.COM, Sept. 19, 2006, http://news.com.com/Gonzales+ISPs+must+keep+records+on+users/2100-1028_3-6117455.html.

35. *Gonzales Wants ISPs to Save User Data*, TOWNHALL.COM, Sept. 20, 2006, http://www.townhall.com/News/NewsArticle.aspx?ContentGuid=202f0538-4011-4568-a902-ae69ddd51436.

36. *See* United States v. Morton Salt Co., 338 U.S. 632, 642-43 (1950); James X. Dempsey, *Digital Search & Seizure: Updating Privacy Protections to Keep Pace with Technology*, 865 PLI/PAT 505, 513 (June-July 2006).

37. Dempsey, *supra* note 36, at 540.

ally not protected under the Fourth Amendment, and thus do not require a showing of probable cause.[38]

When a subpoena is served on the subject of the investigation, that person has notice and can make a motion to quash or modify the subpoena for privilege, burdensomeness, or irrelevance.[39] However, third parties holding "personal" information may have little or no incentive to challenge a government subpoena, and have little or no obligation to inform the record subject that his or her information is sought.[40]

Because recent cases interpreting the Fourth Amendment do not extend protection to digital information such as internet searches or ISP subscriber information, most subpoenas are dictated only by a standard of relevance.[41] Part II discusses the cases that led to this lack of Fourth Amendment protection for third-party information. It also addresses statutory protections for internet data under ECPA.

## II. EROSION OF FOURTH AMENDMENT PROTECTION FOR THIRD-PARTY INFORMATION

The Fourth Amendment to the U.S. Constitution shields individuals from unreasonable government searches and seizures of their "persons, houses, papers, and effects."[42] In addition, federal law requires more stringent legal process to obtain certain types of information.[43] There are at

38. *See id.*; Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211, 229-30 (2006).

39. *See* Christopher Slobogin, *Subpoenas and Privacy*, 54 DEPAUL L. REV. 805, 806 (2005).

40. Dempsey, *supra* note 36, at 527.

41. Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999); *see also infra* Parts II and IV. Some subpoenas are regulated by statutes governing the type of information sought. For example, under the Electronic Communications Privacy Act (ECPA), the government can obtain ISP user logs by a grand jury or an administrative subpoena if the records are "relevant and material to an ongoing criminal investigation." 18 U.S.C. §§ 2703(c), (d) (2006); *see infra* Section II.B (explaining ECPA's standards for government subpoenas of electronic information).

42. U.S. CONST. amend. IV.

43. Many state statutes require more stringent legal process. State law as it pertains to electronic data is beyond the scope of this Note. For more information, see Stephen E. Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U.L. REV. 373 (2006).

least five federal legal standards for government access to electronic information. In order of descending stringency, these include:[44]

1) The very high "probable cause plus" standard for wiretaps;
2) The Fourth Amendment probable cause standard for basic search warrants;
3) The "specific and articulable facts giving reason to believe" standard for court orders for access to certain stored records;[45]
4) The certification of relevance standard for court orders for pen register and trap and trace devices; and
5) The relevance standard for subpoenas.

This Part first analyzes Fourth Amendment protections, focusing on Supreme Court cases decided prior to the internet. Second, it examines federal statutory protections for online information under ECPA.

### A. Fourth Amendment Jurisprudence

Historically, the Fourth Amendment provided protection against unwarranted government intrusion into private property and information.[46] Yet today, the Fourth Amendment offers little protection for information in the hands of third parties, and therefore little protection to internet and search engine users. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[47]

In 1967, the Supreme Court interpreted the Fourth Amendment to protect "reasonable expectations of privacy" in the landmark case, *Katz v.*

---

44. Dempsey, *supra* note 36, at 513.

45. 18 U.S.C. § 2703(d). Section II.B of this Note describes Title II of ECPA, the Stored Communications Act (SCA), codified at 18 U.S.C. §§ 2701-2711.

46. In *Mapp v. Ohio*, 367 U.S. 643 (1961), the Court held that in all criminal proceedings, evidence obtained in violation of the Fourth Amendment is excluded from evidence in criminal trials.

47. U.S. CONST. amend. IV.

*United States*.[48] In *Katz*, the Court held that the government's act of electronically listening to and recording Katz's conversation in a public telephone booth violated Katz's "reasonable expectation of privacy," and therefore, violated the Fourth Amendment.[49] The Court stated, "the Fourth Amendment protects people, not places . . . . [W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[50] Therefore, the government required a warrant supported by probable cause to access Katz's telephone conversation content because it constituted a "search" protected under the Fourth Amendment.

Justice Harlan's concurrence in *Katz* explained the circumstances in which one might "justifiably" have an expectation of privacy. Harlan described the appropriate inquiry as encompassing two questions: (1) whether the person exhibited an actual expectation of privacy (subjective prong); and (2) whether the expectation is one "that society is prepared to recognize as 'reasonable'" (objective prong).[51] Harlan's two-pronged analysis has been adopted in a number of subsequent cases.[52] In 2001, the Court in *Kyllo v. United States* used Harlan's test to hold that using sense-enhancing technology to obtain information about a home interior constituted a Fourth Amendment search and therefore required a warrant.[53]

Notwithstanding the continued relevance of Harlan's test, the Supreme Court curtailed Fourth Amendment protection in 1976 in *United States v. Miller*, holding that the Fourth Amendment does not cover instances where information is given to, or gathered by, third parties.[54] In *Miller*, the Court held that no "reasonable expectation of privacy" attached to financial records shared with private banks.[55] The Court distinguished "private

48. Katz v. United States, 389 U.S. 347, 360 (1967) (establishing the doctrine of "reasonable expectation of privacy").

49. *Id.* at 359.

50. *Id.* at 351.

51. *Id.* at 361 (Harlan, J., concurring).

52. *See, e.g.*, Bond v. United States, 529 U.S. 334, 340-41 (2000) (using *Katz* legitimate expectation of privacy inquiry); Minnesota v. Olson, 495 U.S. 91, 95 (1990) ("Since the decision in *Katz v. United States*, 389 U.S. 347 (1967), it has been the law that 'capacity to claim the protection of the Fourth Amendment depends . . . upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place.'"); United States v. Knotts, 460 U.S. 276, 285 (1983) (using *Katz* legitimate expectation of privacy inquiry).

53. Kyllo v. United States, 533 U.S. 27, 40 (2001); *see also infra* Part IV.

54. United States v. Miller, 425 U.S. 435 (1976).

55. *Miller*'s business record holding relied on an earlier case, *Couch v. United States*, 409 U.S. 322 (1973). *Id.* at 442 (citing *Couch*, 409 U.S. at 335). In *Couch*, the IRS issued a summons to compel an accountant to surrender records that Couch provided to the accountant for use in preparing Couch's tax return. The Court held that "there can be

papers" from "business papers," finding bank records to fall into the latter category.[56] In addition to its "business record" holding, the *Miller* Court introduced an assumption-of-risk analysis, not previously addressed in the business records cases.[57] The Court reasoned that Miller voluntarily revealed his financial information to a third party, the bank, and therefore "assumed the risk" that the bank could reveal this information to the government.[58] Broadly interpreted, *Miller* suggests that conveying documents to a third party, without regard to the type of documents or the purpose for which they were provided, eliminates an expectation of privacy in those documents.[59]

In 1979, in *Smith v. Maryland*, the Supreme Court followed *Miller's* assumption-of-risk holding and held that monitoring dialed phone numbers did not implicate the Fourth Amendment.[60] The Court reasoned that people generally do not have privacy expectations in the phone numbers they dial because they know the phone company uses the numbers for a variety of legitimate purposes.[61] As in *Miller*, the Court used broad language, stating "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[62] The Court concluded that because the numbers were captured at the phone company's central offices, the police did not intrude into a "constitutionally protected area."[63] The Court distinguished *Katz*, stating that the pen registers at issue in *Smith*, which capture numbers dialed, "do not acquire the 'contents' of communications," such as the conversation at issue in *Katz*.[64]

The *Miller* and *Smith* assumption-of-risk doctrine has been applied to ISP customer records to preclude Fourth Amendment privacy protection in this area. In *Guest v. Leis*, the Sixth Circuit held that ISP customers lacked a Fourth Amendment privacy interest in their ISP subscriber information "because they communicated it to the systems operators."[65] Similarly, in

---

little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return." *Couch*, 409 U.S. at 335.

56. *Miller*, 425 U.S. at 440-41, 445.

57. Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1402 (2004).

58. *See Miller*, 425 U.S. at 443.

59. Bellia, *supra* note 57, at 1402.

60. Smith v. Maryland, 442 U.S. 735, 742 (1979).

61. *Id.*

62. *Id.* at 743-44.

63. *Id.* at 741.

64. *Id.* at 747-48.

65. 255 F.3d 325, 336 (6th Cir. 2001).

*United States v. Kennedy*, the court held that the defendant did not have a Fourth Amendment privacy interest in his ISP subscriber information because when he entered into an agreement for internet service, he knowingly revealed the information to the ISP.[66] However, two military courts have found a reasonable expectation of privacy in stored e-mail messages.[67]

As the law currently stands, the broad "assumption-of-risk" language in *Miller* and *Smith* provides the basis for arguments that search engine users lack an expectation of privacy in communications held by search engines and ISPs.[68] Many legal scholars have criticized their application to online communications cases.[69] Part IV of this Note addresses the Fourth Amendment "legitimate expectation of privacy" as applied to search engine records and challenges the providence of applying *Miller* and *Smith* to online searches. First, Section II.B outlines the current federal statutory framework protecting electronic information.

### B. Statutory Protection: Electronic Communications Privacy Act (ECPA)

In 1986, Congress passed ECPA to clarify federal privacy protections in new and emerging technologies.[70] Since its passage, opportunities for government surveillance have expanded in ways not contemplated when ECPA was written.[71]

---

66. 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); *see also* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) (finding no Fourth Amendment protection in ISP records because the user "knowingly revealed his name, address, credit card number, and telephone number to Mindspring and its employees").

67. United States v. Long, 64 M.J. 57, 66-67 (C.A.A.F. 2006); United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) (finding reasonable expectation of privacy in e-mail files held by AOL).

68. *See* Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000).

69. *See, e.g.*, Bellia, *supra* note 57, at 1397-1413; Henderson, *supra* note 43; Slobogin, *supra* note 39; *infra* Part IV.

70. Electronic Communications Privacy Act, 18 U.S.C §§ 2510-2711 (2006). ECPA is structured in three sections: (1) Title I, the Wiretap Act; (2) Title II, the Stored Communications Act (SCA); and (3) Title III, the Pen Register Act. The Stored Communications Act is codified at 18 U.S.C. §§ 2701-2711 (2000 & Supp. II 2002). The Wiretap Act, codified at 18 U.S.C. §§ 2510-2522, and the Pen Register Act, codified at 18 U.S.C. §§ 3121-3127, are not covered in this Note.

71. ECPA also has a notable discrepancy in that it provides relatively strong protection to communications in transit, but much weaker protection to stored communications. Katherine A. Oyama, Note, *Email Privacy After* United States v. Councilman*: Legislative Options for Amending ECPA*, 21 BERKELEY TECH. L.J. 499, 508 (2006).

Title II of ECPA, the Stored Communications Act (SCA), applies to communication contents stored by third parties and is most applicable to internet searches, server logs, and stored e-mail.[72] The SCA prohibits anyone from "intentionally access[ing] without authorization a facility through which an electronic communication service is provided."[73] The SCA exempts providers of electronic or wire communications services, regardless of whether the provider acts in the normal course of business.[74] ECPA only constrains government access to data.[75] ISPs are not regulated by ECPA in accessing any customer stored data and need not obtain a subpoena to access stored customer records.[76]

Under ECPA, the government must obtain a warrant supported by probable cause to access information stored 180 days or less.[77] For electronic communications stored more than 180 days, the government needs either a warrant, a subpoena and notice to the subscriber, or a § 2703(d) court order and notice to the subscriber.[78] Section 2703(d) orders are available when the government shows "specific and articulable facts showing that there are reasonable grounds to believe" the information sought is relevant and material to an ongoing criminal investigation.[79] This showing is far less than the Fourth Amendment's "probable cause" standard. It is also less than would be required under ECPA'S Wiretap Act for real-time interception of phone and e-mail communications, which requires a warrant based on probable cause.[80]

Whether search queries and URLs are protected "content information" under ECPA remains an open issue. This statutory issue is addressed further in Part V. First, the Google subpoena incident illustrates the interplay between user privacy, third-party record holders, and government access. It also exemplifies the user privacy issues at stake in this developing body of law.

---

72. *See* 18 U.S.C. §§ 2701-2711.
73. § 2701(a)(1).
74. *See* § 2702.
75. *See* § 2703.
76. *See* § 2703(c)(1).
77. § 2703(a).
78. § 2703(b).
79. § 2703(d).
80. § 2518(3). For an analysis of ECPA's inconsistencies, see Oyama, *supra* note 71.

## III. *GONZALES V. GOOGLE, INC.*: RESISTANCE TO GOVERNMENT SUBPOENA

In *Gonzales v. Google, Inc.*, the U.S. government subpoenaed Google to obtain thousands of search queries entered by its users and thousands of URLs produced by Google searches.[81] The U.S. District Court for the Northern District of California held that trust in Google would be unnecessarily eroded if Google was forced to divulge the search queries entered by its users.[82] The court compelled Google to provide a sample of 50,000 URLs but did not require Google to disclose any user search queries.[83]

### A. Facts and Procedural History

#### *1. Government Defense of the Child Online Protection Act*

The government requested Google's search queries and URLs to aid its defense of the Child Online Protection Act (COPA).[84] Congress enacted COPA in 1998 in order to prohibit making commercial communications by means of the internet, "available to any minor and that includes material that is harmful to minors."[85] The American Civil Liberties Union and other plaintiffs sought a preliminary injunction against COPA's enforcement, arguing that less restrictive means of filtering explicit content, including user-end software filters, were superior.[86] The United States District Court for the Eastern District of Pennsylvania granted the preliminary injunction, finding that COPA unduly burdened protected speech.[87]

In *Ashcroft v. ACLU*, the Supreme Court affirmed the ruling that COPA likely violates the First Amendment.[88] The Court also held that there was an insufficient record before it by which the government could carry its burden to show that any less restrictive alternatives were less effective

---

81. Gonzales v. Google, Inc., 234 F.R.D. 674, 679 (D. Cal. 2006).

82. *Id.* at 684.

83. *Id.* at 688.

84. *Id.* at 678-79.

85. 47 U.S.C. § 231(a)(1) (2006). COPA defines "material that is harmful to minors" as obscene material or material meeting each prong of a three-part test. *See* 47 U.S.C. § 231(e)(6) (2006).

86. *Google*, 234 F.R.D. at 678-79; Declan McCullagh, *Google to feds: Back off*, CNET NEWS.COM, Feb. 17, 2006, http://news.com.com/Google+to+feds+Back+off/2100-1030_3-6041113.html. COPA, if constitutional, is to be codified at 47 U.S.C. § 231.

87. ACLU v. Reno, 31 F. Supp. 2d 473, 497-98 (E.D. Pa. 1998).

88. Ashcroft v. ACLU, 542 U.S. 656 (2004). The Court of Appeals for the Third Circuit affirmed the grant of the preliminary injunction. ACLU v. Reno, 217 F.3d 162 (3d Cir. 2000).

than COPA.[89] Of these alternatives, the Court focused on blocking and filtering software programs which restrict speech at the receiving end, not universal restrictions on content at the source.[90] The Court remanded the case to allow the parties to supplement the record "to reflect current technological realities."[91]

*2. Government Subpoena of ISP and Search Engine Information*

In August 2005, the federal government subpoenaed Google in support of its defense of COPA.[92] The government contended that it was studying the effectiveness of blocking and filtering software for child pornography.[93] To provide data for its study, the government served subpoenas on Google, AOL, Yahoo!, and Microsoft.[94] The subpoena required the companies to produce a list of URLs available to users of their services, and to produce the text of users' search queries.[95] While AOL, Yahoo, and Microsoft complied with the government's request, Google objected.[96] The government then scaled back its request for Google to produce only 50,000 URLs and 5,000 search queries entered by users between June 1 and July 31, 2005.[97] When Google still refused to comply, the government moved to compel Google to comply with the subpoena on January 18, 2006.[98]

## B. U.S. District Court Opinion

The U.S. District Court for the Northern District of California allowed the government's request for Google's URLs only.[99] The court found that production of both the URLs and the search queries would unduly burden Google by potentially diminishing user trust or disclosing trade secrets.[100] The court also discussed user privacy issues.[101]

89. *Ashcroft*, 542 U.S. at 673.
90. *See id.* at 667.
91. *Id.* at 672.
92. *Google*, 234 F.R.D. at 678.
93. *Id.*
94. *Id.* at 679.
95. *Id.*
96. *Id.*
97. *Id.*
98. *Id.* at 678.
99. *Id.* at 688.
100. *Id.* at 686.
101. *Id.* at 687.

*1. Relevance and Undue Burden*

Under Federal Rule of Civil Procedure 26(b), the information sought by a subpoena must be "reasonably calculated to lead to admissible evidence."[102] Regarding the URL sample, the court was "able to envision" a study whereby the sample would be reasonably calculated to lead to admissible evidence by testing the filtering software.[103] Based on the broad definition of relevance in Rule 26 and the narrowed scope of the government subpoena, the court held that the 50,000 URLs were relevant to the issues in *ACLU v. Gonzales*.[104]

The court also held that the search queries were reasonably calculated to lead to admissible evidence.[105] As defined in the government's subpoena, "queries" included only the text of the search string entered by a user, not any information that would identify the person or the computer from which the string was entered.[106]

Despite the finding of relevance under Rule 26(b), the court held that the burden on Google outweighed the government's need for both the URLs and search queries, under Federal Rule of Civil Procedure 45(c)(3)(a).[107] Google argued that revealing users' search queries would have a chilling effect on its business, because its success depends in part on the volume of users, many of whom are attracted to Google's anonymity and privacy.[108]

The court stated that neither URLs nor search strings with personal information redacted were reasonably "personal information" under Google's stated privacy policy.[109] However, the court held that even if Google users *unreasonably* expected Google to prevent disclosure of their search queries, this expectation of privacy might have an appreciable impact on the way in which Google is perceived, and consequently on the frequency with which Google is used.[110] The court concluded that many

102. FED. R. CIV. PRO. 26(b). This requirement is liberally construed to permit the discovery of information that ultimately may not be admissible at trial. *See, e.g.*, Moon v. SCP Pool Corp., 232 F.R.D. 633, 637 (C.D. Cal. 2005) (quashing subpoena seeking production of all purchasing information where underlying dispute was limited to a particular region).

103. *Google*, 234 F.R.D. at 681.

104. *Id.* at 686.

105. *Id.* at 682.

106. *Id.*

107. *Id.* at 686.

108. *Id.* at 683.

109. *Id.* at 684.

110. *Id.*

users do expect privacy, as over a quarter of all internet searches are for pornography.[111]

Additionally, the court found the subpoena presented a burden from potential loss of trade secrets.[112] A narrow sample of Google's index and query log could lead to further disclosure of confidential information in the event more information was sought.[113]

Therefore, in balancing the government's need for the proprietary information against the claim of injury resulting from disclosure, the court held that the government did not demonstrate a substantial need for *both* the URL and search query information.[114] It would be unreasonably cumulative and duplicative to compel Google to produce both sets of proprietary information.[115] Thus, court granted the government's motion to compel only as to the URL sample, not for any search queries.[116]

*2. Google User Privacy*

The court also raised concerns about the privacy of Google's users. The government contended that its request for search queries raised no privacy issues because the text of the queries would not yield identifiable information.[117] However, the court expressed concern that queries such as "bomb placement white house," or entry of users' own names presented privacy concerns.[118]

Moreover, the court was concerned about government use of information in unrelated investigations, stating it was "conceivable that the government may have an obligation to pursue information received for unrelated litigation purposes under certain circumstances . . . ."[119] In footnote 7, the court quoted DOJ spokesperson Charles Miller as stating, "I'm assuming that if something raised alarms, we would hand it over to the prop-

111. *Id.*

112. FED. R. CIV. P. 45(c)(3)(B) provides protections where the party challenging the subpoena makes "a strong showing that it has historically sought to maintain the confidentiality of this information." *Google*, 234 F.R.D. at 684 (citing Compaq Computer Corp. v. Packard Bell Elec., Inc., 163 F.R.D. 329, 338 (N.D. Cal. 1995)). This rule was intended to provide protections for the intellectual property of non-parties. *Google*, 234 F.R.D. at 685 (citing Mattel, Inc. v. Walking Mountain Prod., 353 F.3d 792, 814 (9th Cir. 2003) (citing Rule 45 Advisory Committee notes)).

113. *Google*, 234 F.R.D. at 684.

114. *Id.* at 685.

115. *Id.*; FED. R. CIV. P. 26(b)(2)(i).

116. *Google*, 234 F.R.D. at 686.

117. *Id.* at 687.

118. *Id.*

119. *Id.*

er [authorities]."[120] Presumably, the government could serve Google with additional subpoenas, even to identify specific users, if it had reason to believe that such users posed a security threat.[121] Ultimately, the court did not express an opinion on these privacy issues, as it denied the government's request for search queries.[122]

In the end, the court ordered Google to develop a protocol for random selection and production of only 50,000 URLs in Google's database.[123] Nicole Wong, Google general counsel, stated, "What his ruling means is that neither the government nor anyone else has carte blanche when demanding data from internet companies."[124]

The *Google* case drew attention to the interplay between online user privacy rights, third-party data holders, and government access. However, it failed to answer the paramount question: to what degree, if any, are internet searches "private"? Part IV addresses the application of the Fourth Amendment to online searches, focusing on the *Katz*, *Miller*, and *Smith* precedents. It argues that the Fourth Amendment should be interpreted consistent with its original purpose, ensuring the "right of the people to be secure" in their "persons, houses, papers, and effects."[125]

## IV. THE FOURTH AMENDMENT APPLIED TO ONLINE SEARCHES

For decades, courts have struggled to balance law enforcement's legitimate need to capitalize on advances in electronic surveillance technology with individuals' Fourth Amendment right to be secure against unreasonable searches and seizures. Although they predated the digital revolution, *Miller* and *Smith* continue to be cited for the proposition that individuals have no constitutionally protected privacy interest in records voluntarily disclosed to third parties, a category which presumably includes search engines like Google. As of today, the law is not settled on the issue of a legitimate expectation of privacy in modern electronic communications,

120. *Id.* at 688, n.7 (Decl. of Ashok Ramani, Ex. B.); Steven Levy, *Technology: Searching for Searches*, NEWSWEEK, Jan. 30, 2006, at 34; *see also* Posting by Kurt Opsahl, DOJ Gone Google-Fishin', EFF Deep Links, http://www.eff.org/deeplinks/archives/004341.php (Jan. 22, 2006, 15:28 PST).

121. *See* Opsahl, *supra* note 120.

122. *See Google*, 234 F.R.D. at 688.

123. *Id.*

124. Posting by Nicole Wong, Associate General Counsel, Judge Tells DOJ "No" on Search Queries, Googleblog, http://googleblog.blogspot.com/2006/03/judge-tells-doj-no-on-search-queries.html (Mar. 17, 2006, 06:00 PM).

125. *See* U.S. CONST. amend. IV.

and no case has explicitly addressed the Fourth Amendment as applied to search terms.[126] This Note proposes that the Fourth Amendment should apply to online search content, consistent with an originalist interpretation.

### A. *Miller* and *Smith*'s Assumption-of-Risk Paradigm Should Not Control Fourth Amendment Jurisprudence in Online Communications

*Miller* and *Smith* have long stood for the proposition that information voluntarily shared with third parties is not constitutionally protected under the Fourth Amendment.[127]

Two arguments advanced in *Miller* and *Smith* arguably support a finding that internet search information is not constitutionally protected by the Fourth Amendment. First, once a user enters a Google query, he or she has no control over what Google does with the information. Google may store the search in its database or use it for business purposes like targeted advertising. Second, according to a narrow reading of *Miller* and *Smith*'s assumption-of-risk holdings, users do not have a legitimate expectation of privacy in information voluntarily disclosed to a third party such as Google.[128]

However, *Miller* and *Smith* have been criticized as advancing an overly-broad conception of assumption-of-risk that equates any disclosure to a third party with a public disclosure.[129] The *Miller* Court quoted language from *Katz* that "what a person knowingly exposes to the public . . . is not subject to Fourth Amendment protection."[130] Yet in *Katz*, the Court explicitly held that the disclosure was protected under the Fourth Amendment because Katz did not *publicly* disclose information, but was talking with his friend and had no expectation that his conversation would be re-

126. Bellia, *supra* note 57, at 1408.

127. *See, e.g.*, California v. Greenwood, 486 U.S. 35, 41-42 (1988) (applying *Smith*'s assumption of risk analysis to hold it was not a search to fly over a backyard to discover marijuana plants); S.E.C. v. Jerry T. O'Brien, Inc., 467 U.S. 735, 742-43 (1984) (following *Miller* to hold that respondents could not argue that "notice of subpoenas issued to third parties is necessary to allow a target to prevent an unconstitutional search or seizure of his papers").

128. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (focusing on an objective inquiry of risk assumption); United States v. Miller, 425 U.S. 435, 442-43 (1976) (explaining that all the documents obtained "contain only information voluntarily conveyed to the banks and exposed to their employees in the normal course of business").

129. *See Miller*, 425 U.S. at 442; *Smith*, 442 U.S at 740; Brenner & Clarke, *supra* note 38, at 257-58.

130. *Miller*, 425 U.S. at 442 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

vealed.[131] The third-party revelation to the phone company did not eliminate Katz's expectation of privacy against government interception.[132]

The telecommunications carrier in *Katz* can be analogized to a search engine or ISP channeling electronic communications. While Google could potentially disclose searches to the government, following *Katz*, this does not necessarily eliminate one's expectation of privacy from government access to this information. Moreover, the *Katz* Court stated that a person placing a telephone call "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[133] The Court emphasized the unique role telephones play in modern life, stating, "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[134] In much the same way, the internet plays a "vital role" in modern communication.[135] The internet would be fundamentally altered if every user's search was recorded, mapped to an IP address, and delivered to the government.

A further critique of *Miller* and *Smith* is that the assumption-of-risk paradigm is problematic as applied to many online communications.[136] Content disclosure to Google or other search engines is practically inevitable in order to participate in modern life.[137] Justice Marshall, dissenting in *Smith*, recognized the Court's error, stating, "It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative."[138] Recognizing this unworkable doctrine, eleven states have rejected the federal "third party doctrine" in their privacy cases, and ten others have shown that they might reject it.[139]

---

131. Katz made a call from inside a public telephone booth. Katz was held to have a reasonable expectation of privacy in that call. *Katz*, 389 U.S. at 351.

132. Bellia, *supra* note 57, at 1385-86.

133. *Id.* at 352.

134. *Id.*

135. In the United States, about sixty-six percent of adults use the internet at least once per day. Pew Internet & Am. Life Project, Daily Internet Activities, *supra* note 1.

136. *See* Smith v. Maryland, 442 U.S. 735, 740 (1979) (converting the inquiry into an objective inquiry of risk assumption); United States v. Miller, 425 U.S. 435, 442-43 (1976) (explaining that all of the documents obtained "contain only information voluntarily conveyed to the banks and exposed to their employees in the normal course of business").

137. *See* Brenner & Clarke, *supra* note 38, at 254.

138. *Smith*, 442 U.S. at 749-50 (Marshall, J., dissenting).

139. *See, e.g.*, People v. Sporleder, 666 P.2d 135, 141-42 (Colo. 1983); State v. Hunt, 450 A.2d 952, 956 (N.J. 1982); *see also* Henderson, *supra* note 43, at 395 (listing the states that have rejected the federal third party doctrine).

Given these difficulties, it is unsurprising that courts have not developed a uniform approach in online communication privacy cases. The following Section summarizes the current state of the law.

### B. Courts Evaluating Fourth Amendment Jurisprudence Could Conclude Search Engine Users Lack a Legitimate Expectation of Privacy in Search Queries

Current caselaw does not resolve whether users retain an expectation of privacy in queries entered into a search engine or in electronic communications stored on a service provider's system.[140] Thus far, two military courts have found a reasonable expectation of privacy in stored e-mail messages.[141] In *United States v. Maxwell*, the United States Court of Appeals for the Armed Forces held that a user possessed a reasonable expectation of privacy in e-mail messages he sent and received on AOL.[142] The court stated that when an individual sends letters, messages, or other information on the computer, the Fourth Amendment expectation of privacy diminishes incrementally.[143] The more open the method of transmission, such as through an online chat room, the less privacy one can reasonably expect.[144]

Other courts have held that users retain a legitimate expectation of privacy in e-mail in transmission, but not once it has been opened by the recipient.[145] In *United States v. Charbonneau*, the court held that defendant had a limited reasonable expectation of privacy in the e-mail messages he sent and received on AOL.[146] The court stated, "Email is almost equivalent to sending a letter via the mails."[147] However, because defendant sent his messages through an open chat room, his reasonable expectation of privacy diminished. The court held there was no reasonable expectation of privacy in messages sent to others in internet chat rooms.[148] Courts have

140. Bellia, *supra* note 57, at 1408.

141. *See* United States v. Long, 64 M.J. 57 (C.A.A.F. 2006); United States v. Maxwell, 45 M.J. 406, 412, 419 (C.A.A.F. 1996) (finding reasonable expectation of privacy in e-mail files held by AOL).

142. *Maxwell*, 45 M.J. at 417.

143. *Id.*

144. *Id.*

145. *See* United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997); Smyth v. Pillsbury, 914 F. Supp. 97, 101 (E.D. Pa. 1996).

146. *Charbonneau*, 979 F. Supp. at 1184.

147. *Id.*

148. *Id.* at 1185; *see also* State v. Moller, No. 2001- CA-99, 2002 WL 628634, at *5 (Ohio App. Apr. 19, 2002) (holding that defendant had no expectation of privacy in communications in chat room, where undercover officer posing as fourteen-year-old girl was among message recipients).

also held that users retain no expectation of privacy in subscriber information supplied to an ISP.[149]

One could argue that the contents of search queries conveyed to Google are more private than messages sent in chat rooms. They are not open to outside viewing and are processed by the search engine automatically, much as ISPs transmit and store e-mail.[150] However, one could also analogize search queries to the phone numbers dialed in *Smith* or the bank records at issue in *Miller*, voluntarily revealed to a service provider for use in their business operations.[151] However, there is a qualitative difference between search query entries and other kinds of transactional data routinely provided to third parties in the course of business. A phone number is "content neutral" and does not give law enforcement any means to reconstruct the conversation itself.[152] By contrast, search terms contain precise language that reveals topics researched. This allows government access to types of information it never had when *Katz*, *Miller*, and *Smith* were decided.[153]

There are several possible analogies one could draw between online searches and other communication methods. No case has decided whether there is a constitutional right to privacy in queries entered into a search engine.[154] The following Section proposes that the Fourth Amendment's traditional protection of "papers and effects" should extend to analogous online communications, potentially including search queries.[155]

### C. Courts Should Interpret the Fourth Amendment Consistent with Original Intent to Ensure the "Right to be Secure"

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches

149. *See* Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (finding no expectation of privacy in subscriber information communicated to online bulletin board operators); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) (finding no expectation of privacy in subscriber information communicated to internet service provider).

150. *See Maxwell*, 45 M.J. at 417 (finding a reasonable expectation of privacy in e-mail stored on AOL's servers).

151. Bellia, *supra* note 57, at 1408; Gavin Skok, *Establishing a Legitimate Expectation of Privacy in Clickstream Data*, 6 MICH. TELECOMM. TECH. L. REV. 61, 78 (2000).

152. Bellia, *supra* note 57, at 1403 ("Neither *Miller* nor *Smith* involved the substance of personal communications."); Skok, *supra* note 151, at 78 (distinguishing the more revealing clickstream data from "content neutral" phone numbers).

153. Bellia, *supra* note 57, at 1457; Skok, *supra* note 151, at 79 (describing information officers can obtain from clickstream data as exceeding that available from library records).

154. Bellia, *supra* note 57, at 1408.

155. *See* U.S. CONST. amend. IV.

and seizures . . . ."[156] In drafting the Fourth Amendment, the Framers intended to curb indiscriminate searches by law enforcement officers and protect citizens' "right to be secure."[157] In deciding modern communication privacy cases, courts should advance an interpretation of the Fourth Amendment that upholds a meaningful right to be secure.[158]

Today, many citizens' most personal papers and records are held and conveyed by third parties. E-mail services and digital record holders provide ways to conveniently store and access personal information such as letters, academic and business papers, music, and photos.[159] Many storage activities that once took place privately in the home have moved into the digital realm. The Fourth Amendment protection of "persons, houses, papers, and effects" should arguably apply to this online information.[160]

The Framers of the Fourth Amendment sought to prohibit forms of physical intrusion upon "persons" or "houses" as well as unreasonable intrusion into "papers and effects" caused by surveillance and indiscriminate general warrants.[161] The specific invasion of privacy they sought to eliminate was "not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings."[162]

In 1886 in *Boyd v. United States*, the government tried to compel a merchant to produce documents in a civil forfeiture proceeding.[163] The

---

156. *Id.*

157. Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 549, 556 (1999).

158. *Id.* at 741.

159. Record Nations is an example of one such service. *See* Record Nations, http://www.record nations.com/services/landing-storage.php?utm_source=google&utm_medium=ppc& gclid=CI6E5eTMzIgCFRl-YAodYXknBQ (last visited Nov. 16, 2006) (record storage service).

160. In 1878, in *Ex Parte Jackson*, the Supreme Court held that the Fourth Amendment prohibited government officials from opening letters without a warrant: "The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be." 96 U.S. 727, 733 (1878). Today, e-mail subsumes the role of many personal letters.

161. Davies, *supra* note 157, at 555 (stating that James Madison, who proposed the draft that ultimately became the Fourth Amendment, viewed his proposal as a ban against "general" warrants, including warrantless searches of offices); Thomas K. Clancy, *The Role of Individualized Suspicion in Assessing the Reasonableness of Searches and Seizures*, 25 U. MEM. L. REV. 483, 528 (1995) ("The core complaint of the colonists was not that searches and seizures were warranted, warrantless, or unauthorized actions; it was the general, suspicionless nature of the searches and seizures.").

162. Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971) (citing Boyd v. United States, 116 U.S. 616, 624-30 (1886)).

163. Boyd v. United States, 116 U.S. 616, 635 (1886).

Court held that the documents could not be compelled, based on the Fourth Amendment.[164] The Court's warning is particularly relevant today:

> [I]llegitimate and unconstitutional practices get their first footing in that way, namely, by silent approaches and slight deviations from legal modes of procedure. This can only be obviated by adhering to the rule that constitutional provisions for the security of person and property should be liberally construed .... It is the duty of courts to be watchful for the constitutional rights of the citizen, and against any stealthy encroachments thereon.[165]

Subpoenas for thousands of search queries entered by Google, Yahoo!, or other search engine users fail to discriminate between lawful and unlawful activity and expose intimate details of Americans' lives. This "exploratory rummaging" is precisely what the Framers sought to eliminate in passing the Fourth Amendment.[166] As the court stated in *Gonzales v. Google, Inc.*, revealing search query content, even when this information pertains to lawful activity, may prompt additional government subpoenas for "suspicious information."[167] Allowing the government to expose the conduct of the innocent in the course of pursuing the guilty contradicts the purpose of the Fourth Amendment.[168]

Moreover, internet searches are more akin to the "private papers" traditionally protected by the Fourth Amendment than "business records" at issue in *Miller* and *Smith*.[169] In *Miller* and *Smith*, the Court noted that the content intercepted was not "personal," but "business records."[170] When the government obtains bank records, as in *Miller*, it learns what transac-

---

164. *Id.* at 638.

165. *Id.* at 635.

166. *Id.*

167. Gonzales v. Google, Inc., 234 F.R.D. 674, 687 (N.D. Cal. 2006); *Id.* at 687 n.7 (Decl. of Ashok Ramani, Ex. B.); Levy, *supra* note 120 (quoting Department of Justice spokesman Charles Miller: "I'm assuming that if something raised alarms, we would hand it over to the proper [authorities]."); *see also* Opsahl, *supra* note 120.

168. Skok, *supra* note 151, at 85 (citing United States v. Rabinowitz, 339 U.S. 56, 82 (1950) (Frankfurter, J., dissenting) ("By the Bill of Rights the founders of this country subordinated police action to legal restraints, not in order to convenience the guilty but to protect the innocent.")).

169. *See* United States v. Miller, 425 U.S. 435, 439 (1976) (distinguishing bank records from "compulsory production of a man's private papers," traditionally protected by the Fourth Amendment (quoting *Boyd*, 116 U.S. at 622)).

170. *Id.* at 440-41, 445 (noting that bank records were integral to the bank's business); Smith v. Maryland, 442 U.S. 735, 742 (1979) ("the phone company has facilities for making permanent records of the numbers they dial . . . [callers] see a list of their long-distance (toll) calls on their monthly bills.").

tions were made and by whom, but not the underlying subjects and circumstances of the transactions.[171] By contrast, a Google search query reveals content, allows the government to research responsive URLs, and may prompt subpoenas to obtain a user's IP address and identity.[172] Roughly twenty-five percent of all web searches are for pornography, and others reveal various private interests.[173] The "content" of these queries is more closely aligned with the phone conversation in *Katz* than to digits dialed on a phone or bank records one knows a human teller might read, at issue in *Smith* and *Miller*.[174]

### D. Fortifying Fourth Amendment Protection for Online Communications

Google's terms of service state that it will disclose personally-revealing information to third parties "in limited circumstances," including when "complying with legal process," preventing imminent harm, or ensuring the security of the network.[175] If search information is not currently protected under the Fourth Amendment, probable cause is not required in order to access personal searches.[176] Indeed, AOL, Yahoo, and Microsoft complied with the government's request for URLs and search queries, without requiring a warrant.[177] Therefore, the "legal process" required for government access to search query information should be better defined by the courts so companies and the public know exactly what is "private," and what is not.

Because users' personal ideas, "papers, and effects" are now conveyed to third party companies like AOL and Google, the *Miller-Smith* paradigm is inadequate and should not foreclose Fourth Amendment protection.

---

171. Skok, *supra* note 151, at 78.

172. *See Google*, 234 F.R.D. at 687 n.7 (Decl. of Ashok Ramani, Ex. B.); Levy, *supra* note 120; *see also* Opsahl, supra note 120.

173. *See* Supplemental Declaration of Phillip B. Stark, Ph.D., at 4 (Feb. 24, 2006), Gonzales v. Google, 234 F.R.D. 674 (N.D. Cal. 2006) (No. MC-80006-22).

174. The *Miller-Smith* approach also ignores the societal benefits of well-placed trust in third party information gatherers and services. Many businesses provide efficient methods of record-keeping, research, and completing transactions. Recognizing this trust as legitimate enables companies to offer these services at a lower price, as consumers need not negotiate for additional privacy protections, which are potentially costly. *See* Brenner & Clarke, *supra* note 38, at 258.

175. *See* Google Privacy Center, Google Privacy Policy Highlights (Oct. 14, 2005), http://www.google.com/privacy.html.

176. *See* U.S. CONST. amend. IV ("no Warrants shall issue, but upon probable cause"); Bellia, *supra* note 57, at 1402 ("Read broadly, *Miller* suggests that the mere fact that documents are conveyed to a third party . . . eliminates any expectation of privacy.").

177. *Google*, 234 F.R.D. at 679.

Consistent with the original intent of the Fourth Amendment, personal records that society recognizes as private should require a warrant and probable cause to access, whether held by an individual or by a private company.[178] Courts should assess whether online communications, like search queries, contain the type of information the Fourth Amendment was intended to protect.[179]

Some legal scholars suggest that obtaining "privately-held," "personal records" should require a warrant and probable cause.[180] Others suggest that First Amendment values are implicated in the Fourth Amendment "right to be secure," and should factor into this calculus.[181] This Note does not evaluate the merits of these various proposals. However, it suggests that search queries contain content and ideas traditionally expressed as "papers" and "effects" protected by the Fourth Amendment.[182] In deciding future cases, courts should consider the original intent of the Framer's of the Fourth Amendment in evaluating whether society should recognize a legitimate expectation of privacy in such communications.

In addition to constitutional protection, federal statutes protect the privacy of some electronic communications.[183] Part V addresses ECPA's

178. *See* U.S. CONST. amend. IV; Katz v. United States, 389 U.S. 347, 350-52 (1967) ("[The Fourth] Amendment protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all.").

179. *See* Skok, *supra* note 151, at 83 ("Net users should retain an expectation of privacy in clickstreams because this data is precisely the type of information the Framers sought to protect against arbitrary government intrusion.").

180. *See* Slobogin, *supra* note 39, at 182-83.

181. Some academics have argued that when First Amendment values are threatened by government access to private information, this should militate in favor of a Fourth Amendment "reasonable expectation of privacy." A complete analysis of this issue is beyond the scope of this note. For insightful work on First Amendment privacy issues in electronic information, see Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 806 (1994); Neil M. Richards, *Essay: The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1118-19 (2006); Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. (forthcoming 2007) (on file with author).

182. *Ex Parte Jackson*, 96 U.S. at 733 (holding that the Fourth Amendment prohibited government officials from opening letters without a warrant); Clancy, *supra* note 161, at 528 ("The core complaint of the colonists . . . was the general, suspicionless nature of the searches and seizures."); Davies, *supra* note 157, at 555 (describing the Fourth Amendment as intended to ban "general" warrants, including warrantless office searches); Skok, *supra* note 151, at 83 ("Net users should retain an expectation of privacy in clickstreams because this data is precisely the type of information the Framers sought to protect against arbitrary government intrusion.").

183. *See* 18 U.S.C. § 2701.

Stored Communications Act (SCA) and standards for government access to electronic communications.

## V. FEDERAL STATUTORY PROTECTIONS: ECPA AND THE STORED COMMUNICATIONS ACT (SCA)

Title II of ECPA, the Stored Communications Act (SCA), sets the standard for government access to electronic communications.[184] Whether search queries fall under the definition of "contents of communications" protected under ECPA is an open question.[185] Expanding and clarifying federal statutory protections for electronic information held by third parties could both increase procedural safeguards and strengthen the reasonable expectation of privacy in online communications.[186]

When the Supreme Court in *Miller* found no constitutional protection for bank records, Congress responded with statutory protection for bank records.[187] After the *Smith* Court found no privacy in dialed telephone numbers, Congress again established statutory protection.[188] Today, the "reasonable expectation of privacy" in online records is uncertain, and some courts have held that ISP users' information is not constitutionally protected.[189] Statutory measures could potentially fill this void left by uncertain constitutional protection.

Statutory measures are also important because data holders like Google and AOL may have little incentive to resist government subpoenas for information used to fight crime or fraud. When Google resisted the subpoena last year, it resisted alone.[190] One cannot be certain how many

184. *Id.*

185. Detailed discussion of whether Google searches are currently covered under ECPA is beyond the scope of this Note. For more information, see Amicus Brief of Center for Democracy & Technology in Support of Google's Opposition to the Motion to Compel of Attorney General Gonzales, Gonzales v. Google, 234 F.R.D. 674 (N.D. Cal. 2006) (No. CV-06-80006-MISC JW), 2006 WL 733757 [hereinafter CDT Amici Curie Brief].

186. The Supreme Court has never squarely addressed the extent to which statutory or common law protection of a communication contributes to the reasonableness of an expectation of privacy. *See* Bellia, *supra* note 57, at 1387.

187. *See* Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-22 (2000), *amended by* 12 U.S.C.A. §§ 3401-22 (West Supp. 2005).

188. *See* 18 U.S.C. §§ 3121-27 (2000 & Supp. 2002).

189. *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, 508 (W.D. Va. 1999) (finding no Fourth Amendment protection in ISP records because the user "knowingly revealed his name, address, credit card number, and telephone number" to his ISP).

190. *Google*, 234 F.R.D. at 679.

requests search engines and ISPs have already complied with.[191] Data brokering companies now aggregate information on individuals and sell it to both government and private litigants.[192] These practices implicate new privacy concerns not addressed in ECPA.[193]

One effective solution is to implement more stringent criterion for government access to third party-held personal information. If search queries were covered by ECPA, the government would be required to follow the procedures outlined in the SCA: obtain a warrant issued in compliance with Federal Rules of Criminal Procedure, or provide notice to the customer if the government uses an administrative subpoena authorized by statute or federal or state grand jury, or obtains a court order for such disclosure.[194]

One district court has held that Google search terms are protected "contents of communications" within the meaning of ECPA.[195] In an amicus brief opposing the government subpoena in *Gonzales v. Google*, the Center for Democracy and Technology (CDT) argued that Google searches should be regulated under ECPA.[196]

If Google searches were covered under ECPA, the pre-trial discovery subpoena issued to Google for its search queries would have been inade-

---

191. AOL receives more than 1,000 subpoenas each month seeking information about its users. *See* Hansell, *supra* note 5.

192. In 2005, four government agencies—the Department of Justice (DOJ), State Department, Homeland Security Department, and the Social Security Administration—spent roughly $30 million to purchase personal information from data brokers. Nancy Libin, *Perspective: The anxious new dawn of cybersnooping*, CNET NEWS.COM, May 3, 2006, http://news.com.com/The+anxious+new+dawn+of+cybersnooping/2010-1028_3-6067598.html. Choicepoint is one example of data aggregation. *See* ChoicePoint, http://www.choicepoint.com (last visited Nov. 26, 2006).

193. *See* Bellia, *supra* note 57, at 1413 ("The legislative reports accompanying ECPA suggest conflicting views of whether subscribers retain an expectation of privacy in communications held by third-party service providers.").

194. 18 U.S.C. §§ 2701-03.

195. *In re* United States for an Order Authorizing the Use of a Pen Register & Trap, 396 F. Supp. 2d 45, 49 (D. Mass. 2005).

196. *See* CDT Amici Curie Brief, *supra* note 185. CDT argued that Google is an outsourcer of search functions, and therefore is a provider of a "remote computing service" and should be covered under ECPA. *Id.* at 3-5. CDT also argued that search queries are "contents of a communication" under EPCA. *Id.*; *see* 18 U.S.C. § 2510(8) (defining "contents" of a communication as including "any information concerning the substance, purport, or meaning of that communication"). In *Gonzales v. Google*, Judge Ware declined to discuss the ECPA issue. *Google*, 234 F.R.D. at 688. Google raised the issue at the end of its brief, stating, "there is good reason to believe they are [covered by ECPA] . . . " Google Opp., supra note 9, at 18-19.

quate.[197] However, the government could still compel disclosure by grand jury subpoena, administrative subpoena, or trial subpoena plus notice to the subscriber.[198] This individual notice can be delayed for up to ninety days.[199]

ECPA is not determinative of user privacy issues, as the restrictions it imposes are usually less than those required by the Fourth Amendment. Furthermore, its protections are more fragile, as Congress could vote to remove them.[200] However, a new statute or amendment to ECPA could provide more privacy protection for electronic communications—including search queries—to the extent Congress clarified the relevant provisions.[201]

## VI. CONCLUSION

Advances in information and communication technologies have outpaced constitutional and statutory privacy protection. Search engines and ISPs now retain massive amounts of data, much of which is intended for private use only.

At the same time, law enforcement agencies increasingly subpoena private companies such as Google and AOL to access this data. In 2006, *Gonzales v. Google, Inc.* marked a collision among individual, business, and government interests in online communications. While illuminating individual privacy dangers, it ultimately failed to address the larger constitutional and statutory issues.[202]

The Fourth Amendment has provided little protection for this third-party information, due to *Miller* and *Smith*'s arguably flawed assumption-of-risk paradigm. Moreover, ECPA's statutory protections for digital

197. *See* FTC v. Netscape Commc'ns. Corp., 196 F.R.D. 559 (N.D. Cal. 2000) (holding that pre-trial discovery subpoena did not fall within the meaning of "trial subpoena").

198. 18 U.S.C. § 2705(a)(1)(B)-(a)(4).

199. § 2705(a)(1)(B) and § 2705(a)(4) permit notice to be delayed for up to ninety days "upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result . . . ."

200. *See* Brenner & Clarke, *supra* note 38, at 219 n.20.

201. For example, after the *Miller* decision Congress passed the Right to Financial Privacy Act of 1978. *See* 12 U.S.C. §§ 3401-22 (2000), *amended by* 12 U.S.C.A. §§ 3401-22 (West Supp. 2005). Congress passed the Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710 (2002), in response to a highly publicized incident of a video store disclosing a politician's rental records. Electronic Privacy Information Center, The Video Privacy Protection Act (VPPA), Aug. 6, 2002, http://www.epic.org/privacy/vppa/.

202. Gonzales v. Google, 234 F.R.D. 674 (N.D. Cal. 2006).

third-party information are less stringent than Fourth Amendment protections and arguably do not apply to search queries and other data.

This Note proposes that these issues are best addressed by an originalist interpretation of the Fourth Amendment. Such an interpretation would meaningfully protect the "right to be secure" in online communications. Courts should reject an assumption-of-risk analysis in favor of an approach that acknowledges the vital role internet technology plays in American life. Finally, expanding and clarifying ECPA to cover "content" disclosures such as search queries could also protect the "right to be secure" guaranteed by the Fourth Amendment.