Data Retention: Privacy, Anonymity, and Accountability Online

Catherine Crump

Follow this and additional works at: https://scholarship.law.berkeley.edu/facpubs

Recommended Citation
Data Retention: Privacy, Anonymity, and Accountability Online

Catherine Crump* 

J.D. Candidate, Stanford Law School, 2004. Special thanks to Lee Tien of the Electronic Frontier Foundation for his patient guidance. Thanks also to Mariano-Florentino Cuéllar, Jay Freedman, Mark Jacobsen, Lawrence Lessig, Scott Michelman, and Stewart Young for their helpful editing and comments.
INTRODUCTION

Motivated by a strong sense of vulnerability to the threat posed by those who cheered as the World Trade Center and Pentagon burned in September 2001, governments worldwide are working to strengthen the hand of law enforcement agencies. The complexity and success of the transcontinental conspiracy to decimate the most recognizable symbols of U.S. power have fundamentally reoriented thinking on the extent to which individuals should be allowed to conduct their activities out of view of law enforcement authorities. As an instrument for clandestine communication, the Internet has been a lightning rod for criticism. What were once portrayed as the medium's virtues, particularly its empowerment of "little people" whose voices are not heard in traditional broadcast and print media, are now characterized as mixed blessings. The "vast democratic forums of the Internet" are also seen as "a powerful new medium for those who wish to commit criminal and terrorist acts."

One method that governments use to make online activity traceable by law enforcement agencies is to institute data retention requirements. Though government-mandated data retention can range in scope, at its core is the requirement that Internet service providers ("ISPs") collect and store data that

1. The Court has been particularly protective of communications methods that are especially accessible to those with few resources. See Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 169 (2002) (striking down an ordinance requiring a permit from the mayor's office for door-to-door solicitation to promote any cause); City of Ladue v. Gilleo, 512 U.S. 43, 57-58 (1994) (striking down an ordinance that banned most residential signs while noting that "[e]specially for persons of modest means or limited mobility, a yard or window sign may have no practical substitute"); Martin v. City of Struthers, 319 U.S. 141, 146 (1943) (invalidating a city ordinance banning door-to-door solicitation and pointing out that "[d]oor to door distribution of circulars is essential to the poorly financed causes of little people").


track the Internet activity of their customers. Several European nations have enacted data retention laws. For example, Switzerland requires Swiss ISPs to record the time, date, sender, and receiver of all emails. The very existence of working European examples of data retention laws and the environment of heightened sensitivity to security threats increases the probability that the United States will consider adopting a data retention law.

This possibility seems all the more realistic given the current use in the United States of a related but slightly less sweeping law enforcement tool known as “data preservation.” The United States government has given law enforcement agencies the tool of data preservation since 1996. In order to

5. ISPs mediate their customers’ connections to the Internet. Consequently, “ISPs can precisely monitor and record an entire clickstream [user’s communications over the Internet] since all of the user’s online commands are sent through the ISP.” Gavin Skok, Establishing a Legitimate Expectation of Privacy in Clickstream Data, 6 Mich. Telecomm. & Tech. L. Rev. 61, 67 (2000), available at http://www.mttlr.org/volsix/skok.html (asserting that courts should recognize a legitimate expectation of privacy in Internet communications).


7. See Jacob Greber, Swiss Surveillance Catches Up With E-mail, Swissinfo, July 21, 2002, at http://www.swissinfo.org/sem/Swissinfo.html?siteSect=111&sid=1192676 (last visited June 22, 2002) (“Since the beginning of 2002, all Swiss Internet service providers (ISPs) have been legally obliged to record the time, date, sender ID and receiver ID of all e-mails.”). Also, Spain passed La Ley de Servicios de la Sociedad de la Informacion y de Comercio Electronico (LSSI), which requires ISPs to retain some types of data on their customers for one year. See Spain Passes Law to Regulate Internet Content, The Mercury News, June 27, 2002, http://www.siliconvalley.com/mld/siliconvalley/news/editorial/3556967.htm (last viewed June 22, 2002); see also Electronic Privacy Information Center, supra note 4 (tracking the passage of data retention laws).

8. Additionally, public opinion in the wake of the September 11, 2001 terrorist attacks may be more supportive of data retention. These events altered views on whether there is a necessary tradeoff between protecting civil liberties and preventing terrorism. Shortly after the terrorist attacks, 55% of those surveyed believed that civil liberties would have to be restricted to prevent terrorism. In April, 1997, only 29% held this view. Lisa Guernsey, Living Under an Electronic Eye, N.Y. Times, Sept. 27, 2001, at G1.


10. 18 U.S.C. § 2703(f):
Requirement to preserve evidence.—(1) In general.—A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process. (2) Period of retention.—Records
prevent ISPs from destroying data in their possession while law enforcement personnel are in the process of obtaining a warrant for that information, law enforcement agencies can compel ISPs to retain data on a specific customer for at least ninety days.11 Though data preservation is different from data retention in that it targets the Internet traffic of a specific individual who is already under investigation, it demonstrates the utility of Internet traffic data as evidence of criminal wrongdoing.12

The purpose of data retention is much broader than that of data preservation. Data retention aims to change the context of Internet activity. The context change that data retention renders makes it easier to link acts to actors.13 Data retention "rearchitects" the Internet from a context of relative obscurity to one of greater transparency.14 This manipulation of context influences what values flourish on the Internet. Specifically, data retention, by making it easier to link acts to actors, promotes the value of accountability, while diminishing the values of privacy and anonymity.15

This seemingly esoteric point about the interplay of three values—accountability, privacy, and anonymity—is of practical importance to those who would require data retention. The two values that data retention would diminish—privacy and anonymity—are protected by the Constitution,16 though

referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

11. Id.

12. For information on how the government has used Internet traffic to apprehend criminals, see John Schwartz, Tools for the Aftermath; In Investigation, Internet Offers Clues and Static, N.Y. TIMES, Sept. 26, 2001, at H1, for a discussion of how the increased use of electronic transactions such as credit cards and emails generates a paper trail that is useful for law enforcement. See also Skok, supra note 5, at 68-69 (describing how Internet usage records would be helpful to law enforcement agents); Bill Miller, Ashcroft: Old Rules Aided Terrorists; FBI Agents Get Freer Hand; Civil Liberties Groups Criticize New Guidelines, WASH. POST, May 31, 2002, at A13 (describing new guidelines for FBI surveillance).

13. I do not mean to invoke the speech/act dichotomy when using the term "acts." Rather, I intend the term to include reading, writing, and other expressive activity.


[EX]perienced as conditions on one's access to areas of cyberspace.... Code sets these features; they are features selected by code writers .... They embed certain values, or they make the realization of certain values impossible. In this sense, these features of cyberspace also regulate, just as architecture in real space regulates.

_id. at 509-10; see also LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) [hereinafter CODE] (describing how code interacts with laws, norms, and markets to shape what we experience when we use the Internet).

15. See generally Shaun B. Spencer, CyberSLAPP Suits and John Doe Subpoenas: Balancing Anonymity and Accountability in Cyberspace, 19 J. MARSHALL J. COMPUTER & INFO. L. 493 (2001) (discussing how civil suit subpoenas that strip pseudonymous Internet message board posters of their pseudonymity implicate the First Amendment right to speak anonymously).

16. U.S. CONST. amend. I; U.S. CONST. amend. IV.
the extent of this protection is an open question.\textsuperscript{17} The Fourth Amendment’s prohibition of unreasonable searches and seizures indicates some limit to the government’s power to make us live transparently in order to promote accountability.\textsuperscript{18} The First Amendment has been interpreted to protect anonymous speech and association, which cannot exist in an environment in which every action is traceable.\textsuperscript{19} The Constitution protects some measure of contextual obscurity.

The question of how far government can go in requiring us to live transparently in order to facilitate accountability though requirements such as data retention takes on increasing urgency in the new context of cyberspace. The nature of cyberspace is highly malleable. It is determined by code, and code can be rewritten.\textsuperscript{20} Further, since just a handful of ISPs provide Internet access to most people in the United States,\textsuperscript{21} these gateways to the Internet are

\begin{itemize}
\item \textsuperscript{17} For more on privacy, see \textit{infra} Part I.A. For more on anonymous speech activity, see \textit{infra} Part II.A.
\begin{quote}
Imagine if government, for similar reasons, required us to live in glass houses, conduct all our conversations loudly and exclusively in English, carry all our personal belongings in clear plastic bags, or keep all of our possessions in unlocked cabinets or drawers. Most Americans would no doubt be deeply troubled by such laws. Government may not bootstrap its way out of Fourth Amendment constraints simply by outlawing methods for preserving privacy that would otherwise be considered reasonable within the broad contours of our customs and traditions.
\end{quote}
\item \textsuperscript{19} See McIntyre v. Ohio Elections Comm’n, 514 U.S. 334, 355 (1995) (striking down a law that forbids the distribution of anonymous election-related literature); Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 558 (1963) (rejecting an attempt of a Florida legislative committee to require the NAACP to produce its membership records); Shelton v. Tucker, 364 U.S. 479, 490 (1960) (striking down a state statute requiring that teachers list all of their association memberships in the previous five years); Talley v. California, 362 U.S. 60, 64 (1960) (declaring unconstitutional a blanket prohibition on anonymous handbill distribution); NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 460 (1958) (holding that requiring the NAACP to produce its membership records would chill association). \textit{But see} Buckley v. Valeo, 424 U.S. 1, 72 (1976) (upholding an identification requirement of certain campaign contributors despite its impact on anonymous speech).
\item \textsuperscript{20} As Lessig puts it: “Cyberspace has no nature; it has no particular architecture that cannot be changed. Its architecture is a function of its design . . . its code.” \textit{The Law of the Horse, supra} note 14, at 506.
\item \textsuperscript{21} The ISP industry is quite concentrated, certainly to the point where government will be able to identify ISPs and hold them to certain regulatory requirements. In a recent survey in which individuals were asked which company provided their Internet access, about a third answered America Online; local phone, cable, and MSN received just under 10% each; and EarthLink, AT&T Worldnet, and Juno each received just under 7%. \textit{Forrester Report, Devices & Access September 2002 Data Overview: Covers TV, Wireless, Gaming, ISPs, and Communication} (2002).
\end{itemize}
obvious targets of regulation.\textsuperscript{22} By requiring ISPs to change their code such that the Internet traffic of their users is archived, the government could alter the mix of anonymity, privacy, and accountability that currently exists online.

Given the possibility that Congress may want to repeal current statutory limits on law enforcement agencies' access to privately maintained customer records, this Note's aim is to probe the current constitutional limitations on government-mandated data retention.\textsuperscript{23} Does the Constitution permit the government to require that Internet service providers archive the Internet usage of their customers, and can law enforcement officials then access these records without any judicial oversight or notice to customers? Although the primary purpose of this Note is descriptive, it uncovers tensions in the doctrine that will be addressed.

A constitutional challenge to data retention would most likely be grounded in the Fourth or First Amendment. Part I of this Note will focus on the Fourth Amendment. Because the Supreme Court has already found in other contexts that it is permissible for government to require businesses to keep copies of customer records and, further, that it is permissible for law enforcement agencies to access these records without a warrant, a Fourth Amendment barrier to government-mandated data retention by ISPs seems unlikely.\textsuperscript{24} If the Fourth Amendment were to be read to place some limit on the ability of government to make us live transparently to facilitate law enforcement, however, those who oppose data retention could find a perverse sort of hope in the fact that the range of human activity that will be catalogued if all Internet traffic is recorded is vast compared to recordkeeping the Court has explicitly approved in the past.\textsuperscript{25} Part II focuses on the First Amendment, specifically the right to engage in speech activity anonymously.\textsuperscript{26} Because data retention eliminates all anonymous speech online by making all online activity traceable.

\textsuperscript{22} Lessig makes this point in reference to the Internet browser market: "In a world where ninety percent of browsers are produced by two companies, the code writers are too prominent to hide." \textit{The Law of the Horse}, supra note 14, at 517.

\textsuperscript{23} A related issue of concern to many civil libertarians is the government purchase of private databases of information about individuals for use in law enforcement. These databases are voluntarily compiled by private sector entities and voluntarily shared with government officials. The issue of voluntary data transfer from the private sector to government is beyond the scope of this Note. For a good overview of the issues this raises, however, see Daniel J. Solove, \textit{Digital Dossiers and the Dissipation of Fourth Amendment Privacy}, 75 S. CAL. L. REV. 1083 (2002).


\textsuperscript{25} \textit{See infra} Part I.E.

\textsuperscript{26} \textit{See infra} Part II.A.
and because the Court applies strict scrutiny to government-mandated identification requirements, data retention would probably need to be narrowly tailored to a compelling governmental need if it is to withstand scrutiny. This Note concludes that, although there is probably no Fourth Amendment bar to compulsory data retention, data retention would probably be considered unconstitutional under current First Amendment doctrine because there are other methods that could be used to monitor Internet activity that would burden speech substantially less.

I. THE FOURTH AMENDMENT

The Fourth Amendment grants, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." It was handwritten at a time when tangible objects and physical spaces were all that existed. The intervening centuries have given rise to an expanding technological capacity that has deeply affected our surveillance capabilities and the means we use to communicate. Law enforcement officials need no longer rely on the unaided eye for observation—technology has been used to enhance night vision and to "see through" walls. In addition, a broad

27. See McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995) (striking down a law that forbids the distribution of anonymous election-related literature). The Court clarified that regulation of identifying information is properly considered content-based regulation when it wrote: "[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment." Id. at 342. Therefore, regulation of identifying information is subject to strict scrutiny.

28. See infra Part II.B.

29. U.S. CONST. amend. IV.

30. See generally STEPHEN SEGALLER, NERDS 2.0.1: A BRIEF HISTORY OF THE INTERNET (1998) (describing the technological breakthroughs that led to the development of the Internet, from the 1960s on). To gain a sense of the current state of surveillance technology and what new technologies government hopes to develop, see generally OFFICE OF JUSTICE PROGRAMS, DEPT. OF JUSTICE, DEPARTMENT OF JUSTICE AND DEPARTMENT OF DEFENSE JOINT TECHNOLOGY PROGRAM: SECOND ANNIVERSARY REPORT 8 (1997), which highlights technologies the Defense and Justice departments hope to develop jointly to meet common surveillance needs; and, NAT'L INST. FOR JUSTICE, U.S. DEP'T OF JUSTICE, INVENTORY OF STATE AND LOCAL LAW ENFORCEMENT TECHNOLOGY NEEDS TO COMBAT TERRORISM (1999), which analyzes a survey of local law enforcement agencies about their technology needs.

31. See Thomas D. Colbridge, 70 FBI L. ENFORCEMENT BULL., Oct. 2001, at 25, at http://www.fbi.gov/publications/leb/2001/oct01leb.htm (last accessed June 22, 2002) (describing thermal imaging technology). The Court has often been called on to evaluate the Fourth Amendment implications of new surveillance technology. See Kyllo v. United States, 533 U.S. 27 (2001) (holding that: "[O]btaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use.

October 2003] DATA RETENTION 197
swath of human activity now takes place through packet-switching technologies such as the Internet, a technology that is "unprecedented in the degree of detailed information that can be gathered and stored."

Each iteration of technological advancement raises anew the question of what kinds of law enforcement observation techniques amount to a Fourth Amendment search and therefore require a warrant. In defining the term "search" in a variety of technological contexts, the Court has laid out a hodgepodge of doctrines—some seemingly contradictory—that bear on our inquiry about data retention. This is an exercise in piecing together what the Court has said in disparate contexts to surmise how it might rule in the case of data retention. For our purposes, the modern doctrine begins with the seminal case of *Katz v. United States*, which sets out the basic inquiry courts follow when determining what is a search under the Fourth Amendment. It moves on to the Court's communications-specific holding in *Smith v. Maryland* that warrantless government collection of the telephone numbers one dials is not a search. The doctrine ends with the Court's sole word on government-mandated records retention, which the Court upheld against a Fourth Amendment challenge in the context of bank records and further held that a warrant was not required for law enforcement agencies to access retained bank records. Part I.A will distill the constitutional principles developed in these precedent-setting cases. Part I.B will explore how these cases could be applied to the context of Internet records retention.

A. "Real Space" Cases


When faced with the question of what is a search for Fourth Amendment purposes, the Court ritualistically invokes the test first laid out in *Katz v. United States* in 1967. While the plain speech meaning of the word "search" might


32. PRESTON GRALLA, HOW THE INTERNET WORKS 52 (1999).

33. Solove, supra note 23, at 1093.

34. 389 U.S. 347, 352 (1967) (holding that defendant justifiably relied on his expectation of privacy when speaking in a closed telephone booth and that law enforcement eavesdropping on him therefore amounted to a Fourth Amendment search).

35. 442 U.S. 735, 742 (1979) (holding that there is no reasonable expectation of privacy in the telephone numbers that individuals dial).

36. See supra note 24 and accompanying text.

37. 389 U.S. at 353.
lead one to believe that every time law enforcement agents actively look for evidence of criminal wrongdoing they are engaged in a search, the Court has adopted a different definition based on expectations of privacy. Since *Katz* both sets out the oft-repeated standard and illustrates the beginnings of the process by which it has been eroded, a review of *Katz* will serve our purpose of understanding why it and its progeny will probably lead the Court to the conclusion that compulsory data retention by ISPs is not a Fourth Amendment search.38

Charles Katz unwittingly launched himself down the path to fame in the legal world by closing himself up in a public telephone booth and making a phone call.39 Unbeknownst to him, the FBI had attached an eavesdropping device to the outside of the phone booth and recorded his conversation.40 In the course of his trial for illegal gambling, Katz argued that eavesdropping of this sort is a search without a warrant and is therefore unconstitutional.41 The Supreme Court agreed.42

The Court’s finding marked a conceptual breakthrough for search and seizure law. In *Katz*, the Court set out the rule that whether government surveillance is a Fourth Amendment search depends on whether a reasonable person would have been justified in assuming privacy.43 Previously, the Court had read the text of the Fourth Amendment quite literally and held that unless law enforcement agents physically intruded into houses, papers, or effects, there was no search.44 The Fourth Amendment thus had been tied very closely to the notion of trespass. The new standard was intended to broaden the scope of Fourth Amendment protection. As the *Katz* majority wrote, “once it is recognized that the Fourth Amendment protects people—and not simply ‘areas’—against unreasonable searches and seizures it becomes clear that the

38. For a similarly pessimistic view, see Skok, supra note 5, at 76: Rigid adherence to the two-prong *Katz* expectation of privacy test requires a Net user to establish a subjective expectation of privacy in her clickstream data as a prerequisite for Fourth Amendment protection. However, it will ultimately be impossible for Net users to hold such an expectation due to the lack of privacy protection on the Net.
40. *Id.*
41. *Id.* at 349.
42. *Id.* at 358.
43. *Id.* at 359.
44. See Goldman v. United States, 316 U.S. 129, 135 (1942) (holding that the use of an eavesdropping device that was placed on the exterior wall of an office did not violate the Fourth Amendment), *overruled by Katz* v. United States, 389 U.S. 347 (1967); Olmstead v. United States, 277 U.S. 438, 464 (1928) (holding that warrantless wiretapping of a residential phone line does not violate the Fourth Amendment because “[t]he evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants”), *overruled by Katz* v. United States, 389 U.S. 347 (1967). For a more detailed discussion of these early search cases, see Robert S. Pasley, *Privacy Rights v. Anti-Money Laundering Enforcement*, 6 N.C. BANKING INST. 147, 159-65 (2002).
reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure." This opened up the possibility that the Fourth Amendment could provide protection against nonphysical intrusions, such as the electronic eavesdropping in *Katz*.

Justice Harlan’s concurrence in *Katz* supplied the rule that is used to apply the principles set out by the majority. He wrote that “there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’” One part hinges on the actual belief of an individual, and the other part is a societal litmus test.

The second prong has been at the heart of much litigation. A feature of this part of the *Katz* test is that it offers courts little concrete guidance on how courts should rule in particular cases, since what society deems reasonable is such an amorphous concept. Beginning in *Katz* itself and continuing through later cases, the Court began to anchor the reasonable expectations test by announcing what society deems reasonable. Crucially, in *Katz* the Court stated that “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” As David J. Solove put it: “The Court’s current conception of privacy is as a form of total secrecy.” The voluntary revelation principle limited the discretion of lower courts to find expectations of privacy reasonable. It was only the first in a series of privacy maxims the Court set out.

It is important to notice that *Katz* is potentially at loggerheads with itself. It does not allow for the possibility that some facts that individuals reveal to others, such as the intimate details concerning one’s medical history, may still be facts that “society” generally considers private. Instead, *Katz* gives us both a flexible test (the Fourth Amendment protects what society deems private) and an immutable principle (but this protection can never include things voluntarily exposed to the public) that do not completely harmonize. Though this contradiction was not outcome-determinative in *Katz*, its ramifications would become of major significance in cases to come.

*Katz* sets up the question courts must answer: Do individuals have a reasonable expectation of privacy in the information possessed by ISPs? Further, the voluntary revelation principle casts doubt on the reasonableness of

46. See id. at 358.
47. Id. at 361 (Harlan, J., concurring).
48. Id.
49. The Harlan test was incorporated as the majority rule in *California v. Ciraolo*, 476 U.S. 207, 211 (1986).
52. See *infra* Part I.A.2-3 for a discussion of others.
this expectation to the extent that individuals voluntarily expose information to their ISPs. Since other cases further restrict the ability of courts to consider an expectation of privacy reasonable, these cases will be discussed next.

2. Communications privacy part II: pen registers, Smith v. Maryland.

*Katz* recognized a right to privacy in the content of one’s telephone conversations. Twelve years later, in *Smith v. Maryland*, the Court found that there is no Fourth Amendment interest in the telephone numbers one dials. Michael Lee Smith robbed Patricia McDonough and then proceeded to call her repeatedly, identifying himself as the robber. At police request the phone company installed a pen register, a device that records the phone numbers of incoming and outgoing calls associated with a particular phone line, on Smith’s phone line. Smith argued that this warrantless surveillance violated his reasonable expectation of privacy as set out in *Katz*. The Court disagreed.

The Court offered two explanations for rejecting Smith’s contention that he had a reasonable expectation of privacy. First, it asserted that Smith had no reasonable expectation of privacy because an inquisitive person would have realized that the telephone company is capable of recording phone numbers. It wrote that:

> Telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes.

The privacy maxim underlying this argument is that technological possibility determines what one can reasonably expect to be private.

The Court suggests that it took this approach because it did not want a telephone company’s choice about what information to collect to take on constitutional significance. The Court wrote:

> The fortuity of whether or not the phone company in fact elects to make a

---

54. See id. at 745 (holding that "in all probability [Smith] entertained no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, the expectation was not 'legitimate'").
55. Id. at 738.
56. Id. at 737.
57. "A pen register is a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses caused when the dial on the telephone is released. It does not overhear oral communications and does not indicate whether calls are actually completed." United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977).
58. Smith, 442 U.S. at 737-38.
59. Id. at 744-45.
60. Id. at 743.
61. Id.
quasi-permanent record of a particular number dialed does not, in our view, make any constitutional difference. . . . We 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 the billing practices of a private corporation.62

In addition to the danger that reliance on routine business practice will lead to arbitrariness in what is protected under the Fourth Amendment, the adoption of a "routine business practice" standard would provide an incentive for companies to collect as little information on their customers as possible, at least those customers who place high value on their privacy.

The second reason the Court advanced in finding that Smith had no reasonable expectation of privacy in the phone numbers he dialed was that phone numbers are not communication "content." The Court distinguishes Smith:

[...]

The net result of Katz and Smith is that the Court subdivides a technologically enhanced communication into parts that are protected under the Fourth Amendment and parts that are not. The content of a phone conversation is protected under Katz, but dialed phone numbers are not protected under Smith. Thus, law enforcement agents must obtain a warrant to access some parts of a communication, but need not do so to access others.64

For purposes of evaluating data retention under the Fourth Amendment Katz and Smith provide the following framework. The framing question is whether one has a reasonable expectation of privacy in data transmitted through an ISP. One cannot have a reasonable expectation of privacy if that information is voluntarily revealed, or if an inquiring user would realize that an ISP is technically capable of monitoring communications, unless the information captured can be said to be communication content.

At this point, a tension in the doctrine is noticeable. In some circumstances,
the two principles the Court sets out in *Smith*—that technological possibility determines what privacy expectations are reasonable and that people reasonably expect the content of their communications to be protected—lead to different conclusions on whether a privacy expectation is justified. 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. Given the fact that live police shows, real trials, and movies based on these events saturate pop culture, most people know that it is technologically possible to eavesdrop on the content of a phone conversation. This public awareness must have been all the more prevalent when *Katz* was decided, for direct dialing for long distance was a relatively new phenomenon—one was usually obliged to interact with an operator who would connect the call.

In any case, *Katz* sets out the general framework for evaluating what is a Fourth Amendment search. *Smith* and *Katz* together speak to the special context of communications privacy. The Court has not ruled on a communications record retention case. However, it has ruled on mandatory records retention in the context of government-mandated banking records retention. These

65. *See Smith*, 442 U.S. at 742 ("All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills.")


Although *Katz* and *Smith* are in tension, there are at least two ways to reconcile them. One is to acknowledge that the Supreme Court's observation of a phenomenon changes that which is observed. If the Supreme Court declares that an expectation of privacy in a given area is "reasonable" that is all the more reason to believe that it is. Thus, a Court opinion has a reinforcing circularity. On this ground, the important distinction between phone numbers and the content of a telephone conversation is the preexisting *Katz* decision itself.

A second way to reconcile the two rulings is to seize upon the content/noncontent distinction made in *Smith* to argue that, although the Court does not make it explicit, these holdings are predicated on some normative understanding, lurking in the background, of what Fourth Amendment privacy entails. In *Smith* the Court writes that the use of a pen register is not a search because pen registers do not reveal the purpose of the call nor the identities of the callers. 442 U.S. at 741 ("Neither the purport of any communication between the caller and the recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.") (quoting United States v. N.Y. Tel. Co., 434 U.S. 159, 167 (1977)). Hence, the information that pen registers capture is inherently less personal and intimate and therefore less valuable and less deserving of Fourth Amendment protection than communications content. This is a relatively weak argument, however, for the Court has never articulated what notion of privacy underlies the Fourth Amendment.

banking record retention cases will be discussed next.

3. Record retention: The bank cases.

The Court's financial privacy jurisprudence arose in reaction to the passage of the Bank Secrecy Act of 1970, which required banks to record the identities of their customers and to keep records of certain financial transactions. Both banks and investors filed suit. The Court rejected all of their Fourth Amendment claims.

The banks' tenuous claim was that, because they were being compelled by the government to keep records, they were in effect acting as government agents in seizing customer records without a warrant and that this violated their Fourth Amendment rights. The Court rejected this argument, pointing out that since banks were parties to these transactions, which took place in the normal course of business, they could hardly be said to be seizing anything.

The depositors argued that, by requiring banks to maintain records on customer financial transactions, the government was doing an end run around the necessity of obtaining a warrant before searching individuals' private papers. The Court rejected the assertion that the government was accessing

69. Shultz, 416 U.S. at 31.
70. The bankers' claims were most extensively addressed in Shultz. Miller focused on the rights of depositors. In Miller, while putting out a fire in Miller's warehouse, law enforcement officers discovered that it contained an illegal distillery. Miller, 425 U.S. at 437. The police launched an investigation in which they subpoenaed Miller's bank records. Since the subpoena was arguably defective, Miller asserted that his Fourth Amendment rights would be violated unless his bank records were suppressed. Id. at 438. The Court disagreed, stating that the validity of the subpoena was irrelevant since depositors have no Fourth Amendment interest in records maintained by banks. Id. at 443.
71. The development of the Court's financial privacy jurisprudence was brought to a halt when the Right to Financial Privacy Act of 1978 granted more privacy protection to consumers under federal statutory law than the Constitution required. Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (1978). For a good overview of the current statutory scheme governing data retention by government see Solove, supra note 23, at 1138-51. As Solove points out, the Bank Secrecy Act is not the only context in which government has mandated records retention when it found that private voluntary efforts did not adequately support its purposes. For example, Congress places requirements on employers to collect certain information to facilitate the collection of overdue child support. Id. at 1101.
72. Shultz, 416 U.S. at 52-53 ("Plaintiffs urge that when the bank makes and keeps records under the compulsion of the Secretary's regulations it acts as an agent of the Government, and thereby engages in a 'seizure' of the records of its customers.").
73. Id. at 48 ("The bank plaintiffs proceed from the premise that they are complete bystanders with respect to transactions involving drawers and drawees of their negotiable instruments. But such is hardly the case.").
74. Miller, 425 U.S. at 441. This argument relies heavily on the fear of a slippery
individuals' private papers on two grounds. First, the Court found it significant that the records were in the possession of the banks. The Court asserted that "[o]n their face, the documents subpoenaed here are not respondent's 'private papers.' . . . Instead, these are the business records of banks." Second, the Court declined to extend the depositors' Fourth Amendment rights to their bank records because the depositors voluntarily engaged in banking, admonishing that "in Katz the Court also stressed that '[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.'"

While it seems harsh to consider information revealed in the course of banking to be voluntarily revealed, given how necessary banking services are to modern day life, the Court may have felt it had little choice. Record keeping requirements are integral to the government's regulation of complex industries, a fact the Court acknowledges in its opinion in Shultz:

While an Act conferring such broad authority over transactions such as these might well surprise or even shock those who lived in an earlier era, the latter did not live to see the time when bank accounts would join chocolate, cheese, and watches as a symbol of the Swiss economy. Nor did they live to see the heavy utilization of our domestic banking system by the minions of organized crime as well as by millions of legitimate businessmen.

Given the increasing power and complexity of private institutions, the Court did not want to constitutionalize an impediment to effective law enforcement.

Having established that there is no Fourth Amendment interest implicated by data retention requirements, these banking cases cleared the way for two sorts of government action. First, they established that the Fourth Amendment does not bar the government from ordering that private parties maintain records for government use. Second, they determined that it is constitutional for government to then access these records without any judicial oversight.

---

75. Id. at 444:
By requiring that such records be kept by all banks, the Bank Secrecy Act is not a novel means designed to circumvent established Fourth Amendment rights. It is merely an attempt to facilitate the use of a proper and long-standing law enforcement technique by insuring that records are available when they are needed.

76. Id.

77. Id. at 440.

78. Id. at 442 (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).


The Fourth Amendment cases are not without internal contradiction. Nevertheless, it is possible to piece together a framework that is useful for our analysis of government-mandated record keeping by ISPs. The two questions raised in *Katz* frame the inquiry. First, did the user believe his acts were private? Second, was this belief reasonable? The answer to the second question can be guided by reading together the Court's communication and data retention precedents, which indicate that the Court would fail to find a reasonable expectation of privacy if the following four conditions were met: First, the records are in the possession of a third party; second, the records were voluntarily turned over to that third party; third, an inquiring user would have realized that the technological context enabled third-party access; and fourth, the records do not capture communication "content." Part I.B of this Note will analyze the case of Internet records according to this framework.

B. Application to the Internet

The range of activity that users engage in online complicates the Fourth Amendment analysis of data retention. The Supreme Court recognized this diversity in *Reno v. ACLU* when it wrote that the Internet "constitutes a vast platform from which to address and hear from a worldwide audience of millions of readers, viewers, researchers, and buyers." Using the Internet can involve reading web pages, emailing, joining online chat rooms, and instant messaging, to give just a few examples.

---

80. See *Miller*, 425 U.S. at 440 (noting that the papers at issue were "the business records of the banks").

81. See id. at 442 (noting that the documents "contain[ed] only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business"); *Katz v. United States*, 389 U.S. 347, 351 (1967) ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.").

82. See *Smith v. Maryland*, 442 U.S. 735, 743 (1979) (noting that "it is too much to believe that telephone subscribers, under these circumstances, harbor any general expectation that the numbers they dial will remain secret").

83. See id. at 741 (noting that "pen registers do not acquire the contents of communications").


85. "A chat room is a Web site, or part of a Web site, or part of an online service such as America Online, that provides a venue for communities of users with a common interest to communicate in real time." *Look it up: Definitions for thousands of the most current IT-related words*, at http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci541370,00.html (last visited June 21, 2003).

86. Instant messaging is:

[T]he ability to easily see whether a chosen friend or co-worker is connected to the Internet and, if they are, to exchange messages with them. Instant messaging differs from ordinary e-mail in the immediacy of the message exchange and also makes a continued exchange
These activities can be classified and compared based on a number of characteristics such as the spontaneity, exclusivity, and interactivity of the communication. For example, instant messaging and chatting are both relatively spontaneous, like a phone call. Also, both email and instant messaging can be relatively exclusive, like a letter. The reason why one might wish to engage in this classification exercise is that this is what courts often do when deciding how to treat a new medium. For instance, one could ask whether sending an email is more like mailing a letter in a sealed envelope, or more like sending a postcard. If the Court applies the standards of review of the letter, it may recognize a reasonable expectation of privacy in the content of an email. If it views email as being like a postcard, then it will not. In the context of electronic communication, however, this analogizing is a far from trivial exercise. The contours of this universe are determined by code. For instance, the security of a given email can vary. An email can be encrypted or unencrypted; sent to one or many users; it can be stored on a third party’s server indefinitely or deleted after a user downloads it. The genus of electronic communication may not break down so easily into a series of categories that analogize neatly to preexisting communications media. In any event, the caveat to note here is that “using the Internet” can mean different things in different contexts, and consequently there may not be a one-size-fits-all Fourth Amendment analysis.

Look it up: Definitions for thousands of the most current IT-related words, at http://searchnetworking.techtarget.com/sDefinition/O,,sid7_gci510743,00.html (last visited June 21, 2003).

87. See also Keeping Secrets, supra note 3, at 1592-94 (detailing what the author describes as the six basic methods of online communication).

88. See infra Part I.C for a discussion of how lower courts have analogized various forms of online communication to more established communication methods. See Keeping Secrets, supra note 3, at 1597, for a discussion of analogies that have been drawn between new methods of communication over the Internet and preexisting methods.

89. See Keeping Secrets, supra note 3, at 1597 (“Individuals retain a reasonable expectation of privacy in sealed first-class mail sent through the postal system, but because anyone can read the contents of a postcard, an expectation of privacy in its contents would be unreasonable and a law enforcement officer’s reading it is thus not a search.”).

90. See Ex Parte Jackson, 96 U.S. 727, 733 (1877) (“Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles.”).

91. Smith v. State, 389 A.2d 858, 873 (Md. 1978) (Cole, J., dissenting) (“While use of the postal service involves essentially public facilities where any writing on the outside of an envelope or on a postcard can be easily read by postal employees, telephones are placed in the home to provide privacy regarding the parties to and content of a conversation.”), aff’d, Smith v. Maryland, 442 U.S. 735 (1979).

92. The Law of the Horse, supra note 14, at 509.
1. Are the records in the possession of a third party?

Turning to the analytical framework, the first question the Court has asked when reviewing the privacy of records is whether they are in the possession of third parties. In our hypothetical this is beyond debate because it assumes record possession by ISPs.

2. Were the records voluntarily turned over to the third party?

The second question is whether the user voluntarily revealed the information the records contained. The least privacy protective answer to this question is that since using the Internet is voluntary, any information revealed while using the Internet is voluntarily revealed. This answer hews most closely to the Court's reasoning in the bank records cases, where it found that since banking is optional, any information conveyed in the course of banking is voluntarily revealed. The fact that banking services are a prerequisite to participation in modern life does not enter into the Court's calculus.

The effect of such a perspective would be to consider all online activity to be voluntarily revealed, save for the rare instance in which someone's hand is literally being forced to the keyboard, or where an individual reasonably expects (such as through the use of advanced encryption) that it is not technologically possible for his activity to be monitored. For although cyberspace and real space share many characteristics—as the Court has noted they can both serve as forums for democratic debate and for commerce—there is one crucial difference: existence in cyberspace is optional. Indeed, though the number is shrinking, there is a residual percentage of Americans who never use email.

Under this strict interpretation of the term "voluntary," the permissible extent of surveillance would be bounded by the mandates of congressional statutory enactments and the limits of technological possibility. Further, when it comes to surveillance of most Americans most of the time, Congress could win this tug of war rather handily. Congress need not compete with technology because Congress can simply regulate technology. It has already done so on numerous occasions. For instance, when telecommunications companies started using digital technology, the government's traditional methods of wiretapping were no longer effective. To restore the power of law enforcement agencies, the

93. See United States v. Miller, 425 U.S. 435, 442 (1976) (holding that bank depositors have no Fourth Amendment interest in bank records); see also discussion supra Part I.A.2.
95. When asked "Do you ever go online to access the Internet or World Wide Web to send and receive e-mail?" 84% said yes, while 16% responded no. PRINCETON SURVEY RESEARCH ASSOCIATES, Oct. 6, 2002, available in LEXIS Academic Universe (accession number 0415182).
government mandated that companies use technology that enabled surveillance.96 Further, Congress has criminalized most uses of technology designed to circumvent copyright protections.97 Just as the government has regulated these technologies, it could criminalize technology that interferes with government's ability to monitor Internet usage.98

Currently, there is a two-tier Internet privacy regime. There are those whose online actions are transparent because they rely on default browser and email settings, and there are those whose actions are concealed because they have invested the added time needed to learn about and use encryption technology.99 A skeptic could classify these two groups as "the naked and the damned," since the former reveal everything and the latter engage in obfuscation techniques that the government has a strong incentive to criminalize.

3. Would an inquiring user have realized that the technological context enabled third-party access?

The next factor in the analytical framework is whether an inquiring user would realize that the technological context of the Internet enables third-party observation. Another way to get at this question is to ask how much research it takes to learn that the unencrypted techniques most people use to surf the Internet are insecure. The answer is that it does not take much research at all. There are several readily accessible sources of information on Internet security. The first is the Internet itself. By typing a straightforward phrase like "Internet privacy" or "Internet security" into a search engine, one can uncover a wide range of homepages by nonprofit organizations offering a wealth of information online.100 These searches also turn up commercial sites

98. For a more extensive list of federal laws regulating the design of certain technologies, see The Law of the Horse, supra note 14, at 531.

Encryption offers Internet users an extraordinarily powerful tool to create privacy in cyberspace. When a computer file is encrypted using software such as PGP, the software scrambles the files into an unreadable form, known as 'ciphertext.' No one, not even the government, can unscramble the message back into readable form (known as 'plaintext') without the encryption key.

100. For example, as of January 23, 2003, typing this term into the search engine Google produced the following among the top ten results: the home page of the Electronic Privacy Information Center, a privacy rights advocacy organization whose website offers extensive information about the risks associated with using the Internet; the Federal Trade Commission's Privacy Initiative Web page, which includes resources explaining how to protect children's privacy online; the homepage of Zero Knowledge, a for-profit entity
offering both a description of the Internet’s current privacy weaknesses and products to enable less traceable Internet usage.\textsuperscript{101} The second resource is the privacy policy of the user’s own ISP. Most ISPs have such policies that detail the security of their systems. For example, one major ISP, America Online ("AOL"), publishes its privacy policy on the Internet.\textsuperscript{102} AOL informs its users that:

AOL does not read or disclose private communications except to comply with valid legal process such as a search warrant, subpoena or court order, to protect the company’s rights and property, or during emergencies when we believe physical safety is at risk. Of course, what you write or post in public or member chat rooms and message boards is available not only to AOL, but to all members.\textsuperscript{103}

A discerning AOL user would realize that although AOL does not routinely peruse its user’s emails, it has the capacity to do so and will disclose these emails not only in response to legal process, but whenever it determines that disclosure is necessary “to protect itself,“\textsuperscript{104} and when “physical safety“\textsuperscript{105} is at risk. Of course, the universe of what constitutes a risk to “physical safety” is undetermined, will presumably be determined by AOL on an ad hoc basis, and has been expanding rapidly in the post-September 11 world.

In \textit{Smith}, the Court stated that routine business practice should not determine when individuals may reasonably expect privacy.\textsuperscript{106} That AOL does not routinely read emails, therefore, is irrelevant. Though not all ISP user agreements will be as easy to dissect as AOL’s, in general it seems safe to conclude that there are many ways an inquiring user can learn that the Internet is an insecure means of communication.

\begin{itemize}
\item \textsuperscript{101} These searches were done on the websites discussed supra note 100.
\item \textsuperscript{103} \textit{Id.}
\item \textsuperscript{104} \textit{Id.}
\item \textsuperscript{105} \textit{Id.}
\item \textsuperscript{106} Smith v. Maryland, 442 U.S. 735, 744-45 (1979) ("Petitioner concedes that if he had placed his calls through an operator, he could claim no legitimate expectation of privacy. We are not inclined to hold that a different constitutional result is required because the telephone company has decided to automate.") (internal citation omitted).
\end{itemize}
4. Do the records capture communication "content"?

The final part of the framework inquires whether the records capture communication "content." To the extent that they do, Katz, as interpreted by Smith, indicates that the Court may at the least require a warrant for government access to these records. The extent to which this would provide protection for Internet activity is unclear because the boundary between the content of a communication and its noncontent aspects is itself unclear. As Justice Stewart pointed out in his dissent in Smith, even the phone numbers one dials have some content, in that a list of the phone numbers a person dials "easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."

The ambiguity of what is content and what is not is particularly acute in the context of the Internet. Take the example of an email. Is the body of an email content? What if the email starts with "Dear John" and ends with "Yours Truly, Jane"—are these greetings content or are they noncontent information like telephone numbers? What about the "to:" and "from:" lines of an email? In some sense they could be classified as noncontent information since they are necessary to the routing of the email, but they provide more information than a phone number because email addresses are regularly tied to one particular individual whereas many telephones are shared by a variety of individuals. As Professor Susan Freiwald points out, an email's subject line and the name of a file attached to an email are also arguably content. Knowing whether an email contains an attachment, and if so, the name of the attachment file (for example, "CommunistManifesto.doc," "XXXgirlz.jpg"), allows law enforcement officials to glean more detailed information about what one is doing than is apparent through knowledge of the phone number one dials.

107. See id. at 741 (distinguishing learning what numbers are dialed from a particular telephone, which the Smith court held could be done without a warrant, from hearing the words of a conversation using sense-enhancing technology, which the Katz court held could not be done without a warrant, on the grounds that a pen register does not detect communication content. "Yet a pen register differs significantly from the listening device employed in Katz, for pen registers do not acquire the contents of communications.").

108. See generally Freiwald, supra note 64, at 953-58 (discussing how one might draw the divide between content and noncontent aspects of a communication in the context of the Internet). For an argument that no such distinction can be drawn in the context of the Internet see John Gilmore's Politech posting on this subject, Apr. 9, 2002, at http://www.politechbot.com/p-03368.html.

109. Smith, 442 U.S. at 748 (Stewart, J., dissenting).

110. See Freiwald, supra note 64, at 956 (discussing how "use of the rapidly growing Internet and commercial on-line services presents difficult classification questions" as to what is content).

111. See id. at 957 (noting how a downloaded "program itself might be considered the communication contents, and all other information, such as the time, date and duration of the download and the downloader's identity, would constitute the communication attributes").
Email, instant messaging, and other online activities analogous to "speaking" are probably the closest match to the Court's communications cases. It is still more uncertain whether other forms of online activity would be covered by the concepts set out in *Katz* and *Smith*. For instance, much online activity involves reading and listening in situations where the purveyor of information, such as the author of a web page, may not actively establish a relationship with the listening or reading party.\(^1\) Is reading a web page a "communication"? If so, does it have content and noncontent aspects? These questions will have to be resolved. While the principles set out in *Katz* and *Smith* may require that government authorities obtain a warrant before accessing some kinds of electronic records, such as the "content" of emails, it is much less certain that other aspects of Internet use such as Web browsing would fall under *Katz* and *Smith*. Further, although these cases may be read to require a warrant to access these customer records, they are probably no bar to the retention of the records.

**C. Lower Court Decisions**

No United States court has decided the constitutionality of government-mandated archiving of Internet usage. However, a few courts have addressed the closely related question of whether users have a reasonable expectation of privacy in information in the possession of ISPs.\(^2\) These questions are

---

112. See id. (discussing how all of the information received in a download "would be considered communication attributes, even though there might be no associated communication contents").

113. Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (holding that "plaintiffs . . . lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the systems operators"); United States v. Hambrick, No. 99-4793, 2000 U.S. App. LEXIS 18665, at *12 (4th Cir. Aug. 3, 2000) (holding that "a person does not have an interest in the account information given to the ISP in order to establish an e-mail account, which is non-content information"); United States v. Cox, 190 F. Supp.2d 330, 332 (N.D.N.Y. 2002) (noting that "courts have already held that criminal defendants have no Fourth Amendment privacy interest in subscriber information given to an internet service provider"); Kelleher v. City of Reading, 2002 WL 1067442, at *8 (E.D. Pa. May 29, 2002) (finding no reasonable expectation of privacy where employment guidelines disclaim any privacy in communication through work email); Garrity v. John Hancock Mut. Life Ins. Co., 2002 WL 974676, at *1 (D. Mass. May 7, 2002) (holding that there is no reasonable expectation of privacy in work email where office had policy explicitly disclaiming any expectation of privacy); United States v. Kennedy, 81 F. Supp.2d 1103, 1110 (D. Kan. 2000) ("Defendant's constitutional rights were not violated when Road Runner divulged his subscriber information to the government."); United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) ("[T]he transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant. However, once the transmissions are received by another person, the transmitter no longer controls its destiny."); Smyth v. Pillsbury Co., 914 F. Supp. 97, 101 (E.D. Pa. 1996) ("Once plaintiff communicated the alleged unprofessional comments to a second person (his supervisor) over an e-mail system which was apparently utilized by the
intertwined because courts would probably be less inclined to find archiving objectionable if there is no privacy interest in the retained information.

In many cases, lower courts have used the voluntary revelation principle to find that there is no legitimate expectation of privacy in online activity. For instance, courts have found no privacy right in email that has been opened by its recipient, or email sent through an ISP that explicitly disclaims that communications are private. Additionally, courts have found that there is no reasonable expectation of privacy in the information users submit to their ISPs in order to establish an account. For example, in United States v. Hambrick, David Hambrick’s subscriber information was obtained from his ISP with what the government later conceded was an invalid subpoena. The court held that Hambrick had no constitutionally protected privacy interest in the subscriber information because it was “merely third-party business records.”

Relying on the bank records retention cases, the court wrote:

While the Court is aware of the “revolutionary” nature of the Internet as well as the vast extent of communications it has initiated, the information at issue in this case is not distinguishable from the materials in *Miller* and *Smith*, as the government merely obtained non-content information that was part of MindSpring’s business records.

On the other hand, where an ISP’s privacy policy and actual practice do suggest that communications are private, one court held that a user had a legitimate expectation of privacy in the message he sent and received. The entire company, any reasonable expectation of privacy was lost.”; United States v. Monroe, 52 M.J. 326, 330 (2000) (holding that a service member had no reasonable expectation of privacy in email stored on a government computer where he had been warned that e-mail was subject to monitoring); United States v. Maxwell, 45 M.J. 406, 417 (A. Ct. Crim. App. 1996) (holding that an individual “possessed a reasonable expectation of privacy, albeit a limited one, in the e-mail messages that he sent and/or received on AOL”); Hause v. Commonwealth, 83 S.W.3d 1, 12 (Ky. App. 2001) (finding that “an individual . . . lacks a Fourth Amendment privacy interest in his subscriber information because he communicated it to the system’s operators”); United States v. Geter, 2003 WL 21254249, at *5 (N.M. Ct. Crim. App. May 30, 2003) (finding no expectation of privacy in work email); Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. 2001) (holding that there is no legitimate expectation of privacy in emails once they have been received and then forwarded to others); McLaren v. Microsoft Corp., 1999 WL 339015, at *1 (Tex. App. May 28, 1999) (holding that an employee had no reasonable expectation of privacy in email stored in personal folders on company workstation).


117. *Id.* at *4.

118. *Id.* at *4 n.4.

The transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant. However, once the transmissions are received by another person, the transmitter no longer controls its destiny. In a sense, e-mail is like a letter.\(^{120}\)

The court reached this conclusion even though the email was “stored in a centralized computer until the recipient opens his or her network and retrieves the e-mail.”\(^{121}\) It would have been quite plausible, under these circumstances, to have considered the email “voluntarily revealed” to the ISP storing the message, and to have held that there was no reasonable expectation of privacy on the part of the sender. Instead, the court chose to analogize to the context of postal mail and to provide the same sort of privacy context for electronic mail.

These cases show how lower courts are grappling with applying privacy maxims developed against the background of one technical reality to a new context. They also illustrate the difficulty of simultaneously staying true to the voluntary revelation principle and replicating in cyberspace the quantum of privacy available in real space communication, a difficulty that would only be more pronounced in the case of government-mandated archiving of Internet usage.

**D. Conclusion on the Fourth Amendment**

Through the use of the four-part framework set out above, this Note has endeavored to show that current Fourth Amendment doctrine is unlikely to pose a bar to government-mandated data retention by ISPs.\(^{122}\) To use the Internet is to voluntarily communicate over an insecure network whose design is predicated on revealing information to third parties. The Court’s protection of communications content as set out in *Katz* and *Smith* may lead the Court to require that law enforcement agents obtain a warrant before reading communications content, but it is unclear what will be considered content, and in any case this only requires judicial review before government can access retained records and is no bar to compulsory data retention itself.\(^{123}\)

---

120. *Id.* at 418.
121. *Id.*
122. For a more optimistic take using a different analytical framework, see *Keeping Secrets*, supra note 3, at 1601.
123. If accessing communications “content” is considered a Fourth Amendment search, then a court might require additionally that the warrant identify the material to be searched with “scrupulous exactitude.” *See Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (“Where the materials sought to be seized may be protected by the First Amendment, the requirements of the Fourth Amendment must be applied with ‘scrupulous exactitude.’”) (citing *Stanford v. Texas*, 379 U.S. 476, 485 (1965)); *see also* *Roaden v. Kentucky*, 413 U.S. 496, 506 (1973) (holding that the warrantless seizure of a film being exhibited at a theater did not meet the requirement of “scrupulous exactitude”); *Tattered Cover, Inc. v. City of*
E. Reasons to Distinguish the Internet from Real Space

There are several arguments that suggest that the Court should recognize the inherent technical differences between the Internet and real space and exercise its discretion in order to develop a contextually nuanced approach to determining when privacy expectations are reasonable. This is a preferable alternative to importing wholesale an old framework into a new technological world that bears not only similarities but also significant and salient differences from its real-world analog.

First, the Court's current approach to determining what is a search, predicated primarily on the idea of voluntary revelation, is highly unstable. For example, over the past fifty years technology has enhanced law enforcement at the expense of privacy. The trend need not always run this direction. Future technological developments, such as perhaps the widespread availability of public key encryption, may enhance privacy. It is hard to justify as a constitutional principle a standard that will allow widely varying degrees of surveillance of human activity, depending on the current technological cycle. The Court recognized the importance of stability in Smith when it declined to "make a crazy quilt of the Fourth Amendment" by giving constitutional weight to corporate privacy practices. Technological possibility is ultimately no more reliable than these business practices. If there is to be a stable zone of privacy on which individuals can rely, then the Court cannot depend on the contours of technological possibility to do its work for it. Instead, the Court must grapple with what constitutes a "reasonable" search, perhaps by articulating a substantive value of privacy.

Second, Internet records should be distinguished from banking records because they are much more revealing. The range of human activity taking place online is vast compared to that which is reflected in bank records. While banking records do provide information about an individual's lifestyle, ultimately they communicate in dollars and cents. Internet users can read

---

Thornton, 44 P.3d 1044, 1047 (Colo. 2002) (requiring law enforcement officials to make a heightened showing before taking actions, including searches and seizures, that chill speech).
124. See Solove, supra note 23, at 1095 ("The government is increasingly contracting with private sector entities to acquire databases of personal information.").
125. See generally STEFAN A. BRANDS, RETHINKING PUBLIC KEY INFRASTRUCTURES AND DIGITAL CERTIFICATES: BUILDING IN PRIVACY (2000) (describing methods by which individuals can communicate with a high degree of privacy).
127. This is essentially what Skok advocates. See Skok, supra note 5, at 82 ("[C]ourts should focus on the historic context of the Fourth Amendment and the intent of its Framers. Government monitoring and analysis of clickstream data is closely analogous to the general searches which the Framers sought to curtail in enacting the Fourth Amendment.").
128. In the context of elections, the Court has stated that revealing identity information concerning election-related financial activity is less revealing than materials individuals have written expressing ideas. See McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 355
anti-establishment political literature, agitate and organize for unpopular causes, or get help with addictions or other ailments, without fear of social stigma. Against the law-enforcement benefits it might bring, one must weigh the chilling effect it would have on such activity. We would all use the Internet in the knowledge that we were leaving behind an indelible record that at some future time could be used against us. Possible use for criminal prosecution or discriminatory profiling is one worry. Another is that we might be judged for actions today by the standards of a different era.

II. THE FIRST AMENDMENT

Since data retention would make all Internet activity traceable, its successful implementation would eliminate anonymity online. Further, it would be a regulation of unprecedented scope because it would eliminate the anonymity of those receiving information as well as those conveying information. The First Amendment is a potentially formidable obstacle to mandatory data retention because the Court has found that the Amendment extends to anonymous speech activity and has applied strict scrutiny to government inhibitions of this right.

This Part will first examine the precedent-setting cases to determine how the Court has valued anonymous speech activity and will then explore whether eliminating anonymity online through data retention would be

(1995):
A written election-related document—particularly a leaflet—is often a personally crafted statement of a political viewpoint. As such, identification of the author against her will is particularly intrusive; it reveals unmistakably the content of her thoughts on a controversial issue. Disclosure of expenditure and its use, without more, reveals far less information.

See supra notes 3-14 and accompanying text.

129. See McIntyre, 514 U.S. at 342 (striking down a law that forbid the distribution of anonymous election-related literature). The Court clarified that regulation of identifying information is properly considered content-based regulation when it wrote that "an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment." Id. Therefore, regulation of identifying information is subject to strict scrutiny. Id.; see also Gibson v. Florida Legislative Investigation Comm., 372 U.S. 539 (1963) (rejecting an attempt of a Florida legislative committee to require the NAACP to produce its membership records); Shelton v. Tucker, 364 U.S. 479 (1960) (striking down a state statute requiring that teachers list all of their association memberships in the previous five years); Talley v. California, 362 U.S. 60, 64 (1960) (declaring unconstitutional a blanket prohibition on anonymous handbill distribution); NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 459-60 (1958) (holding that requiring the NAACP to produce its membership records would chill association). But see Buckley v. Valeo, 424 U.S. 1 (1976) (holding that the government's need to ensure the integrity of the elections process outweighed speakers' interest in anonymous speech); State v. Miller, 398 S.E.2d 547 (Ga. 1990) (upholding an antimask statute targeted at mask-wearing for the purpose of intimidation). For further analysis, see discussion infra Part II.A.

130. See infra Part II.A.
Justifiable given the government's need to hold criminals accountable for their online acts.\textsuperscript{132} Thus far, the Court's cases have focused on only two aspects of anonymity: anonymous information-giving\textsuperscript{133} and anonymous association.\textsuperscript{134} In addition to exploring the values that underlie the Court's decisions in these cases, this Part will argue that the same principles and the Court's scattered dicta on the subject support a right to receive information anonymously.

This Part will then explore the right to speak anonymously in light of the new context of the Internet, probing whether the widespread availability of perfect anonymity justifies the use of data retention to prevent speech-based harms such as conspiracy and libel.\textsuperscript{135} Parts II.A and II.B below will endeavor to show that the Court's protection of anonymous speech and anonymous association in real space tacitly depends on the difficulty of achieving true anonymity in real space. In other words, the Court's anonymity-protective talk is cheap because the architecture of real space will do the work of keeping this unaccountable form of speech to a minimum. Because anonymity is substantially easier to achieve on the Internet, this new context raises the cost of the Court's anonymity-protective rhetoric. A review of the precedent-setting cases will show that there are hard, unanswered questions as to how far the Court will go in protecting anonymity when perfect anonymity threatens to be widespread.\textsuperscript{136} This Part concludes that data retention is probably unconstitutional on First Amendment grounds because the Court requires narrow tailoring of government regulations that impinge on speech rights, and data retention is by no means narrowly tailored.

\textbf{A. Anonymous Speech in Real Space}

Part II.A will review cases in which the Court has found a right to convey information anonymously and associate anonymously and will then argue that this protection of anonymity should logically extend to the receipt of information, an important point for purposes of understanding the constitutional implications of data retention, since so much online activity involves reading. Since the foundations for the protection of anonymous speech are most extensively laid out in cases focusing on the right to anonymous information-

\begin{itemize}
  \item[132.] See infra Part II.B.
  \item[133.] See infra Part II.A.1.
  \item[134.] See infra Part II.A.2.
  \item[135.] See infra Part II.B.
  \item[136.] For an argument that the anonymity-enabling aspect of cyberspace is so threatening to the rule of law that true anonymity online ought to be criminalized and that there is no constitutional barrier to this, see George F. du Pont, \textit{The Criminalization of True Anonymity in Cyberspace}, 7 MICH. TELECOMM. & TECH. L. REV. 191, 195 (2001) (arguing "that a narrowly tailored legislative restriction on 'true' anonymity in cyberspace would not violate the First Amendment").
\end{itemize}
giving, these cases will be discussed first.

1. The right to give information anonymously.

In *Talley v. California* and *McIntyre v. Ohio Elections Commission*, the Court announced a right to convey information anonymously, explained the value of anonymous speech, and applied strict scrutiny to government regulations impinging anonymous speech. In *Talley*, the Court confronted the issue of whether it violated the First Amendment for government to place a blanket prohibition on the distribution of anonymous handbills. In *McIntyre*, it addressed a more narrowly tailored statute that prohibited the distribution of anonymous, election-related literature.

In both cases, the government asserted that it had a compelling law enforcement need in ascertaining identity. In *Talley*, the Court noted that the government “has urged that this ordinance is aimed at providing a way to identify those responsible for fraud, false advertising, and libel.” In *McIntyre*, the government argued that requiring pamphleteers to identify themselves was reasonable in the elections context.

Despite the government’s assertions, the Court held in both cases that the First Amendment protects anonymous speech and that this right trumped the government’s proffered need to facilitate easier enforcement of the laws. In the process, it identified three reasons why anonymous speech is valuable. First, anonymous speech helps to limit government power since “[p]ersecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.”

---

137. See *McIntyre v. Ohio Elections Comm’n*, 514 U.S. 334, 338 (1995) (addressing an ordinance that banned anonymous election-related literature); *Talley v. California*, 362 U.S. 60, 64 (1960) (considering an ordinance that “bars all handbills under all circumstances anywhere that do not have the names and addresses printed on them in the place the ordinance requires”).


140. *Talley*, 362 U.S. at 64.


142. Id. at 353 (“We recognize that a State’s enforcement interest might justify a more limited identification requirement, but Ohio has shown scant cause for inhibiting the leafletting at issue here.”); *Talley*, 362 U.S. at 64-65.

143. *Talley*, 362 U.S. at 64.
special utility of anonymous speech for those with unpopular views opens up the argument that government regulations of anonymity are viewpoint discriminatory. 144 Second, the Court recognizes that some people will only participate in debate on important issues anonymously. 145 Writing that "identification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance," 146 the Court acknowledges the utility of anonymous speech in enriching public debate by lowering the risk of contributing. Third, the Court recognizes that good ideas may come from unpopular sources and that allowing ideas to be divorced from the identity of their authors may enable such ideas to be considered without bias. 147

Because the option of speaking anonymously increases both the quantity and diversity of speech, anonymous speech acts as a check on government power. Each of the Court's rationales for protecting anonymous speech is predicated on the notion that distrust of government is healthy. 148 They also lean heavily on the instrumental value of anonymity as a condition that enriches public discourse, rather than, for instance, some notion that anonymous speech is fundamental to individual self-fulfillment.

Even while recognizing the speech-maximizing value of anonymity, the Court's protection of anonymity has not been absolute. When anonymity conflicts with government's ability to advance legitimate state interests, which is not rare because of the inverse relationship between anonymity and accountability, sometimes anonymity loses. 149 In reconciling the right to speak anonymously with the compelling government need to enforce the law, the Court has taken into account a number of factors. First, it considers the value of anonymous speech. 150 In the process, it takes into account whose anonymity is being threatened, extending greater protection to the politically vulnerable; 151 the subject matter of the speech, extending greater protection when the topic is

144. See Tien, supra note 137, at 128-31.
145. Talley, 362 U.S. at 65.
146. Id.
147. See McIntyre, 514 U.S. at 342:
On occasion, quite apart from any threat of persecution, an advocate may believe her ideas will be more persuasive if her readers are unaware of her identity. Anonymity thereby provides a way for a writer who may be personally unpopular to ensure that readers will not pre-judge the message simply because they do not like its proponent.
148. Additionally, in his concurrence in McIntyre, Justice Thomas advanced an originalist argument for a First Amendment right to anonymous speech, asserting that protecting anonymous speech was within the original meaning of the First Amendment. Id. at 359-71 (Thomas, J., concurring).
149. See Buckley v. Valeo, 424 U.S. 1, 72 (1976) (upholding an identification requirement of certain campaign contributors despite its impact on anonymous speech).
150. McIntyre, 514 U.S. at 342; see also supra notes 51-58 and accompanying text.
151. For instance, the Court is more inclined to require identifying information from a candidate for political office than from "individuals acting independently and using only their own modest resources." Id. at 351.
a political issue;\textsuperscript{152} and the likelihood that the speech is libelous.\textsuperscript{153} Second, it scrutinizes whether the identification requirement will actually be effective in permitting the government to achieve its law enforcement goal.\textsuperscript{154} Third, it examines the necessity of the identification requirement, asking whether compelling identity disclosure is the only way government can accomplish its goal.\textsuperscript{155}

It is this third requirement—the lack of an alternate means for achieving a compelling governmental goal, that has led the Court to sanction identification requirements in the past. In \textit{Buckley v. Valeo}, the Court found that the combined government interest in promoting an informed electorate,\textsuperscript{156} stemming actual corruption and the appearance of corruption,\textsuperscript{157} and having the financial data necessary to detect violations of campaign laws\textsuperscript{158} was adequate justification for requiring campaign contributors to identify themselves where there was no other effective way for the government to achieve these goals.\textsuperscript{159}

The different architecture of physical space and cyberspace may make this third factor particularly contentious in the debate over data retention. It is substantially easier to speak anonymously on the Internet than in physical space. In physical space, it is difficult to erase all links to one’s physical person in the process of distributing speech. Handbills must be printed and distributed. A newspaper ad must be paid for. We read about anonymous leafleting cases such as \textit{McIntyre} and \textit{Talley} because the authorities identified Margaret McIntyre and Manuel D. Talley. Although the Court has confronted the issue of anonymity before, it has not confronted the widespread availability of \textit{perfect} anonymity. It is exactly this possibility that cyberspace has created.

\textsuperscript{152} "A public question clearly cannot be the victim of character assassination." \textit{Id.} at 353 n.16 (quoting People v. White, 506 N.E.2d 1284, 1288 (Ill. 1978)).

\textsuperscript{153} \textit{Id.} at 351 (acknowledging the state’s “assuredly legitimate” governmental interest in deterring “the making of false statements by unscrupulous prevaricators”).

\textsuperscript{154} This was a concern in \textit{McIntyre}. As the Court stated, “Nor has the State explained why it can more easily enforce the direct bans on disseminating false documents against anonymous authors and distributors than against wrongdoers who might use false names and addresses in an attempt to avoid detection.” \textit{Id.} at 352-53.

\textsuperscript{155} \textit{Id.} at 352 (using the apprehension of Margaret McIntyre as proof that “the absence of the author’s name on a document does not necessarily protect either that person or a distributor of a forbidden document from being held responsible for compliance with the Election Code”).

\textsuperscript{156} 424 U.S. 1, 66-67 (“Disclosure provides the electorate with information . . . in order to aid the voters in evaluating those who seek federal office.”).

\textsuperscript{157} \textit{Id.} at 67 (“[D]isclosure requirements deter actual corruption and avoid the appearance of corruption by exposing large contributions and expenditures to the light of publicity.”).

\textsuperscript{158} \textit{Id.} at 67-68 (“[R]ecordkeeping, reporting, and disclosure requirements are an essential means of gathering the data necessary to detect violations of . . . contribution limitations.”).

\textsuperscript{159} \textit{Id.} at 72.
2. The right to associate anonymously.

In addition to the right to convey information anonymously, the Court has protected the right to associate anonymously.\(^{160}\) Data retention would effectively eliminate anonymous association online because no group could function there and keep its membership secret. In *NAACP v. Alabama ex rel. Patterson*, the Court found that Alabama could not require the NAACP to disclose its membership lists.\(^{161}\) It recognized that the group’s singular unpopularity would serve as a major deterrent to membership, were members not able to join anonymously.\(^{162}\) Similarly, in *Shelton v. Tucker* the Court invalidated a law that required public school teachers to disclose all of the associations to which they had belonged in the previous five years.\(^{163}\)

As was the case for anonymous information-giving, the Court protects anonymous association because it is instrumental in maximizing speech. As the Court succinctly noted in *Patterson*: “Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association, as this Court has more than once recognized by remarking upon the close nexus between the freedoms of speech and assembly.”\(^{164}\) The Court acknowledges that groups can be capable of expressing ideas more effectively than could their individual members acting alone.\(^{165}\) Therefore, enabling people to form associations anonymously so as to avoid the social stigma that may come with overt group membership helps promote speech.\(^{166}\)

---

160. See Gibson v. Florida, 372 U.S. 539, 558 (1963) (holding that a legislative committee investigating communist activities could not compel the NAACP to disclose its membership list); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 460 (1958) (holding that requiring the NAACP to produce its membership records would chill association).

161. 357 U.S. 449, 466 (1958): We hold that the immunity from state scrutiny of membership lists which the Association claims on behalf of its members is here so related to the right of the members to pursue their lawful private interests privately and to associate freely with others in so doing as to come within the protection of the Fourteenth Amendment.

162. Id. at 462-63 (“[C]ompelled disclosure of petitioner’s Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate, in that it may induce members to withdraw from the Association.”).

163. 364 U.S. 479, 480 (1960) (“An Arkansas statute compels every teacher, as a condition of employment in a state-supported school or college, to file annually an affidavit listing without limitation every organization to which he has belonged or regularly contributed within the preceding five years.”).

164. *Patterson*, 357 U.S. at 460.

165. Id. at 460 (“Effective advocacy of both public and private points of view, particularly controversial ones, is undeniably enhanced by group association.”).

166. The strength of the Court’s protection of anonymous association is particularly evident in *Shelton*, where the Court protects the right to associate anonymously even while acknowledging the “relevance of a State’s inquiry into the fitness and competence of its teachers.” *Shelton*, 364 U.S. at 485.
3. The right to receive information anonymously.

Finally, though the Court has not confronted the question of whether there is a right to receive information anonymously, such a right follows logically from the principles that undergird protection of anonymity in the information-giving and association contexts. As a preliminary matter, the Court has found that "the Constitution protects the right to receive information and ideas." In her seminal article on the subject, Professor Julie E. Cohen explored the question of whether the right to engage in speech activity anonymously properly extends to the receipt of information. Since so much online activity consists of receiving information through reading web pages, it is important to set out these arguments briefly here.

First, the freedom to receive information anonymously has instrumental value in maximizing speech because it widens the audience for speech and also gives would-be speakers uninhibited access to a range of ideas. As Cohen points out: "A central insight that both copyright and literary theory can lend to First Amendment jurisprudence is that the content of one’s speech is shaped by one’s response to all prior speech, both oral and written, to which one has been exposed." Speech is a process of discursive interaction, in which discrete statements build on previous dialogue. Allowing individuals to avoid the stigma associated with particular ideas will permit them to consider these ideas more fully before making their own contributions to public debate.

Second, "the Supreme Court’s opinions reflect a sense that individual freedom to read and think lie at the heart of the zone of activity that the First Amendment protects." In Denver Area Educational Telecommunications Consortium, Inc. v. FCC, the Court recognized this obliquely when it struck down a law requiring that cable companies make adult material available only when customers requested in writing that they do so. It wrote that, "the

167. The lack of Court activity can be explained because, as Julie Cohen points out in her article on the right to read anonymously, "[u]ntil recently . . . the technological means to monitor individuals’ reading habits did not exist." Julie E. Cohen, A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace, 28 CONN. L. REV. 981, 1003 (1996).


170. Id. at 1006.

171. Id.

172. Id. at 1008; Tien, supra note 137, at 177.

173. 518 U.S. 727, 755 (1996) ("[W]e do not agree that the ‘segregate and block’ requirements properly accommodate the speech restrictions they impose and the legitimate
‘written notice’ requirement will further restrict viewing by subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch the ‘patently offensive’ channel.”174

In summary, the Court has protected anonymous speech activity because it maximizes involvement in the exchange of ideas.175 In the process, anonymous speech works to limit government power by allowing oppressed groups a voice;176 increases the likelihood that reticent speakers will participate by lowering the risks associated with contributing;177 and allows ideas to be considered without bias.178 At the same time, this right is not absolute. When anonymous speech activity conflicts with other compelling goals such as law enforcement, the Court takes into account the value of the speech at issue;179 whether an identity requirement will achieve the government’s goal;180 and whether an identity requirement is the least restrictive alternative.181 With this background in mind, this Note will continue on to discuss the case of government-mandated data retention by ISPs.

B. Data Retention and Anonymous Speech Activity

Let us take as a given that the government has a compelling reason for instituting data retention: the apprehension of criminals who use the Internet to further their objectives.182 Examining compulsory data retention in light of the value of anonymous speech that the Court has articulated, there are persuasive reasons to hold it unconstitutional because of its effect on anonymous speech

objective they seek to attain.”).

174. Id. at 754.


176. See id. at 64 (“Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.”).

177. Id. at 65 (providing historical examples of the risks associated with nonanonymous speech).

178. See McIntyre v. Ohio Elections Comm’n, 514 U.S. 334, 342 (1995) (noting that “an advocate may believe her ideas will be more persuasive if her readers are unaware of her identity”).

179. See supra notes 153-58 and accompanying text.

180. See McIntyre, 514 U.S. at 352 (noting reasons why the Government’s prohibition will not be effective).

181. Id. at 353 (“We recognize that a State’s enforcement interest might justify a more limited identification requirement, but Ohio has shown scant cause for inhibiting the leafletting at issue here.”).

182. The government’s need to stop conspiracy is arguably more compelling than its need to stop other speech-based harms such as libel because a remedy for libel, effective counter-speech, is not available for conspiracy. Thus, this is a particularly difficult test case.
activity. This Part II.B will explore the special value of online anonymity; consider the weighing factors the Court has enumerated; and then probe a few different data retention models to explore how the design of data retention can vary in its protection of speaker identity.

1. The value of online speech.

Though the imperfect anonymity of real space goes far to maximize the exchange of ideas in the ways the Court has noted, the perfect anonymity of the Internet goes further still. As a highly accessible cheap speech medium, the Internet plays an especially valuable role in limiting government power by giving voice to diverse viewpoints. The Court has been particularly protective of those methods of communication that are useful in promoting the "poorly financed causes of little people."\(^{183}\) The Court identified the Internet as such a medium when it wrote that, "through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox."\(^{184}\) The low cost of participation, particularly when coupled with the Internet's decentralized control structure,\(^{185}\) makes the Internet a natural ally of the dissenter.

Second, if the imperfect anonymity of physical space could be said to lower the risk of contributing to debate, the easily achievable perfect anonymity of the Internet surely goes farther still. The risk of accidental discovery drops quite low when one takes advantage of technologies, such as anonymous remailers, designed for the specific purpose of decoupling speech and speaker.\(^{186}\)

Third, and perhaps most powerful, is the Internet's ability to allow ideas to be considered without bias. The perfect anonymity of the Internet allows individuals to be completely divorced from those immutable characteristics that shape our everyday interactions. In physical space:


\(^{184}\) Reno v. ACLU, 521 U.S. 844, 870 (1997).

\(^{185}\) See also Tien, supra note 137, at 137 ("Computer networks represent a shift in the architecture of everyday communication, moving from an institutionalized, one-way print media to 'a communication mode in which many share knowledge among themselves.'" (quoting U.S. CONG., OFFICE OF TECH. ASSESSMENT, 100TH CONG., SCIENCE, TECHNOLOGY AND THE FIRST AMENDMENT 7 (U.S. Gov't Printing Office 1988)).

\(^{186}\) "A re-mailer is an Internet site to which you can send e-mail for forwarding to an intended destination while concealing your own e-mail address." Look it up: Definitions for thousands of the most current IT-related words, at http://whatis.techtarget.com/definition/0,,sid9_gci212886,00.html (last visited June 22, 2003).
Even if we cannot individually identify someone, during a face-to-face encounter we can almost always be categorically identified and "placed" in the social structure. These means of identifying people are socially constructed. They govern social interaction, especially in terms of demand and disattention. . . . Going to a fast-food joint dressed in a tuxedo will get people's attention. To be a young black male in a large department store or a young woman alone on a city street late at night can be fateful.\textsuperscript{187}

The perfect anonymity of the Internet facilitates a true divorce between speaker identity and the message conveyed. Thus, even subconscious reactions to immutable characteristics such as gender and race can be overcome.

If one examines anonymous online speech according to the values that the Court has set out, the perfect anonymity of the Internet is still more valuable than anonymity in the physical world. Its unique accessibility gives voice to the poor and unpopular, lowers the risk of stigma associated with sharing one's views, and allows ideas to be considered on their merits alone.

2. Anonymity versus accountability.

As discussed above, the Court's protection of anonymous speech activity has not been absolute. Where anonymous speech conflicts with a compelling interest such as the government's ability to enforce the law, the Court has sought to balance these competing values through examination of three factors: first, the value of the speech at issue; second, the existence of alternate ways of achieving the government's goal; and, third, whether compelling identity disclosure will result in the achievement of the government's goal.

The first consideration, the value of the anonymous speech, weighs strongly against finding a data retention regime constitutional, because such a regime would as a practical matter completely purge the element of anonymity from Internet communications. Data retention is a blanket policy that would capture all speech.\textsuperscript{188} It does not differentiate between types of speech activity (for example, information-giving and information-receiving).\textsuperscript{189} It indiscriminately strips anonymity from protected and unprotected speech alike.\textsuperscript{190}

The question is whether the Court will see a constitutional problem with eliminating so much protected anonymous speech to hold a small subset of

\textsuperscript{187} Tien, supra note 137, at 163.
\textsuperscript{188} See supra notes 4-7 and accompanying text.
\textsuperscript{189} See supra Part II.A.
\textsuperscript{190} Some speech is more valuable than other speech. Although the phrase "Congress shall make no law . . . abridging the freedom of speech," U.S. CONST. amend. I, sounds monolithic, the Court has long recognized that the First Amendment does not protect some types of speech, such as libel. See N.Y. Times Co. v. Sullivan, 376 U.S. 254, 268 n.6 (1964) (citing cases in which the court found the speech in question was not protected because it was libelous).
speakers accountable for their unprotected speech. There is reason to believe that it will, for the Court has rejected similarly broad speech regulations in the recent past. In striking down a law that banned virtual child pornography, the Court wrote that "[t]he argument, in essence, is that protected speech may be banned as a means to ban unprotected speech. This analysis turns the First Amendment upside down. The Government may not suppress lawful speech as the means to suppress unlawful speech. . . . The Constitution requires the reverse." The principle at work is that the value of protected speech is so high that even otherwise unprotected speech must be tolerated if the only alternative would be to restrict protected speech. This idea was also in evidence in McIntyre, where the Court stated that "our society accords greater weight to the value of free speech than to the dangers of its misuse." Thus, consideration of the first weighing factor, the value of the speech at issue, disfavors sweeping speech regulations such as data retention.

The second factor the Court considers is whether compelled identity disclosure is the only way government can achieve its goal, in this case adequate law enforcement. The issue is whether data retention is the least restrictive method of apprehending criminals who use the Internet in furtherance of their crimes. An expedient way of getting at this question is to ask what data retention offers law enforcement agents that other available surveillance techniques do not.

Data retention does supply the government with a new tool. The unique feature of data retention is that it would permit law enforcement agents to develop individualized suspicion after accessing Internet usage records. Under this ex post model of generating suspicion, law enforcement officials would have at their disposal a wealth of data about individuals in the form of their emails and web page viewing habits. After developing a model of what constitutes suspicious Internet usage, law enforcement agents could search for patterns of behavior that match and then focus further investigative resources on these suspect individuals.

There are potentially great advantages and great risks under this ex post approach. If the model of suspicious behavior were accurate, such an approach would have the potential for great efficiency, since resources would be targeted at likely wrongdoers, and expediency, since there would be fewer bad leads. To the degree that the model is inaccurate, lawful Internet use would be deterred

191. An essential aspect to the Court's reasoning was that expert witnesses would have a hard time telling the difference between pornography using children as models and virtual child pornography. See Ashcroft v. Free Speech Coalition, 535 U.S. 234, 255 (2002): [T]he Government says that the possibility of producing images by using computer imaging makes it very difficult for it to prosecute those who produce pornography by using real children. Experts, we are told, may have difficulty in saying whether the pictures were made by using real children or by using computer imaging.
192. Id.
and innocent individuals unnecessarily scrutinized by the government. There is an additional risk associated with this model regardless of its accuracy: the danger of unauthorized access, by outside criminals and corrupt insiders alike.

That a potential law enforcement tool provides an additional capability does not make that tool necessary, especially where there are other ways to achieve adequate law enforcement. The government currently has such an adequate tool. It is known as Carnivore, and it enables the government to monitor Internet usage. As the Federal Bureau of Investigation explains Carnivore and the rationale behind it:

> Because many Internet Service Providers (ISP[s]) lacked the ability to discriminate communications to identify a particular subject's messages to the exclusion of all others, the FBI designed and developed a diagnostic tool, called Carnivore. The Carnivore device provides the FBI with a "surgical" ability to intercept and collect the communications which are the subject of the lawful order while ignoring those communications which they are not authorized to intercept.

Like data retention, Carnivore enables law enforcement officers to observe Internet usage patterns. The significant difference is that because federal law requires that law enforcement agents demonstrate probable cause and obtain a court order before using Carnivore, it requires that agents develop suspicion ex ante. This requirement of ex ante suspicion is all the more important since "[p]articularized suspicion keeps the government's profound investigative power in check, preventing widespread surveillance and snooping into the lives and affairs of all citizens."

That data retention may prove more powerful than Carnivore does not justify its use. After all, if the Court accepted that the "least restrictive means" inquiry involved sanctioning the least restrictive means to accomplish the precise effect of the challenged government practice, then the government would always win. The government does not always win. For instance, in Ashcroft v. Free Speech Coalition, the government argued that it should be permitted to ban virtual child pornography because experts would have a

194. See Carnivore: Diagnostic Tool, at http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (last accessed June 22, 2003); see also Thomas R. McCarthy, Don't Fear Carnivore: It Won't Devour Individual Privacy, 66 Mo. L. Rev. 827, 832 (2001) (providing an overview of Carnivore's capabilities and arguing that Carnivore does not harm individuals' privacy rights).


196. Id.

197. Solove, supra note 23, at 1109. For an argument that using databases to identify individuals engaging in suspicious activity is problematic, see Solove at id. ("[A]utomated investigation is troubling because it alters the way that government investigations typically take place... Particularized suspicion keeps the government's profound investigative power in check preventing widespread surveillance and snooping into the lives and affairs of all citizens.").
difficult time distinguishing between pornography made using real children and those using graphic rendering.\textsuperscript{198} Without denying the plausibility of the government’s argument, the Court nonetheless held that “[t]he government may not suppress lawful speech as the means to suppress unlawful speech.”\textsuperscript{199} The mere fact that data retention might augment the government’s law enforcement capabilities does not justify its use. Especially given the existence of an adequate alternative such as Carnivore, data retention should not be considered the least restrictive alternative.

The third and final factor the Court considers is whether compelled identity disclosure will allow the government to achieve its compelling interest.\textsuperscript{200} Given the limitations of current technology and the scope of United States jurisdiction, any data retention scheme would be ineffective. First, just because the government can access communications does not mean that government can understand them. Encryption technology allows individuals to send messages in a code so secure that the government cannot break it.\textsuperscript{201} Since individuals with something to hide face relatively strong incentives to encrypt their communications, data retention could have the perverse effect of stripping the anonymity of benign communications and increasing the inaccessibility of others. Second, U.S. jurisdiction extends only to U.S. ISPs. Without international cooperation, much Internet communication would remain unarchived. Not only would international actors escape data retention but so would Americans willing to make an international phone call to a foreign ISP.

In summary, the values the Court has articulated in support of anonymous speech in real space hold true for the space of the Internet as well. By providing cheap access to anonymous speech, the Internet limits government power by strengthening the voices of the poor and unpopular. Because it makes anonymity easy, the Internet lowers the risks associated with contributing to political debate. By virtue of the fact that anonymity online is perfect anonymity, it allows ideas to be considered without bias. Further, the factors that the Court considers when balancing anonymity against other compelling needs all disfavor compulsory data retention. Data retention is too indiscriminate, sweeping in all protected anonymous speech; it is not the least restrictive alternative, since the government has Carnivore available to it; and it will not be effective, at least as long as it is applied to U.S. ISPs alone. For these reasons, compulsory data retention should be struck down on First Amendment grounds.

\textsuperscript{199} Id.
\textsuperscript{200} See McIntyre v. Ohio Elections Comm’n, 514 U.S. 334, 353 (1995) (noting that “Ohio has shown scant cause for inhibiting the leafletting at issue here”).
\textsuperscript{201} See Kerr, supra note 99, at 503 (describing the power of encryption technology).
CONCLUSION

Data retention would dramatically rearchitect the Internet from a medium that promotes relative obscurity to one of relative transparency. The Internet’s malleable architecture makes it vulnerable to this form of manipulation in ways that physical space is not. This malleability, coupled with the increasing diversity of activity that individuals engage in online, has the potential to force the Court to address unanswered questions. In the Fourth Amendment context, the underlying question is how far the government may go in rearchitecting the Internet to promote accountability. In the First Amendment context, the issue is the extent to which the government can eliminate anonymity to promote accountability. It is this feature of the Internet—the fact that its different contours make untenable the truces negotiated between competing values in other contexts—that makes it such an interesting test case. Ultimately, it forces us to ask to what extent current limits on government regulation are the product of the architecture of physical space and to what extent they are constitutionally required. At least under the Internet’s current form, this Note concludes that government-mandated data retention should be considered unconstitutional on First Amendment grounds.