2005

Web Surfing In Chilly Waters: How The Patriot Act'S Amendments to the Pen Register Statute Burden Freedom of Inquiry

James McClintick

Follow this and additional works at: http://digitalcommons.wcl.american.edu/jgspl

Part of the Constitutional Law Commons

Recommended Citation
WEB-SURFING IN CHILLY WATERS:

HOW THE PATRIOT ACT’S AMENDMENTS TO THE PEN REGISTER STATUTE BURDEN FREEDOM OF INQUIRY

JAMES MCCINTICK*

Introduction .................................................................................................................. 353
I. Background ............................................................................................................. 357
  A. The Development of Pen Register Surveillance Law Prior to the Patriot Act .......... 357
  B. How the Patriot Act Expanded the Surveillance Capacity of the Pen Register Law ............................................................................................................. 360
II. Overbreadth in the Pen Register Amendments and the Danger to the First Amendment ................................................................. 361
  A. The First Amendment Encompasses Freedom of Inquiry .................. 361
  B. Judicial Rejection of Past Legislative Attempts to Regulate or Prohibit Intellectual Speech ................................................................. 363
  C. Beyond Specific Proscriptions: How Indiscriminate Data-Gathering Chills Intellectual Activity ................................................................. 367
  D. Internet Surveillance Anxiety as a Justiciable Injury ......................... 372
III. “Fixing” the Pen Register Statute: Fears and Solutions ................. 376
Conclusion ............................................................................................................... 380

INTRODUCTION

The September 11, 2001 terrorist attacks on New York City and Washington, D.C. ushered in an American era defined largely by...

* J.D. Candidate, American University Washington College of Law, May 2005. The author would like to dedicate this article to his parents, Michael and Kathleen McClintick, whose unwavering commitment to academic freedom and civil rights has served as a tremendous source of inspiration.

353
national security concerns. In an effort to safeguard the United States and Americans everywhere from similar acts of destruction in the future, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act" or "Patriot Act"). Congress passed the 400-page Act almost exactly six weeks after the events of September 11, 2001. The Patriot Act provides a lengthy and elaborate compilation of amendments to pre-existing federal law in areas such as surveillance, international money laundering, border protection, and foreign intelligence.

The staggeringly swift passage of this vast piece of legislation meant that members of Congress had little opportunity to review the Act’s myriad provisions before voting on it. One set of provisions expanded the pen register surveillance law, which traditionally had guided federal agents when monitoring the numbers dialed from a suspect’s telephone. In the eyes of civil libertarians and

1. See Bart Kosko, Editorial, Your Privacy Is a Disappearing Act: A Digital Spying Net May or May Not Catch Terrorists, but It Will Ensnare Us, L.A. TIMES, Dec. 2, 2001, at M5 (arguing that after the attacks, people living in the United States sacrificed various civil liberties for a “potential increase in protection from terrorists”).


3. See President’s Remarks, supra note 2 (verifying that President Bush signed the Act into law on October 26, 2001).

4. See Patriot Act § 1, 115 Stat. at 272-75 (displaying ten separate titles and a total of 158 subsections). Each subsection makes numerous amendments to the United States Code, and these amendments vary in length and specificity. Id. §§ 1-1016, 115 Stat. at 275-402. Some amendments replace existing terms, while others add new paragraphs and subsections to existing definitions and enforcement guidelines. Id.

5. See Surveillance Under the “USA/Patriot” Act, ACLU Online Archives (Jan. 1, 2002) (explaining that Congress passed the Patriot Act because the Bush Administration “bullied” Congress into it, and remarking that the bill went “straight to the [Congressional] floor with no discussion, debate, or hearings”), at http://www.aclu.org/Privacy/Privacy.cfm?ID=13465&c=130 (on file with the American University Journal of Gender, Social Policy & the Law).

6. See United States v. N.Y. Tel. Co., 434 U.S. 159, 161 n.1 (1977) (defining pen register as “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”).

commentators across the political spectrum, the amendments to this area of the law jeopardize an already fragile privacy interest in the content of electronic, computer-based communications.8

This Comment argues that the Patriot Act’s pen register amendments threaten First Amendment academic freedom guarantees in addition to Fourth Amendment privacy rights.9 This Comment suggests that academic research in controversial areas, such as terrorism or critical examination of national security policy, will suffer a particular burden as a result of the government’s enhanced Internet surveillance powers.10

Part I examines how the Patriot Act expanded the government’s Internet surveillance power through seemingly innocuous “modifications” to the pen register law.11 Part I also reviews the law and technology on which today’s Internet monitoring is based.12 Because privacy rights and free speech rights are closely intertwined in surveillance law, Part I briefly discusses concerns that the new pen

of Justice to place wiretaps” on computers and telephones of terrorism suspects, and that these amendments form the basis for the “Providing Appropriate Tools Required to Intercept and Obstruct Terrorism” portion of the USA PATRIOT Act’s title).


9. See infra Part II.A (explaining that scholars have argued that the Act violates the Fourth Amendment probable cause standard and using Justice Douglas’ First Amendment “penumbra theory” to suggest that, in modern times, the freedom to conduct Internet research for scholarship purposes is a facet of the First Amendment guarantee of free inquiry).

10. See infra Part II.B-C (expanding upon the holdings and reasoning of prior case law to argue that broad restrictions on speech and poorly delimited government surveillance powers chill inquiry into and discussion of politically sensitive topics); see also R. Kenton Bird & Elizabeth Barker Brandt, Academic Freedom and 9/11: How the War on Terrorism Threatens Free Speech on Campus, 7 COMM. L. & POL’Y. 431, 436-37 (2002) (observing that the post-September 11 threat to academic freedom is the greatest since the days of the Vietnam War protests).

11. See infra Part I.B (providing an in-depth discussion of how the post-Patriot Act pen register definition enabled the federal government to glean a considerable amount of personal information from records of Web use data); see also Rich Haglund, Comment, Applying Pen Register and Trap and Trace Devices to Internet Communications: As Technology Changes, Is Congress or the Supreme Court Best-Suited to Protect Fourth Amendment Expectations of Privacy?, 5 Vand. J. Ent. L. & Prac. 137, 145 (2003) (defending the amendments to the pen register/trap and trace statutes as “modifications” that fall short of creating a “new law of the Internet” and instead merely help police “keep up with changing” communications technologies).

register law endangers Fourth Amendment guarantees.\textsuperscript{13}

Part II begins by arguing that the First Amendment includes the right to conduct Internet research.\textsuperscript{14} Part II then assesses the constitutionality of the pen register law in light of the judiciary’s reaction to analogous laws that have sought to grant government authorities broad regulatory or surveillance powers.\textsuperscript{15} The constitutional assessment presupposes that the pen register statute, like any surveillance law, has two main functions that could implicate the First Amendment: the elimination of specific criminal activity and the more mysterious act of long-term data-gathering and record-keeping.\textsuperscript{16} The final section of Part II suggests that the pen register law places a real and substantial burden on scholars that courts should not dismiss as merely theoretical.\textsuperscript{17}

Part III of the Comment proposes ways to preserve the enhanced surveillance provisions of the pen register amendments while continuing to allow American citizens and others to browse the Internet without fear of government intrusion into their scholarly activities.\textsuperscript{18} This Comment concludes that the current pen register law poses an unnecessary and unacceptable danger to the First Amendment guarantee of intellectual freedom.\textsuperscript{19}

\begin{flushleft}
\textsuperscript{13} See infra Part I.B (noting that journalists and civil liberties groups fear that government monitoring of Web-surfing activity burdens privacy rights because Web addresses can contain personal information); see also United States v. U.S. Dist. Ct. for the E. Dist. of Mich., 407 U.S. 297, 313 (1972) (explaining that national security cases are unique in that they involve a “convergence of First and Fourth Amendment values” with historic roots in the English “struggle for freedom of speech and press”).

\textsuperscript{14} See infra Part II.A (arguing that Internet research, as a modern-day component of freedom of inquiry, fits comfortably within the Supreme Court’s liberal and long-standing formulation of First Amendment guarantees).

\textsuperscript{15} See infra Part II.B-C (exploring the Supreme Court’s generally negative response to laws and regulations that chill intellectual endeavors by explicitly forbidding certain forms of speech or authorizing surveillance of politically controversial activities).

\textsuperscript{16} See infra Part II.C (noting that while the pen register law seeks to curtail criminal activity, it also goes beyond this objective and allows data-gathering for virtually any reason); see also E. Dist. of Mich., 407 U.S. at 320 (conceptualizing “official surveillance” as a potentially oppressive government activity that serves the two objectives of “criminal investigation” or “ongoing intelligence gathering”).

\textsuperscript{17} See infra Part II.D (arguing that a scholar’s fear of Internet surveillance substantially chills academic activity and Constitutes a justiciable injury for which to seek a remedy in court).

\textsuperscript{18} See infra Part III (discussing strategies for redrafting portions of the pen register law or limiting its scope and duration to harmonize it with the panoply of First Amendment intellectual freedom guarantees).

\textsuperscript{19} See infra Conclusion (stating that the low evidentiary hurdle that law enforcement must overcome to secure an Internet pen register order burdens the First Amendment right to free inquiry and represents the triumph of national security considerations over Constitutional rights).
\end{flushleft}
I. BACKGROUND

A. The Development of Pen Register Surveillance Law Prior to the Patriot Act

Courts historically have resisted concluding that law enforcement violates a person’s Fourth Amendment rights when it secretly records and analyzes the telephone numbers that a person dials. Judicial reluctance to recognize a reasonable expectation of privacy in telephone numbers also extends to the Internet, as several recent federal circuit decisions have shown. As a result, Congress largely has shouldered the burden of deciding which forms of electronic communication, and under what circumstances, merit privacy protection.

The first major piece of federal telephone-line surveillance legislation was Title III of the Omnibus Crime Control and Safe Streets Act of 1968, commonly referred to as the Wiretap Act. This law proscribes the unauthorized collection and analysis of the contents of telephone conversations. The Wiretap Act explicitly permits, however, the use of pen register/trap and trace equipment.

Generally defined, a pen register is a mechanical device or

20. See Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that the monitoring of dialed phone numbers does not implicate the Fourth Amendment because people generally do not have a subjective privacy expectation “in the numbers they dial”).

21. See, e.g., United States v. Hambrick, 55 F. Supp.2d 504, 508-09 (W.D. Va. 1999) (concluding that the Fourth Amendment, when applied to the technology of the Internet, does not protect an Internet customer’s privacy expectation in personal information released to an Internet service provider); Guest v. Leis, 255 F.3d 325, 335-36 (6th Cir. 2001) (finding no reasonable expectation of privacy in non-content Internet information, such as the user’s subscriber data because the user placed the information under the control of a third party); see also Orin S. Kerr, Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn’t, 97 NW. U. L. REV. 607, 630 (2003) (describing telephone and Internet surveillance law as a “constitutional vacuum” that federal statutory law, rather than judicially rendered constitutional interpretation, has filled).

22. See Kerr, supra note 21, at 630 (noting that Congress passed a law banning wiretapping before the Supreme Court held that wiretapping violates the Fourth Amendment, and that Congress has since conducted an ongoing review of surveillance statutes in light of evolving “social norms”).

23. See 18 U.S.C.A. §§ 2510-2515 (2003) (listing definitions of surveillance terms and placing specific restrictions on the interception and disclosure of communications); see also Kerr, supra note 21, at 630 (noting that the Wiretap Act still regulates telephone monitoring today).

24. See 18 U.S.C.A. §§ 2511(1),(4)(a) (stating that those who intercept wire, oral, or electronic communications without a court order or proper certification will be fined, imprisoned for up to five years, or both).

25. See id. § 2511(2)(g)(i) (stating that, despite the prohibition on intercepting the substance of any communication, it "shall not be unlawful" for law enforcement agents to use a pen register or trap and trace device).
procedure that, when attached to a telephone line, monitors and records the electrical impulses generated by the act of dialing a telephone number. These impulses, analyzed together, reveal the numbers dialed from a given telephone but nothing about the conversations themselves. Telephone companies have long employed pen register technology for billing and various other purposes.

The complement to the pen register is the trap and trace device, which collects the numbers associated with incoming telephone calls. Like the pen register, the trap and trace device neither "hears" nor records the actual conversations of the party under surveillance. In light of these definitions, it seems that the Wiretap Act’s drafters never envisioned pen register/trap and trace equipment as technology that could collect the actual substance of communications.

As stated earlier, the U.S. Supreme Court recognizes no reasonable expectation of privacy in the telephone numbers a person dials. Instead, the Court has separated conceptually the number dialed from the ensuing conversation and has granted Fourth Amendment protection only to the latter. An analogous distinction exists between the address on an envelope and the letter inside: the former


27. See id. (noting that pen registers record telephone numbers without overhearing oral communications and without indicating whether the suspect has completed the call).

28. See N.Y. Tel. Co., 434 U.S. at 174-75 (stating that phone companies regularly use pen registers to ensure correct dialing, check for overbilling, and to discover whether a customer is running a business with her home telephone).

29. See 18 U.S.C.A. § 3127(4) (2003) (defining the trap and trace device in language virtually identical to that of the pen register definition, but stating that trap and trace devices capture incoming electronic impulses generated by dialing a telephone number). Pen registers capture outgoing information only. Id. § 3127(3).

30. See id. § 3127(4) (emphasizing that the “dialing, routing, addressing, and signaling” information that a trap and trace device captures shall not include the contents of any communication).

31. See N.Y. Tel. Co., 434 U.S. at 167-68 (analyzing the Wiretap Act and concluding that the Act’s drafters did not regard pen registers as a threat to privacy because these instruments do not record the contents of communications).

32. See Smith v. Maryland, 442 U.S. 735, 742 (1979) (reasoning that, because all telephone users must transmit the numbers they dial to the telephone company, and because telephone users know that the company can make permanent records of the numbers dialed, people could not have an actual expectation of privacy in this information).

33. See Katz v. United States, 389 U.S. 347, 352 (1967) (recognizing a constitutionally protected privacy interest in a conversation made from a telephone in a public booth, and adding that one who uses a telephone booth is "surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world").
is merely “addressing” information, while the latter is considered “content” information and thus falls within the protection of the Fourth Amendment. This distinction has allowed the pen register to play a very broad role in federal surveillance activities, but its post-Patriot Act application is of questionable constitutional legitimacy.

The first statute explicitly governing federal pen register use appeared within a series of amendments to the Wiretap Act and eventually became part of the Electronic Communications Privacy Act of 1986 (“ECPA”). Under the ECPA, a magistrate “shall enter an ex parte order authorizing the installation and use of a pen register” if the investigator “has certified to the court that the information likely to be obtained . . . is relevant to an ongoing criminal investigation.” The relevance standard is far less rigorous than probable cause. Moreover, the Justice Department acknowledges that judicial approval of pen register/trap and trace equipment is a procedure that is “ministerial in nature.” Once federal law enforcement agents obtain the order, they may use the surveillance device for up to sixty days before requesting additional sixty-day extensions.

From its enactment up until the passage of the Patriot Act, the ECPA made it clear that law enforcement officials could use pen register equipment only to collect numbers dialed and sent over a

34. See Surveillance Under the “USA/Patriot” Act, supra note 5 (discussing the two types of surveillance distinguished in the original pen register law).

35. See Kosko, supra note 1, at M5 (warning that the Patriot Act gives the Federal Bureau of Investigation (FBI) broader powers to monitor Internet activity than before). This is especially worrisome because no one knows whether the government’s data-gathering technology will properly separate Web content from Web addressing information. Id.


37. Id. § 3123(a)(1).

38. See ROBERT M. BLOOM & MARK S. BRODIN, CRIMINAL PROCEDURE § 4.1 (2d ed. 2000) (defining probable cause as an evidentiary hurdle that requires “specific facts, not simply conclusory assertions” that add up to more than a vague suspicion but less than proof beyond a reasonable doubt); see also Surveillance Under the “USA/Patriot” Act, supra note 5 (describing the evidentiary requirement for pen register use as “essentially non-existent”).

39. See COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, U.S. DEP’T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS (2002) [hereinafter SEARCHING AND SEIZING COMPUTERS] (explaining that a court will grant a pen register order without assessing the veracity of the stated facts if the applicant states her name, identifies the agency investigating the crime, and certifies that the desired information is relevant to the investigation), at http://www.cybercrime.gov/s&smanual2002.htm (last visited Apr. 21, 2005).

40. See id. (describing the application and issuance procedures for a pen register order and stating that, during the time the pen register is in use, the investigating officer should not disclose its existence to anyone).
telephone line.41 Nevertheless, some courts assumed that the ECPA’s
definition of the pen register was flexible enough to allow monitoring
of computer network communications as well as telephonic
communications.42 Despite the courts’ broader application, however,
at least one federal magistrate judge adhered to the idea that pen
registers were available only for telephonic surveillance.43

B. How the Patriot Act Expanded the Surveillance Capacity of the Pen
Register Law

Widespread public anxiety after the September 11 tragedies
spurred Congress to grant some of the Justice Department’s demands
for enhanced surveillance capability.44 One result was the Patriot
Act’s revisions to the pen register law, which redefined the pen
register to cover Internet as well as telephone monitoring.45 Congress
similarly expanded the definition of the trap and trace device.46
While the Justice Department has pointed out that the pen register
amendments expressly forbid the collection of the “contents of any
communication,”47 journalists and commentators have discovered
ambiguity in the new law because no bright-line distinction exists
between addressing information and content on the Internet.48 The
Patriot Act’s language, they argue, is far too simplistic to address this

a device that records “numbers dialed or otherwise transmitted on the telephone
line” and noting that this statutory definition does not include devices used by a
provider of a wire or electronic communication service).

42. See Kerr, supra note 21, at 634 (noting that a federal magistrate judge in Los
Angeles granted an Internet pen register order despite his recognition that the
drafters of the original pen register statute never imagined this use for the device).

43. See id. at 635 (noting that a magistrate judge in northern California denied a
government application for an Internet pen register order after reviewing the ECPA’s
pen register law and concluding that the law covered only telephonic devices).

44. See id. at 636 (explaining that the Justice Department had been “clamoring
for changes to the antiquated surveillance laws for years”).

45. See 18 U.S.C.A. § 3127(3) (2003) (defining a pen register as a “device or
process which records or decodes dialing, routing, addressing, or signaling
information transmitted by an instrument or facility from which a wire or electronic
communication is transmitted”).

46. See id. § 3127(4) (defining a trap and trace device as something that
“captures the incoming electronic or other impulses which identify the originating
number or other dialing, routing, addressing, and signaling information”).

47. See SEARCHING AND SEIZING COMPUTERS, supra note 39 (stating that the newly
amended pen register law regulates the collection of “addressing and other non-
content information”); see also 18 U.S.C.A. § 3127(3) (permitting the use of a pen
register to capture information so long as that information does not include the
“contents of any communication”).

48. See Surveillance Under the “USA/Patriot” Act, supra note 5 (analogizing a list
of Internet addresses to a list of purchased books, and arguing that both contain rich
and revealing information).
The pen register law’s ambiguity stems from the idea that, unlike a telephone number, an Internet address contains an element of content. While a telephone number is strictly a sequence of digits, an Internet address could contain search terms, concepts, titles, and trademarks, as well as the names of businesses, schools, or political organizations. In light of the variety and abundance of words potentially present in an Internet address, the American Civil Liberties Union (“ACLU”) has characterized Internet addresses as a source of “intimate information that reveals who we are and what we are thinking about.” The expanded definition of the pen register, now addressing and signaling information in electronic communications, strongly suggests that government agents now may access lawful Internet addresses with nothing more than a pen register order.

II. OVERBREADTH IN THE PEN REGISTER AMENDMENTS AND THE DANGER TO THE FIRST AMENDMENT

A. The First Amendment Encompasses Freedom of Inquiry

Civil libertarians generally have invoked the Fourth Amendment for their most withering attacks on the expanded pen register law.
Unfortunately, this intense focus on Fourth Amendment rights largely has overshadowed discussion of the pen register law’s implications for First Amendment rights.\textsuperscript{55} Intimately linked to the issue of privacy in Internet use is the issue of free speech and, more specifically, intellectual freedom.\textsuperscript{56}

Courts have long recognized that the First Amendment protects far more than the mere oral or written expression of ideas.\textsuperscript{57} Justice Douglas, for instance, famously reasoned that each provision of the Bill of Rights possesses a “penumbra” that encompasses numerous unnamed but constitutionally protected activities.\textsuperscript{58} In a description of the rights that give the First Amendment “life and substance,” Justice Douglas employed his penumbra theory to argue that the Amendment protects not only freedom of speech and press but also “the right to read... and freedom of inquiry, freedom of thought, and freedom to teach."\textsuperscript{59}

In modern times, the right to conduct Internet-based research for academic purposes is an important part of “freedom of inquiry,” and, as such, falls within the scope of the First Amendment.\textsuperscript{60} Intrusive law enforcement is nothing new.\textsuperscript{61} Throughout American history, of information between criminal and intelligence operations).

\textsuperscript{55} \textit{See id.} (arguing that the Patriot Act endangers not just Fourth Amendment rights but also First Amendment rights, such as freedom of political association and freedom to voice dissent, by broadening the definition of domestic terrorism to include activities that “appear to be intended . . . to influence the policy of a government by intimidation or coercion”).

\textsuperscript{56} \textit{See Surveillance Under the “USA/Patriot” Act, supra} note 5 (explaining that the Patriot Act grants the federal government unfettered power to investigate people’s Internet and library usage, book purchases, travel habits, and other activities that the First Amendment protects).

\textsuperscript{57} \textit{See Griswold v. Connecticut}, 381 U.S. 479, 484-85 (1965) (holding that the right to family planning receives protection within a “zone of privacy” emanating from several constitutional amendments including First Amendment free speech guarantees as well as Fourth Amendment privacy guarantees). The Court observed that the Constitution guarantees many individual rights that do not appear specifically in its text. \textit{Id.}

\textsuperscript{58} \textit{See id.} at 484 (stating that numerous Supreme Court decisions over the years demonstrate that explicitly mentioned guarantees in the Bill of Rights have penumbras, formed by “emanations from those guarantees”).

\textsuperscript{59} \textit{Id.} at 482.

\textsuperscript{60} \textit{See, e.g., Doe v. 2TheMart.com, Inc.,} 140 F. Supp.2d 1088, 1092 (W.D. Wash. 2001) (stating that a civil subpoena compelling the disclosure of names of anonymous Internet users should satisfy a high threshold because First Amendment protections encompass Internet-based speech activity); \textit{see also} Reno v. ACLU, 521 U.S. 844, 870 (1997) (holding that regulation of the Internet demands nothing less than stringent First Amendment scrutiny because it provides an ideal forum for a vigorous exchange of thoughts and ideas).

government surveillance has been an almost reflexive response to perceived threats to national security. However, the reckless data collection that the Patriot Act sanctions poses a uniquely modern dilemma: by exposing Internet addresses to government surveillance, the expanded pen register law may inhibit Internet-based scholarly inquiry into terrorism or national security policy. Though the new law does not ban explicitly research or any other First Amendment activity, there is little or no constitutional difference between an unstated burden and an outright ban on such activities.

B. Judicial Rejection of Past Legislative Attempts to Regulate or Prohibit Intellectual Speech

The U.S. Supreme Court has long viewed the right to exchange ideas freely as inseparable from freedom of intellectual inquiry. For this reason, the unfettered commerce of ideas ranks among the most fiercely protected activities in the United States. The relationship between freedom of inquiry and the freedom to share ideas received special attention in *Sweezy v. New Hampshire*.

At issue in *Sweezy* was an anti-"subversive behavior" statute that penalized a professor for discussing socialism in the classroom. In


63. See Brigitte Anderson & William Rossiter, *Backward March!* *The USA-Patriot Act and the Bill of Rights*, 12 Mont. Professor 6, ¶ 27 (Spring 2002) (advising readers to "be careful what you put in the Google Search," and warning that, under the expanded surveillance provisions of the Patriot Act, a graduate student researching Al Qaeda, a political scientist studying Sinn Fein, or an activist for Amnesty International all could be exposing their communications to the government and could become the target of investigation), available at http://mtprof.msun.edu/Spr2002/BAWRart.html (last visited Apr. 21, 2005).

64. See United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 826 (2000) (invalidating restrictive provisions of the Telecommunications Act on First Amendment grounds, and reasoning that an overbroad regulation deserves no "special consideration or latitude" simply because the regulation burdens, rather than blatantly suppresses, a constitutional right).

65. See *Sweezy* v. New Hampshire, 354 U.S. 234, 262-63 (1957) (Frankfurter, J., concurring) (emphasizing the importance of shunning any government regulation that tends to "check the ardor and fearlessness of scholars," and defining freedom of inquiry as freedom to examine, question, and engage in "disputation on the basis of observation”).

66. See *Keyishian v. Bd. of Regents*, 385 U.S. 589, 603 (1967) (observing that the United States has a profound commitment to safeguarding academic freedom, "which is of transcendent value" to everyone).

67. See 354 U.S. at 250 (noting that freedom to express inflammatory political ideas is no less fundamental to a democratic society than freedom to acquire knowledge).

68. See id. at 246 (explaining that the statute in question comprehensively
striking down the statute for its broad sweep, the Court described the law as a “strait jacket” upon academic inquiry and warned that such a restriction on speech could severely hamper the learning process.\(^69\) The Court supported its holding by reasoning that all areas of scholarship, and especially controversial ones, provide endless opportunities to gain wisdom and knowledge.\(^70\)

While scholars of terrorism or Islam may arouse the suspicion of government agents and become the targets of electronic surveillance, these subjects are no less valid as academic fields than is the study of Marxism.\(^71\) Moreover, like the academic activity at issue in *Sweezy*, Islamic studies and terrorism merit special protection because of, not despite, their controversial nature.\(^72\) For these reasons, burdening inquiry into the latter subjects is as unconstitutional an act as burdening inquiry into the former.\(^73\)

The Supreme Court issued a similar ruling several years later in *Keyishian v. Board of Regents*.\(^74\) The law at issue in *Keyishian* punished “treasonable” or “seditious” behavior without defining those two adjectives, and the Court reasoned that the law endangered free speech by creating uncertainty about the speech or conduct being regulated.\(^75\) As a means of vividly portraying the nightmarish

---

\(^{69}\) See id. at 250 (asserting that students, and the teachers who guide them, are vital to the preservation of democracy, and cautioning that “[s]cholarship cannot flourish in an atmosphere of suspicion and distrust”).

\(^{70}\) See id. (arguing that researchers have not explored any field so thoroughly that new discoveries are impossible, and that this may be especially true in fields “where few, if any, principles are accepted as absolutes”).

\(^{71}\) See *Bird & Brandt*, supra note 10, at 449 (observing that, for many years prior to the September 11, 2001 terrorist attacks, scholars had been exploring the origins of Islamic fundamentalism and dissatisfaction with U.S. foreign policy).


\(^{73}\) See Kathryn Martin, Note, *The USA PATRIOT Act’s Application to Library Patron Records*, 29 J. LEGIS. 283, 290-91 (2003) (noting that the First Amendment includes the right to receive speech and protects the efforts of a “curious mind” to learn more about political or world views with which many may disagree).

\(^{74}\) See 385 U.S. at 597-98 (noting the oppressive nature of a New York statutory provision that broadly called for the removal of any public-school employee responsible for any “treasonable or seditious word or words or the doing of any treasonable or seditious act or acts”).

\(^{75}\) See id. at 598 (comparing the statutory provision to the Sedition Act of 1798, which similarly failed to specify the meaning of “seditious,” and cautioning that the absence of a definition of the word “treasonable” in the statutory provision makes this
consequences of such a vague restriction, Justice Brennan invoked the image of a frightened academic who can only "guess what conduct or utterance may lose him his position." Furthermore, in *Keyishian*, as in *Sweezy*, the Court employed the metaphor of a "strait jacket" to illustrate the danger of broad regulations on intellectual life.

A strait jacket on scholarship similar to the ones discussed in *Sweezy* and *Keyishian* exists today. The pen register law permits authorities to record Internet addressing information whenever it becomes relevant to a criminal investigation. This language allows broad discretion in the gathering of Internet addresses from a search. In *Sweezy*, the distinction between a subversive person and a loyal one was unclear. In *Keyishian*, the teachers feared crossing the shadowy line between seditious and non-seditious acts. Scholars today could find that the line between what is relevant and irrelevant to a criminal investigation likewise lies in shadow, causing education to suffer as a result.

*Sweezy* and *Keyishian* are two examples of lawmakers’ failed efforts to ferret out socially disruptive speech and conduct at the expense of intellectual freedom. Other statutes have burdened academic inquiry by regulating access to inflammatory or obscene books. The word "no less dangerously uncertain").

76. See id. at 604 (arguing that only extremely precise laws that clearly alert teachers of the forbidden behavior can combat the chilling effect on First Amendment rights because these rights cannot survive without “breathing space”).

77. See id. at 603 (warning of imperiling America’s freedom by “impos[ing] any strait jacket upon the intellectual leaders in our colleges and universities”) (quoting *Sweezy*, 354 U.S. at 250).

78. See Patriot Act § 216, 115 Stat. at 290 (amending the pen register law to allow law enforcement authorities to collect the addressing information of any electronic communication that may seem relevant to criminal activity).

79. See SEARCHING AND SEIZING COMPUTERS, supra note 39 (stating somewhat paradoxically that the distinction between addressing information and content applies to the Internet, despite the fact that there can sometimes be “debate” about what constitutes content in electronic communications).

80. See 354 U.S. at 246 (noting that the definition of subversive persons in the statute casts a net over far more people than just those who seek violent overthrow of the government).

81. See 385 U.S. at 599 (emphasizing that the definition of seditious is virtually limitless, and theorizing that the law could punish a teacher who carries a copy of the Communist Manifesto in public).

82. See Anderson & Rossiter, supra note 63 (predicting that the vague language in the Patriot Act may create “minefields of study,” such as aerosol biology or Middle Eastern studies, that students will avoid pursuing for fear of intrusive surveillance or criminal prosecution).

83. See Bird & Brandt, supra note 10, at 446 (describing the statutes at issue in *Sweezy* and *Keyishian* as “sweeping and often clumsy attempts” to curtail subversive behavior, and suggesting that these two cases stand for the bedrock principle that “the state may not use universities as a weapon in an overbroad and ill-defined fishing expedition”).
Supreme Court examined and rejected such a statute in *Bantam Books v. Sullivan.* Like the Patriot Act’s pen register amendments, the law at issue in *Bantam Books* made it relatively easy for the authorities to cast a watchful eye on activities intimately related to academic inquiry, regardless of whether those activities were illegal.

In striking down the statute, the Court reasoned that it would have unduly burdened adults by making it much harder for them to acquire books deemed too obscene for young people. Remaining faithful to the spirit of this decision nearly forty years later, the Court held that a vaguely worded statute forbidding sexually explicit depictions of minors would prevent adults from reading textbooks and classic works of literature.

The Supreme Court is likely to be as critical of legal interference with Internet research as it was of book regulation, given the similar educational roles of the two media. The Court addressed the relationship between education and Internet regulation when it evaluated the Communications Decency Act of 1996 ("CDA"). Like the pen register law, the CDA suggested that a broad range of Web-based activity could trigger an investigation or criminal liability. In striking down the CDA for failing to define “indecent” and “patently offensive” communications, the Court once again refused to allow sweeping regulations to burden the learning process. Since this

---

84. See 372 U.S. 58, 60 (1963) (striking down a Rhode Island statute that established a local commission to investigate and prosecute those who sold books containing “obscene, indecent, or impure” language). Another part of the statute called upon the commission to promote morality by investigating situations that could cause “undesirable behavior in juveniles.” Id.

85. See id. at 72 (holding that the operation of the commission was nothing more than a “scheme of state censorship,” and noting that the law creating the commission sought not to advise booksellers but to “suppress” their lawful activities).

86. See id. at 71 (arguing that the commission’s mandate was vague, resulting in book distributors’ elimination of a wide variety of adult books and forcing adults to cross state lines in order to find these prohibited publications).

87. See Ashcroft v. Free Speech Coalition, 535 U.S. 234, 252-54 (2002) (invalidating on First Amendment grounds the Child Pornography Prevention Act of 1996, which prohibited any virtual or actual visual depiction of minors engaging in sexual conduct). The law’s broad language would, for example, prevent adults from looking at photos in psychology textbooks or watching film adaptations of Shakespeare’s Romeo and Juliet. Id. at 246-48.

88. See Reno, 521 U.S. at 853 (analogizing an Internet search to the act of selecting books from a “vast library including millions of readily available and indexed publications”).

89. See id. at 849 (examining two provisions of the Communications Decency Act of 1996 that sought to shield minors from “indecent” or “offensive” Internet-based communications).

90. See id. at 859 (noting that the statute subjected violators of the Act’s provisions to a fine and/or a prison sentence of up to two years in length).

91. See id. at 878 (criticizing the open-ended provisions of the law for their potential to ban artistic renderings of nude images, as well as Web-based inquiries)
decision, other courts confronting challenges to similar legislation have embraced the theory that broad regulation of Internet use chills inquiry into various critical issues.92

The aforementioned decisions show that legislatures generally have failed in their attempts to regulate educationally valuable speech, books, or electronic communications by enacting statutes containing sweeping proscriptive language.93 The Patriot Act’s pen register law limits the exercise of First Amendment rights to an equal, if not greater degree, by targeting the vast category of Web-browsing information that law enforcement officials may deem relevant to a criminal investigation.94 In so doing, the law ignores the enormous contribution that modern communications technologies play in the exploration of ideas.95 On a more general level, this impediment to free speech violates the constitutional requirement that a law clearly and accurately draws the line between unfettered and regulated speech at all times.96

C. Beyond Specific Proscriptions: How Indiscriminate Data-Gathering Chills Intellectual Activity

The pen register law, like the statutes under attack in Sweezy, Keyishian, and the later cases discussed in the previous section, provides only a vague description of the activity under regulation.97 The difference between those statutes and the pen register law, however, is that the former generally provided a swift and clear punishment for a violation of the proscribed behavior, while the latter allows law enforcement to generate and compile records of Internet

into such subjects as prison rape, safe sex, and birth control).

92. See, e.g., ACLU v. Johnson, 194 F.3d 1149, 1152-53, 1160 (10th Cir. 1999) (invalidating a New Mexico law proscribing computer communications depicting “sexual conduct,” and noting that the plaintiffs’ Internet-based “speech” included informative discussions of art, literature, sexuality, and civil rights issues).

93. See, e.g., Playboy, 529 U.S. at 827 (striking down on First Amendment grounds a provision of the Telecommunications Act of 1996 requiring cable television providers to “scramble” erotic programming or limit it to late hours).

94. See Evans, supra note 7, at 977 (arguing that the extremely low evidentiary requirement of relevance allows law enforcement to visit Web sites, review e-mail communications, and severely undermine the privacy rights of many people whose activities have nothing to do with the government’s criminal investigation).

95. See Playboy, 529 U.S. at 818 (characterizing technology as a “revolution” that “expands the capacity to choose” among competing opinions and statements about esthetics, morality, and other academic subjects).

96. See id. at 817 (cautioning that a failure to draw the fine line properly between guaranteed and prohibited speech “exacts an extraordinary cost” of preventing people from seeking knowledge without the intrusion of law enforcement).

97. See 18 U.S.C.A. § 3123(a)(2) (explaining that the court will grant the pen register order after a showing that the “information likely to be obtained . . . is relevant to an ongoing criminal investigation”).
addresses for no clear purpose. This potential for abusive and indiscriminate data-gathering reinforces the argument that the expanded pen register law, alone and in conjunction with other provisions of the Patriot Act, chills scholarly activity.

Legislators must narrowly tailor any law that authorizes data collection on teachers in pursuit of a legitimate state purpose. In Shelton v. Tucker, the Court determined that a statute requiring teachers to disclose group membership lists inhibits their “free play of the spirit” and, therefore, fails the narrow tailoring analysis. Because the pen register law makes it relatively easy for authorities to collect lists of Web addresses that a teacher or student visits, it burdens their “free play of the spirit” in a similar way. A slightly earlier decision had emphasized that such a close nexus between the governmental purpose for proscribing the speech or activity and the restraint upon the freedom to express becomes critical when unpopular views are vulnerable to suppression. The pen register law does not satisfy a narrow tailoring analysis because it is unclear that gathering and analyzing Internet address information will achieve its intended governmental interest—namely, preventing acts of terrorism.

Even when the legislative purpose is more urgent and compelling

98. Compare Keyishian, 385 U.S. at 614 (displaying the full anti-sedition statute, which provided for the “disqualification or removal” of teachers who violate its provisions), with Searching and Seizing Computers, supra note 39 (noting that the Pen/Trap Statute broadly defines pen register devices, which applies to a wide range of communications technologies that capture and store addressing information).

99. Cf. Michael N. Dolich, Note, Alleging a First Amendment “Chilling Effect” to Create a Plaintiff’s Standing: A Practical Approach, 43 Drake L. Rev. 175, 175-76 (1994) (illustrating the chilling effect of government surveillance by describing a hypothetical person who avoids a public meeting because the FBI will monitor it).

100. See Shelton v. Tucker, 364 U.S. 479, 488 (1960) (explaining that the principle of narrow tailoring requires lawmakers to employ the least drastic and restrictive means of achieving the legitimate governmental interest).

101. See id. at 487 (explaining that the Bill of Rights protects teachers’ freedom to think and act upon their thoughts). The Arkansas statute at issue in Shelton required every state teacher to submit a list of all organizations to which he or she belonged during the previous five years. Id. at 488.

102. See Searching and Seizing Computers, supra note 39 (describing the procedure for obtaining a pen register order, and explaining that the judicial role in approving pen register devices is only “ministerial” (quoting United States v. Fregoso, 60 F.3d 1314, 1320 (8th Cir. 1995))).

103. See NAACP v. Alabama, 357 U.S. 449, 464-66 (1958) (invalidating a policy requiring the NAACP to reveal its membership lists to the state, and reasoning that the state’s goal of identifying illegal business practices was an insufficient justification for burdening the NAACP’s activities).

104. See Kerr, supra note 21, at 636 (stating that the attacks of September 11 “did not directly implicate the Internet”); see also Martin, supra note 73, at 298 (arguing that monitoring a person’s reading activity to determine if she is a terrorist is no more effective than monitoring a person’s dietary habits to determine if she is Moslem).
than a teacher’s competency or the discovery of illegal business activities, the Supreme Court insists that government data collection activities still satisfy a narrow tailoring analysis. The Court remained loyal to this principle, for instance, in *Gibson v. Florida Legislative Investigation Committee*, where the Court found the express purpose of the legislation was the identification of communist threats to national security. The Court emphasized that a broad list-making power deprives free speech guarantees of the “breathing space” essential to their survival.

The federal government’s fearful efforts to combat communist infiltration during the McCarthy era parallel the government’s reaction to the modern terrorist threat. Indeed, some commentators assert that the current war on terrorism will wreak even more long-term havoc on civil liberties than did McCarthyism. Whether the perceived threat is communism or terrorism, national security is a vital governmental interest that the Court has, at times, used to justify extraordinarily repressive measures. Nevertheless, the Court’s decisions in both *Gibson* and in subsequent cases firmly establish that broad data collection for national security purposes must yield to the right to learn, question, and research controversial topics. This principle should apply equally to the present-day...

105. See *Shelton*, 364 U.S. at 488 (stating that even a legitimate and substantial government purpose can never justify means “that broadly stifle fundamental personal liberties” if there is the possibility of an equally effective and more closely tailored statute).

106. See *372 U.S. 539, 549 (1963)* (rejecting the argument that it is permissible to require admittedly legitimate organizations to disclose their membership records when the purpose of such a requirement is the general prevention of communist infiltration).

107. See *id.*, at 544 (arguing that data collection and other subtle forms of governmental interference are just as suspect as more overt attempts at regulation when these methods restrict the exercise of First Amendment guarantees).

108. See *Lardiere*, supra note 62, at 976-77 (predicting, nearly two decades before the September 11 terrorist attacks, that if the government perceives a threat to its stability as it did with communism until 1976, the government will again resort to unconstitutional data-gathering against innocent citizens).

109. See, *c.g.*, Robert D. Richards & Clay Calvert, *Nadine Strossen and Freedom of Expression: A Dialogue with the ACLU’s Top Card-Carrying Member*, 13 GEO. MASON U. CIV. RTS. L.J. 185, 206-07 (2003) (reproducing a statement of ACLU president Nadine Strossen, who argues that much of the civil rights abuse of the McCarthy era ended with the dismantling of congressional committees, whereas the civil liberties violations the Patriot Act sanctions will remain indefinitely because statutes are very difficult to repeal once they are “on the books”).

110. See, *e.g.*, *Korematsu v. United States*, 323 U.S. 214, 223 (1944) (holding that the internment of Japanese-Americans after the attack on Pearl Harbor was an acceptable means of satisfying the overwhelmingly important goal of national security).

111. See *Gibson*, 372 U.S. at 567 (Douglas, J., concurring) (arguing that far-reaching surveillance and record-keeping powers allow the government to “look over the shoulder of everyone who reads” and ultimately discourage free inquiry); see also
Freedom of inquiry suffers when government data-gathering burdens the scholar’s search for information, and this is no less true outside of a classroom or organizational setting. Lamont v. Postmaster General, decided just two years after Gibson, protected the First Amendment rights of an individual who sent for and received communist propaganda via the postal service. The Court explained its reasoning by noting that postal mail functions as a “flow of ideas.”

Because searching the Internet is in many ways the modern equivalent of sending away for published, hard-copy information, the Lamont Court’s “flow of ideas” metaphor accurately characterizes computer-based communications. The pen register laws, like the postal service statute, create an opportunity for the government to gather data whenever it determines that the activity of the information-seeker is controversial. As mentioned earlier, the Constitution combats this phenomenon by guaranteeing a large degree of anonymity to those who exercise their right to explore controversial subjects.

\[\text{E. Dist. of Mich.}, 407 \text{ U.S. at 314-21 (striking down a federal statute authorizing the President and Attorney General to gather and maintain intelligence pertaining to subversive forces, and reasoning that such official surveillance chills criticism of government policies).}\]

\[\text{112. See Sean Mussenden et al., USF Professor Arrested on Terror-Related Charges, ORLANDO SENTINEL, Feb. 21, 2003, at A1 (discussing the arrest of Professor Sami Al-Arian, whom the FBI accused of using the “academic environment” at the University of South Florida as a “staging point” for terrorist activity on behalf of the Palestinian Islamic Jihad).}\]

\[\text{113. See Bird & Brandt, supra note 10, at 437 (noting that the notion of academic freedom, as defined by the American Association of University Professors and recognized by law, includes the right to talk and write about matters outside of the classroom and beyond one’s field of expertise).}\]

\[\text{114. 381 U.S. 301 (1965).}\]

\[\text{115. See id. at 305-07 (invalidating on First Amendment grounds a federal postal service statute that allowed the Postmaster General to detain all mail appearing to contain communist political propaganda until the addressee submitted a reply card requesting delivery of the mail).}\]

\[\text{116. See id. at 306 (noting that the postal service statute hinders the flow of mail, and thus the “flow of ideas,” by requiring administrative officials to inspect the mail for communist propaganda, set it aside if it contains such propaganda, write the addressee about the problem, and await the reply card before finally sending the mail to the addressee).}\]

\[\text{117. See Surveillance Under the “USA/Patriot” Act, supra note 5 (noting that visiting a Web page is really the act of downloading the information from an electronic document on a remote computer to the Web-surfer’s computer).}\]

\[\text{118. See Lamont, 381 U.S. at 307 (expressing concern that schoolteachers and other public officials will fear disastrous consequences if the government believes that they are sending for and receiving treasonous materials).}\]

\[\text{119. See NAACP, 357 U.S. at 462-63 (invoking First Amendment protection after a}\]
Legal scholars and commentators often invoke George Orwell’s “Big Brother” concept when attempting to show how ever-present, real-time government surveillance creates anxiety and diminishes free will. Generally, this effect still arises even if the person under surveillance knows that her activities are lawful. Courts have recognized, for instance in *White v. Davis*, that free speech and inquiry suffer dramatically when undercover officers sit in college classrooms and compile records of their observations. The preservation of the classroom as the “crucible of new thought” has guided these decisions. Given the enormous amount of information it offers, one could view the Internet as another crucible of thought. In light of this analogy, the use of a pen register to collect Web-surfing activity is no less Orwellian than the use of undercover policemen to monitor classroom discussions.

A fear of Orwellian surveillance procedures, however, is not necessarily enough to invalidate a national security or crime-control measure. For example, the New Jersey Supreme Court upheld police department policies authorizing official showing that sharing membership lists and records with others has exposed individual members to loss of employment, threats of physical harm, and general public hostility in the past and could bring about these same results again).

120. See James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 12 (2003) (observing that data-collection systems, like the radically authoritarian regime known as “Big Brother” in George Orwell’s novel, 1984, are an ongoing form of observation that limit freedom by tightening the government’s hold over various aspects of citizens’ lives).

121. See id. at 15 (noting that most people legitimately fear that information collected about them could be used in a derogatory or dangerous manner, even where the information is mundane and harmless).

122. See 533 P.2d 222, 229 (Cal. 1975) (invalidating on free-speech grounds a policy of the Los Angeles Police Department that allowed undercover policemen to attend university classes and meetings in order to take notes for their files). The goal of this practice was the anticipation and prevention of future crime. *Id.* at 227.

123. See id. at 231 (describing the campus classroom as sacred and warning that classroom surveillance practices by undercover police endanger everyone’s sense of security in free expression and is only one step removed from a totalitarian regime).

124. See *Reno*, 521 U.S. at 851-52 (noting that Internet newsgroups accommodate about 100,000 daily message postings, allowing for the exchange of information on everything from music to politics, and concluding that the Internet is as varied and colorful as the full range of human thoughts).

125. See Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1105-04 (2002) (arguing that the absence of checks on the government’s power to collect Web-surfing information poses a threat to anonymity in intellectual pursuits, and that such an absence is one facet of an anti-democratic culture).

126. See Haig v. Agee, 453 U.S. 280, 307 (1981) (upholding the Secretary of State’s revocation of an American citizen’s passport because it is “obvious and unarguable” that no government interest is more important than national security).

data-gathering at public events.\textsuperscript{128} Though \textit{Sills} may seem at odds with \textit{White}, the specific rights of education and freedom of inquiry were more directly at stake in the latter case.\textsuperscript{129} Because these rights have an exalted position among the First Amendment guarantees, burdens on those rights may invite even greater scrutiny than burdens on the right to assemble.\textsuperscript{130}

The decisions above also suggest that courts evaluate data-gathering methods more rigorously if a legislative body has sanctioned those methods.\textsuperscript{131} The Supreme Court provided support for this idea two years after \textit{Sills} when it upheld army surveillance tactics not unlike those at issue in \textit{Sills}.\textsuperscript{132} In each case, the data-gathering occurred pursuant to a general policy or practice rather than an actual law.\textsuperscript{133} The Internet surveillance provisions in the pen register law, by contrast, are a product of Congress and therefore should not escape full judicial review.\textsuperscript{134}

\textbf{D. Internet Surveillance Anxiety as a Justiciable Injury}

Given the \textit{Laird} Court’s refusal to address the merits of, let alone strike down, the Army’s broad surveillance tactics, a student or teacher may have difficulty persuading a court that the Patriot Act chilled her Internet use enough to warrant a remedy.\textsuperscript{135} However,

\begin{itemize}
\item \textsuperscript{128} See id. at 688-89 (upholding the constitutionality of an internal police department memorandum that urged law enforcement officials to exercise their crime-prevention duties by gathering intelligence on rallies, demonstrations, and other public events because such actions were necessary and reasonable for police to accomplish their mission).
\item \textsuperscript{129} Cf. id. at 682-83 (emphasizing that the plaintiffs only “envison” harassment and injury as a result of police surveillance at protests, demonstrations, marches, or other purely hypothetical activities).
\item \textsuperscript{130} See Keyishian, 385 U.S. at 603 (discussing the inherent value of academic freedom and stating that it is a “special concern of the First Amendment”).
\item \textsuperscript{131} See, e.g., \textit{Sills}, 265 A.2d at 684 (noting that the surveillance provisions appeared in a general memorandum circulated among law enforcement agencies, and concluding that the Constitution demands precision only of a legislative enactment).
\item \textsuperscript{132} See \textit{Laird} v. Tatum, 408 U.S. 1, 14-16 (1972) (holding that Army surveillance policies do not cause an unconstitutional chilling effect on citizens’ exercise of their First Amendment rights).
\item \textsuperscript{133} See, e.g., id. at 16 (Douglas, J., dissenting) (noting that the Army’s activities under challenge result from Pentagon policy rather than law). If Congress had passed an actual law authorizing surveillance this extensive, “a most serious constitutional problem” would exist. \textit{Id}.
\item \textsuperscript{134} See \textit{LEVY}, supra note 8 (noting that the Patriot Act subverts the separation of powers doctrine by authorizing “rubber-stamp judicial supervision” of government surveillance of the Internet, and warning that the Executive branch will not always use its power in benevolent or constitutional ways).
\item \textsuperscript{135} See \textit{Laird}, 408 U.S. at 11 (explaining that the complainant lacked standing to allege a chilling effect because the Army’s policy was not “regulatory, proscriptive, or compulsory in nature” and did not injure the complainant through any regulations or
\end{itemize}
while the pen register laws are neither directly regulatory nor proscriptive, the harm that they could inflict on an Internet researcher is real. Moreover, the U.S. Supreme Court has not distinguished between a burden on a First Amendment right and the wholesale elimination of that right. Indeed, a legally actionable injury can result from a system of ongoing surveillance that creates nothing more than the mere possibility of a First Amendment burden.

The arguments above support the proposition that, Laird notwithstanding, the question of what constitutes a justiciable First Amendment injury remains unsettled. For example, due to the ease with which the government can obtain a pen register order and monitor Web sites, a person may avoid researching terrorism via the Internet. This type of "chill" stems from a fear of punishment for exploring or expressing an unpopular idea, and several courts have recognized that such a fear is a valid injury.

The fear may be particularly acute, and the injury exceptionally proscriptive).
severe, if one considers the pen register definition’s relationship to other parts of the Patriot Act. Even an innocent person reasonably may worry that investigators will, at some future date, interpret the fruits of their surveillance as evidence of terrorism or other forms of criminal activity.\textsuperscript{142}

One basis for this fear is the Patriot Act’s expansive definition of terrorism, which could cause the government to regard numerous Web sites with suspicion.\textsuperscript{143} Once law enforcement authorities certify that an Internet researcher’s work is somehow relevant to an investigation, little prevents them from determining that Web sites discussing Al Qaeda, for example, seek to influence national policy by intimidation or coercion.\textsuperscript{144} Less than three months after September 11, then-Attorney General John Ashcroft went a step further by suggesting that people who criticize the “War on Terror” only would be helping the enemies of the United States.\textsuperscript{145}

Another basis for this fear of arrest is the “technology-neutral” definition of the pen register itself, which may enable investigators to use inappropriately sophisticated and intrusive data-collection devices as they monitor the Internet.\textsuperscript{146} At the same time, another section of the Patriot Act grants immigration officials and various other authorities easy access to terrorist-related surveillance data.\textsuperscript{147} Thus,

\textsuperscript{142} See Nehf, supra note 120, at 23-24 (noting that data collection allows businesses or law enforcement to judge people on the basis of scattered information, and that this often leads to a harmful and negative mischaracterization of a person).

\textsuperscript{143} See Patriot Act § 802, 115 Stat. at 376 (defining domestic terrorism as acts dangerous to human life, which are a violation of the criminal laws of the United States, and are intended “to intimidate or coerce a civilian population” or “influence the policy of a government by intimidation or coercion”).

\textsuperscript{144} See Chang, supra note 49 (arguing that law enforcement could construe the Patriot Act’s definition of domestic terrorism broadly to justify surveillance of environmental activists, anti-abortion activists, and political organizations that question government policies).

\textsuperscript{145} See Testimony of Attorney General John Ashcroft Before the Senate Comm. on the Judiciary (Dec. 6, 2001) (advising all those who “scare peace-loving people with phantoms of lost liberty” that such statements “only aid terrorists” and “erode our national unity and diminish our resolve”), available at http://www.usdoj.gov/ag/testimony/2001/1206transcriptsenatejudiciarycommittee.htm.

\textsuperscript{146} See Searching and Seizing Computers, supra note 39 (noting that the pen register/trap and trace devices have such “broad, technology-neutral” definitions that law enforcement agents may not always know whether a given device fits the statutory definition of these instruments); see also Chang, supra note 49 (stating that the vague language of the pen register provisions implicitly permit the use of Carnivore (now called DCS-1000), a controversial surveillance tool that may collect Web pages visited and other content). But see Haglund, supra note 11, at 141 (arguing that criticism of DCS-1000 is inaccurate, because this device collects only source and destination information, as opposed to specific terms in the Web address, when operating in pen register mode).

\textsuperscript{147} See Patriot Act § 203, 115 Stat. at 281 (stating that investigators may share any foreign intelligence information they obtain from a criminal investigation with any “Federal law enforcement, intelligence, protective, immigration, national defense, or
under this system of potentially reckless surveillance and liberalized data-sharing, it seems that officials will possess almost limitless power to scrutinize a person’s Web addresses. As with the new definition of terrorism, these concerns have a basis in reality: the Patriot Act already has enabled the government to arrest scholars whose activities may or may not indicate a true terrorist threat.

The infamous “nationwide service” provision of the Patriot Act provides the third major way that law enforcement may abuse the pen register to the detriment of Internet users. Because it allows investigators to use a single pen register order to monitor Internet usage anywhere in the United States, commentators fear that it unconstitutionally authorizes the equivalent of blank warrants. This procedural simplification arguably strips away some of the judiciary’s power and legitimacy. This system of virtually unchecked surveillance may scare Internet researchers into confining their scholarship to “safe” topics. Such an environment further discourages explorations of Islam or terrorism at a time when these constitutionally protected activities are already coming under fire.

national security official” in order to assist that official in her own duties); see also Surveillance Powers: A Chart, ACLU Online Archives (2002) (explaining that, prior to the passage of the Patriot Act, much of the information gleaned from surveillance procedures was unavailable to non-relevant law enforcement authorities), at http://www.aclu.org/Privacy/Privacy.cfm?ID=13601&c=130 (last visited Apr. 9, 2005).

148. See Evans, supra note 7, at 983 (arguing that the extensive sharing of surveillance data among government agencies effectively erases their separate roles and makes them more likely to abuse their power).

149. See, e.g., Mussenden et al., supra note 112, at A1 (stating that Attorney General Ashcroft credits the Patriot Act, and particularly its data-sharing provision between intelligence and law enforcement, for the investigation and arrest of Professor Sami Al-Arian).

150. See Patriot Act § 216, 115 Stat. at 288-89 (amending Title 18 of the United States Code to authorize a court to issue a pen register/trap and trace order “anywhere within the United States,” as opposed to the specific jurisdiction in which the investigator wishes to conduct surveillance).

151. See Evans, supra note 7, at 978-79 (arguing that, because the Fourth Amendment requires the court to state with particularity the person or place to be searched, the “nationwide service” of pen register orders violates this constitutional requirement).

152. See id. at 978 (noting that, under the blank warrant system, the judge will be unable to ensure that investigators are focusing on the correct target and collecting data for legitimate reasons).

153. See Nehf, supra note 120, at 11 (stating that limitless surveillance and data-collection evoke images of Bentham’s Panopticon, which allowed full surveillance of hundreds of prisoners simultaneously by a single authority). Knowledge of surveillance, whether from the Panopticon or modern methods of data collection, curtails free will and shapes human behavior to satisfy a prescribed norm. Id.

154. See AMERICAN COUNCIL OF TRUSTEES AND ALUMNI, supra note 72, at 6 (criticizing American colleges and universities for adding courses on Islamic and Asian cultures, instead of additional courses on “the civilization under attack,” after the September 11 events).
III. "FIXING" THE PEN REGISTER STATUTE: FEARS AND SOLUTIONS

Given the vagueness of the Patriot Act’s definition of the pen register and the problematic ways in which this definition interacts with other Patriot Act provisions, a legally justiciable chill on an Internet user’s freedom of inquiry certainly exists. This section proposes ways to correct the constitutional defects in the pen register legislation while preserving law enforcement’s ability to combat crime and safeguard national security.

The drafters of the Patriot Act’s expanded pen register definition probably presumed that the phrase “routing, addressing, and signaling information” would exclude content from Internet surveillance. The Justice Department believes that this is the case, and it notes that the pen register law explicitly forbids the collection of “content.” Nevertheless, because the definition of Internet content is no clearer than the concept of Internet addressing information, the argument is circular and does nothing to clarify the law’s ambiguity.

An obvious way to save this provision from its own vagueness is to define one or both of these terms in technology-specific language. Much of the confusion would disappear, for instance, if the pen

155. See Dolich, supra note 99, at 189-90 (noting that, though the law of standing and judicially cognizable injury is still taking shape, a regulation containing a veiled threat to the exercise of free speech rights may pose a legally actionable injury).

156. See generally LEVY, supra note 8 (stating that the U.S. government’s most important obligation is the protection of life from “domestic and foreign predators” while safeguarding civil liberties to as great a degree as possible).


158. See 18 U.S.C.A. § 3127(3) (stating that the addressing information that the pen register collects “shall not include the contents of any communication”); see also SEARCHING AND SEIZING COMPUTERS, supra note 39 (stating that Title III of the Omnibus Crime Control and Safe Streets Act of 1968, and not the pen register statute, allows the seizure of Internet contents).

159. See 18 U.S.C.A. § 2510(8) (defining content, as the term appears in the pen register statute, as “any information concerning the substance, purport, or meaning of “any wire, oral, or electronic communication”); see also Kerr, supra note 21, at 647 (noting that the Patriot Act’s pen register provisions represent a “missed opportunity” to clarify the foggy distinction between addressing and content information in human-to-computer communications).

160. See Kerr, supra note 21, at 647 (noting that the statutory definition of “contents” is unacceptably vague and has not changed since 1986, many years before the arrival of the Internet).
register definition stated that addressing information, in the Internet context, includes only "source and destination information."161 This relatively simple solution presumably would satisfy scholars who fear that surveillance of their Internet research will reveal too much about their thoughts or interests.162

In the absence of changes to the statutory definitions, Internet researchers might feel less fearful of intrusive surveillance if it were more difficult to obtain a pen register order.163 Currently, investigators need only state the crime under investigation.164 It is very likely that more speech and privacy protection would be available if pen register applicants had to show probable cause and obtain a warrant.165 Moreover, even those who question the assumption that a probable cause showing would increase privacy seem to accept that this evidentiary requirement would not hamper law enforcement.166

Conditioning the granting of a pen register order upon a showing of probable cause is a more drastic proposal than it may appear because it necessitates overruling the Supreme Court decision in Smith, which deals with the pen register.167 Judges, however, never have embraced fully the notion that transactional information, such as telephone numbers and Web addresses, deserve such minimal privacy protection.168 In addition, commentators note that the Smith

161. See Haglund, supra note 11, at 141 (explaining that any surveillance device that limits its collection to Internet source and destination information could retrieve no letters, words, or search terms from a Web address beyond the Internet protocol, such as yahoo.com).

162. See Surveillance Under the “USA/Patriot” Act, supra note 5 (arguing that a list of Web addresses that a person visits displays intimate information about a person’s thoughts and identity, much like the title of a book that a person wishes to read).

163. See Evans, supra note 7, at 977-78 (arguing that the current “relevant to an ongoing criminal investigation” standard of proof is extremely low and has the unpleasant effect of disrupting the lives of many innocent people with which the government has no interest).

164. See 18 U.S.C.A. § 3123(b)(1)(D) (requiring that the contents of the order shall specify “a statement of the offense to which the information likely to be obtained by the pen register or trap and trace device relates”).

165. See Solove, supra note 125, at 1162-63 (arguing that the Fourth Amendment’s warrant requirement, issued upon a finding of probable cause, helps prevent the government from abusing its surveillance powers by minimizing its collection powers to only essential information thereby ensuring that a specific person is the target of the surveillance, and by calling for a neutral and detached magistrate to authorize the surveillance).

166. See Kerr, supra note 21, at 639 (conceding that a “specific and articulable facts” requirement would not significantly hamper law enforcement, even if this evidentiary requirement protects privacy only “on paper”).

167. See Smith, 442 U.S. at 744 (reasoning that a person has no legitimate expectation of privacy in the telephone number she dials because using a telephone requires conveying that number to the telephone company and thus “assum[ing] the risk” of disclosure).

168. See id. at 748 (Stewart, J., dissenting) (arguing that a telephone number
holding is antiquated and increasingly unpopular. Finally, Smith seems to go against most people’s intuitive conception of privacy. For these reasons, and because modern telephonic communications resemble Internet communications, overruling Smith statutorily may be appropriate and even desirable.

Because the Patriot Act’s definition of domestic terrorism is as sweeping as the definitions of content or addressing, it too requires revision to protect the Internet researcher from undeserved surveillance. A meaningful and appropriately precise definition of domestic terrorism should not draw within its scope potentially ambiguous activities, such as those intended to “intimidate or coerce a civilian population” or “influence the policy of a government by intimidation or coercion.” Thus, Congress should repeal the two subparts above and leave the third provision, which describes the malicious nature of true terrorism more accurately.

Another solution involves placing clear time limits on the duration of every clause of the pen register law and the intra-governmental data-sharing provisions of the Patriot Act. These Congressionally contains an element of content because, like a full conversation, it could reveal “the most intimate details of a person’s life” by displaying the identities of the caller and the people called).

169. See Solove, supra note 125, at 1137-38 (observing that Smith has received a great deal of criticism over the years because its holding is based on simplistic notions of privacy that allow electronic monitoring to become increasingly intrusive as surveillance technology evolves).

170. See Smith, 442 U.S. at 748 (Stewart, J., dissenting) (expressing doubt as to whether “there are any who would be happy to have broadcast to the world” a record of the telephone numbers they have dialed); see also Haglund, supra note 11, at 137 (observing that despite the Supreme Court’s position, people generally regard addressing information, such as Internet addresses, as private).

171. See Haglund, supra note 11, at 147 (explaining that the technology in use to route telephone calls increasingly resembles the packet-based technology in use to transmit computer communications). Because this new form of telephone technology, like computer communications, blurs the distinction between addressing and content information, a pen register order may soon be as inappropriate for telephone calls as it is for the Internet. Id.

172. See CHANG, supra note 49 (cautioning that until Congress clarifies the definition of terrorism, the public needs a mechanism that closely monitors the types of organizations and activists that the government selects for surveillance pursuant to this definition).


174. Id.

175. See id. (providing an amendment to the United States Code that defines terrorism as activities intended to “affect the conduct of a government by mass destruction, assassination, or kidnapping”).

176. See Ann Harrison, Behind the USA Patriot Act (Nov. 5, 2001) (noting that while certain portions of the Patriot Act expire in 2005, the pen register law and the provision allowing the sharing of grand jury information will continue indefinitely), at http://www.alternet.org/story.html?StoryID=118547.
determined expiration dates, known as “sunset laws,” may be the path of least resistance. Sunset laws preserve the Patriot Act’s statutory language and all underlying judicial decisions while ensuring that any resulting incursions on civil liberties last no longer than national security concerns require. On the negative side, however, sunset provisions raise troublesome questions concerning the acceptable duration of burdens on basic constitutional rights. More specifically, the comprehensive sunset solution fails to address the extent to which investigators may monitor Web browsing. A comprehensive set of sunset provisions, however, would at least provide Congress with an opportunity to reevaluate the Patriot Act and draft a more efficient and narrowly tailored law from scratch.

A final proposal involves leaving the pen register law and other parts of the Patriot Act untouched while raising public awareness of the real-life threat these provisions pose to First Amendment rights. The government could help by reversing course and sharing pre- and post-Patriot Act data-collection statistics with the public. University leaders also could raise awareness of civil liberty issues by encouraging, rather than stifling, inquiry into government policies.

177. See BLACK’S LAW DICTIONARY 1450 (7th ed. 1999) (defining a sunset law as a “statute under which a governmental agency or program automatically terminates at the end of a fixed period unless it is formally renewed”).

178. See LEVY, supra note 8 (praising sunset laws as a means of ensuring that drastic legislative measures are temporary and as a means of forcing the government to justify periodically any continuing intrusions on civil liberties).

179. See Jacob R. Lilly, Note, National Security at What Price?: A Look Into Civil Liberty Concerns in the Information Age Under the USA PATRIOT Act of 2001 and a Proposed Constitutional Test for Future Legislation, 12 CORNELL J.L. & PUB. POL’Y 447, 463 (2003) (observing that sunset provisions are powerless to prevent violations while the questionable law is in effect and therefore provide little consolation to the person whose constitutional rights suffer during this period).

180. See Kerr, supra note 21, at 639 (explaining that the pen register amendments actually enhanced privacy protections on the Internet by requiring a court order for surveillance, where quite possibly no authorization was necessary before).

181. See Richards & Calvert, supra note 109, at 208 (quoting ACLU President Nadine Strossen, who argues that the Patriot Act, as a whole, is not narrowly tailored to fight terrorism because “the vast majority of its provisions, even on their face, really had nothing to do with terrorism” or deal only with criminal law enforcement in general). Many members of Congress might not vote for the Patriot Act today if they received a chance to reconsider their decision. Id. at 207.

182. See id. at 215 (pointing out that people are generally indifferent to the constitutional rights of others until they believe that their own rights may be at stake).

183. See ACLU, 265 F. Supp.2d at 34-35 (denying the ACLU’s Freedom of Information Act request that the Justice Department produce statistics revealing how often and under what circumstances the government has used the Patriot Act).

184. See Bird & Brandt, supra note 10, at 459 (reporting that college presidents often have disavowed controversial statements by faculty members and suggesting that these administrators fear experiencing public criticism for endorsing unpopular views).
Widespread public apathy of both the average citizen and the Internet scholar damages First Amendment safeguards more than terrorism or the legislation Congress enacts to combat it.\textsuperscript{185}

\textbf{CONCLUSION}

The Patriot Act’s amendments to the pen register statute, and particularly the expanded pen register definition, burden intellectual freedom by simplifying law enforcement’s ability to monitor and record Web addresses. The history of pen register use and Congress’ rushed passage of the amendments suggest that this tool should not extend to the Internet without a higher evidentiary showing.\textsuperscript{186} Because the precise connection between Web browsing and terrorism remains unclear, allowing virtually unregulated collection of Internet addresses “burn[s] the house to roast the pig.”\textsuperscript{187} National security concerns seem to overshadow civil liberties under such a scheme, and this runs counter to the spirit and tradition of American law.\textsuperscript{188}

Textual modifications to the Patriot Act or a comprehensive sunset plan may lighten the burden on freedom of Web-based inquiry.\textsuperscript{189} In the meantime, the academic world can and should nurture the exploration and debate of controversial ideas.\textsuperscript{190} Tolerance of new perspectives and the desire for legislation embodying that tolerance, however, are of paramount importance and must come solely from the individual.\textsuperscript{191}

\textsuperscript{185}See Richards & Calvert, supra note 109, at 241 (opining that the greatest menace to free speech is too little awareness of and interest in other people’s rights to express their ideas).

\textsuperscript{186}See Evans, supra note 7, at 988 (noting that because the Patriot Act provides no specific guidelines governing how investigators should avoid capturing content with an Internet pen register order, greater collaboration between the Attorney General and the FBI is necessary in this area).

\textsuperscript{187}See Butler v. Michigan, 352 U.S. 380, 383 (1957) (striking down a statute banning the sale of lewd books to all members of the general public, and cautioning that the State’s legitimate desire to “promote the general welfare” does not justify legislation that “burn[s] the house to roast the pig”).

\textsuperscript{188}See Richards & Calvert, supra note 109, at 207-08 (noting Nadine Strossen’s observation that, because no provision in the Bill of Rights explicitly states that constitutional rights are subject to restriction during a time of war, the Constitution contains a “presumption in favor of freedom”).

\textsuperscript{189}See Lilly, supra note 179, at 469 (proposing, as a means of making the Patriot Act more constitutionally sound, a sunset clause lasting until the national security crisis ends or until the end of a two-year period, whichever date comes first).

\textsuperscript{190}See Bird & Brandt, supra note 10, at 432 (noting that universities are uniquely able to incubate the most advanced scientific, artistic, and political ideas because of their “insularity” from popular opinion and economic concerns).

\textsuperscript{191}See Richards & Calvert, supra note 109, at 202 (calling upon everyone to “look through the substance” of opinions they despise and recognize that free speech principles cannot apply to themselves unless they apply equally to others).