

## Protecting the Lady from Toledo: Post-USA PATRIOT Act Electronic Surveillance at the Library\*

Susan Nevelow Mart\*\*

*Library patrons are worried about the government looking over their shoulder while they read and surf the Internet. Because of the broad provisions of the USA PATRIOT Act, the lack of judicial and legislative oversight, the potential for content overcollection, and the ease with which applications for pen register, section 215 orders, or national security letters can be obtained, these fears cannot be dismissed.*

If the lady from Toledo can be required to disclose what she read yesterday and what she will read tomorrow, fear will take the place of freedom in the libraries, bookstores, and homes of the land.<sup>1</sup>

¶1 The ability to investigate ideas, without “the spectre of a government agent . . . look[ing] over the shoulder of everyone who reads,”<sup>2</sup> is a cornerstone of democracy. If one goal of the First Amendment is to achieve the “widest possible dissemination of information from diverse and antagonistic sources,”<sup>3</sup> the library is the place the public goes to investigate those ideas. The USA PATRIOT Act<sup>4</sup> will, unless amended by legislative or court action, alter the traditional role libraries have played as neutral, private places to investigate the full range of ideas necessary to be an informed citizen of a democracy. The library will not be “the quintessential locus of the receipt of information”<sup>5</sup> if patrons are worried that the government is looking over their shoulder while they read. The USA PATRIOT Act has expanded and simplified the ability of the government to compel the disclosure of patrons’ reading habits.

¶2 In his article *An Overview of the Law of Electronic Surveillance Post-September 11, 2001*, Robert A. Pikowsky suggested that many of the amendments

---

\* © Susan Nevelow Mart, 2004.

\*\* Reference Librarian, University of California, Hastings College of the Law Library, San Francisco, California.

1. *United States v. Rumely*, 345 U.S. 41, 58 (1953) (Douglas, J., concurring) (House Committee authorized to investigate “lobbying” was not authorized to demand the names of those who purchased, for distribution, books of a particular political persuasion; and therefore the conviction of a witness refusing to produce such names could not be upheld.).
2. *Id.* at 57.
3. *Associated Press v. United States*, 326 U.S. 1, 20 (1945).
4. *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter USA PATRIOT Act].
5. *Kreimer v. Bureau of Police*, 958 F.2d 1242, 1255 (3d Cir.1992).

made to existing legislation by the provisions of the USA PATRIOT Act were technical in nature, and that librarians had simply been unaware that the basic statutory schemes had long been in place for surveillance in the library.<sup>6</sup> In light of the preexisting nature of surveillance techniques, Pikowsky stated that the USA PATRIOT Act did not have an “unreasonable impact on the privacy of library clients; it merely awakened the library community to the issues of electronic surveillance that had already existed.”<sup>7</sup> Pikowsky further suggested that, balancing the need for surveillance of terrorists against the privacy of library patrons, privacy might be the loser.<sup>8</sup>

¶3 However “technical” in nature, the changes the USA PATRIOT Act made to federal laws that directly implicate libraries greatly broaden the powers of the government to seize patron information seeking records and greatly reduce accountability and judicial oversight. This increased power and decreased accountability has a chilling effect on the First Amendment rights of all library patrons. Where patron records of reading material are concerned, patron privacy and the constitutional right to receive information should trump government fishing expeditions.

¶4 This tension between the need for information to combat domestic or international crime and the need for protecting the privacy of library patrons is not new.<sup>9</sup> The previous outcome of these battles has eventually been in favor of granting a fairly high level of due process protection to records of reading material.<sup>10</sup> To paraphrase Justice Douglas, if the lady from Toledo knows that what she read yesterday at the library and what she will read tomorrow from the library can be secretly disclosed to the government, fear will take the place of freedom in the libraries of the land.<sup>11</sup>

### Post-September 11 Developments in Library Electronic Surveillance

¶5 Looking at the statutory framework affecting libraries before the USA PATRIOT Act and after, this writer respectfully disagrees with Pikowsky that the changes are technical and will “not have an unreasonable impact on the privacy of library patrons.”<sup>12</sup> Looking only at those provisions that affect libraries in a

---

6. Robert A. Pikowsky, *An Overview of the Law of Electronic Surveillance Post-September 11, 2001*, 94 LAW LIBR. J. 601, 620, 2001 LAW LIBR. J. 37, ¶ 71.

7. *Id.*

8. *Id.* at 619–20, ¶ 70 (questioning whether it is appropriate to allow a library patron “greater anonymity than someone who uses his own home computer”).

9. *See infra* ¶¶ 40–41.

10. Many of the present library record protection statutes were passed in response to the FBI’s Library Awareness Program. HERBERT N. FOERSTEL, SURVEILLANCE IN THE STACKS: THE FBI’S LIBRARY AWARENESS PROGRAM 133–34 (1991).

11. *See supra* text accompanying note 1. Douglas is eloquent on the chilling effect of having the nature of the information one receives exposed.

12. Pikowsky, *supra* note 6, at 620, ¶ 71.

new or altered way, the landscape for library surveillance has clearly changed.<sup>13</sup> Of the provisions of the USA PATRIOT Act that apply to information that is available from library records, the following provisions are of special concern to librarians. Each raises questions about civil liberties for library patrons that did not exist before September 11, 2001.

- **Section 216**<sup>14</sup> amended the authorities governing the use of pen registers, so that federal courts must now issue a pen register order for real-time interception of noncontent information from computers, not just from telephones.
- **Section 214** amended the Foreign Intelligence Surveillance Act (FISA),<sup>15</sup> broadening the reasons the government may apply to the FISA court for a pen register order for real-time interception of noncontent information from computers and telephones.<sup>16</sup>
- **Section 218** allowed a FISA wiretap of content information on any computer where a “significant purpose” of the investigation is to gather foreign intelligence.<sup>17</sup> The FISA court must issue the warrant if the government certifies that certain conditions are present.<sup>18</sup>
- **Section 206** made this FISA wiretap a roving wiretap, to be attached to any computer a suspect uses, including a library computer.<sup>19</sup>
- **Section 215** amended FISA and now includes libraries as entities subject to a FISA warrant for records and any tangible thing.<sup>20</sup>
- **Section 505** allowed national security letters, which are issued administratively and come with a gag order, to be issued by a broader range of government personnel and to require a lower standard of relevancy.<sup>21</sup>

---

13. There are provisions of the USA PATRIOT Act that may impact libraries that will not be addressed in this article. For example, although sections 201 and 202 of the Act broadened the list of crimes for which a Title III wiretap order might be issued, the change has little impact on libraries in particular. The need for the government to establish probable cause for a Title III warrant is still a statutory requirement. See Omnibus Crime Control and Safe Streets Act of 1968, § 802, 82 Stat. 197, 218–19. For accessible charts that provide an overview of the full range of legal process that could be directed to a library, see Mary Minow, *Library Records Post-PATRIOT Act*, at <http://www.llrx.com/features/libraryrecords.htm> (Sept. 16, 2002); Wiley, Rein & Fielding, LLP, *The Search & Seizure of Electronic Information Before and After the USA PATRIOT Act*, at <http://www.aau.edu/resources/Patriot.pdf> (Jan. 18, 2001). For a brief but useful overview, color coded for risk of potential for violation of civil liberties, see Erwin Chemerinsky, *Code Red, White, & Blue: Litigation Alerts in the USA PATRIOT Act*, CAL. LAW., Apr. 2003, at 29–31.

14. USA PATRIOT Act, Pub. L. No. 107-56, § 216, 115 Stat. 272, 288–90 (amending 18 U.S.C. §§ 3121(c), 3123(a), 3123(b)(1), 3123(d)(2), 3124(b), (3124(d), 3127(1)–(4) (2000)).

15. Foreign Intelligence Surveillance Act, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (hereinafter FISA).

16. § 214, 115 Stat. at 286–87 (amending 50 U.S.C. § 1842 (2000)).

17. § 218, 115 Stat. at 291 (amending 50 U.S.C. § 1823(a)(7)(B), 50 U.S.C. § 1804(a)(7)(B) (2000)).

18. 50 U.S.C. § 1805(a)(5) (2000).

19. § 206, 115 Stat. at 282 (amending 50 U.S.C. § 1805(b)(2)(B) (2000)).

20. § 215, 115 Stat. at 287–88 (amending 50 U.S.C. §§ 1861–1863 (2000)).

21. § 505, 115 Stat. at 365 (amending 18 U.S.C. § 2709(b) (2000)).

### *Pen Register Orders under Section 216*

¶6 If the government wants to perform electronic surveillance, it makes a difference what kind of information is being sought. The courts have long drawn a distinction between noncontent information, such as a telephone number, and content information, such as the actual words spoken during the telephone call. In *Smith v. Maryland*, the Supreme Court adopted the definition of a pen register as “a mechanical device that records the numbers dialed on a telephone by monitoring the electrical impulses cause when the dial on the telephone is released,”<sup>22</sup> and held that since the installation and use of a pen register was not a search under the Fourth Amendment, a warrant was not needed.<sup>23</sup> If no content is recovered, it’s not a search; since no warrant is needed, the government does not have to show probable cause. The standard for issuing a pen register order was set by statute in 1982.<sup>24</sup> The standard is that “the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation.”<sup>25</sup> By way of contrast, where a warrant is required, probable cause is generally defined as:

A reasonable ground to suspect that a person has committed or is committing a crime or that a place contains specific items connected with a crime. Under the Fourth Amendment, probable cause—which amounts to more than a bare suspicion but less than evidence that would justify a conviction—must be shown before . . . [a] search warrant may be issued. . . .

“Probable cause may not be established simply by showing that the officer who made the challenged arrest or search subjectively believed he had grounds for his action. . . . ‘If subjective good faith alone were the test, the protection of the Fourth Amendment would evaporate, and the people would be ‘secure in their persons, houses, papers, and effects’ only in the discretion of the police.’”<sup>26</sup>

The standard for issuing an order for a pen register was not changed by the USA PATRIOT Act. What the USA PATRIOT Act made clear was that pen register orders could attach to computers.<sup>27</sup>

- 
22. 442 U.S. 735, 736 n.1 (1979). The trap and trace device is the flip side of a pen register; it records incoming information. 18 U.S.C. § 3127(4) (Supp. 2001). The analysis of pen registers applies to trap and trace devices. However, this article is more directly concerned with pen registers; the recording of outgoing information in the form of Web browsing information, whether directly or as a byproduct of utilizing on line forms, is the activity in the library librarians are most concerned with protecting.
  23. *Smith*, 442 U.S. at 745–46.
  24. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. § 3123(a) (2000)). Prior to this act, there was no standard. See Pikowsky, *supra* note 6, at 608, ¶ 23.
  25. 18 U.S.C. § 3123(a).
  26. BLACK’S LAW DICTIONARY 1219 (7th ed. 1999) (quoting WAYNE R. LAFAVE & JEROLD H. ISRAEL, CRIMINAL PROCEDURE § 3.3, at 140 (2d. ed. 1992)). For a pen register order, a subjective belief is more than adequate.
  27. Because the pre-USA PATRIOT Act version of 18 U.S.C. § 3127(3) (2000) applied by its express terms only to telephone lines, the applicability of the statute to computer line surveillance was not clear. The section previously read: “‘pen register’ means a device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted *on the telephone line* to which such device is attached.” (emphasis added). *But see* Orin S. Kerr, *Internet Surveillance Law*

¶7 The critical amendments section 216 made to pen register orders are:

- Orders authorizing pen registers now apply to any “routing” or “addressing” information as well as any “dialing” information, and to “the processing and transmitting of wire or electronic communications” instead of just “call processing” information.<sup>28</sup> The orders apply “to any person or entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order.”<sup>29</sup>
- The order can now be served anywhere in the United States on anyone providing such a service, whether named in the order or not.<sup>30</sup>
- A law enforcement agency can implement an ex parte order by installing and using its own software.<sup>31</sup>
- Although some sections of the USA PATRIOT Act have a sunset provision and expire in 2005,<sup>32</sup> section 216 does not and will continue to be the law.

¶8 What section 216 did, from the librarian’s perspective, is extend the reach of a pen register order, issued without any Fourth Amendment protections, to patron use at a library computer terminal. Now the government is capable of watching what patrons are reading online, while they are reading it. This is a major change. Because the USA PATRIOT Act was passed so quickly and with so little debate, there is no way to ascertain legislative intent. But even if the purpose of section 216 was only to allow more liberal access to e-mail header information while the e-mail was in transit, the result is much broader than that. Pen register orders apply to “processing and transmitting of wire or electronic communications. . . .”<sup>33</sup> These amendments allow the government to create and install its own software and track all noncontent information from a computer or computer network on a mere showing that the information is likely to be relevant to an ongoing investigation.

---

*After the USA PATRIOT Act: The Big Brother That Isn't*, 97 Nw. U. L. REV 607, 633–34 (2003) (arguing that federal judges had signed hundreds of pen register orders authorizing Internet e-mail and packet surveillance prior to the passage of the USA PATRIOT Act).

28. USA PATRIOT Act, Pub. L. No. 107-56, § 216(a), 115 Stat. 272, 288 (amending 18 U.S.C. § 3121(c) (2000)).
29. § 216(b)(1), 115 Stat. at 289 (amending 18 U.S.C. § 3123(a) (2000)).
30. *Id.* Any notice required by law to be given to the recipient of an order can be delayed “for a reasonable period,” pursuant to section 213. The period of delay can be extended “for good cause shown.” § 213, 115 Stat. at 285–86 (amending 18 U.S.C. § 3103a (2000)).
31. § 216(b)(1), 115 Stat. at 289 (amending 18 U.S.C. § 3123(a) (2000)). The software developed by the government was known as Carnivore, and is now known as DCS1000. *Nomination of Robert S. Mueller, III to be Director of the Federal Bureau of Investigation: Hearing Before the Senate Comm. on the Judiciary*, 107th Cong. 108 (2001) (statement of Robert S. Mueller).
32. Except for listed sections, including section 216, the amendments made by the USA PATRIOT Act “cease to have effect on December 31, 2005.” § 224(a), 115 Stat. at 295 (codified at 18 U.S.C. § 2510 nt. (Supp. 2001)). On May 21, 2004, Senator Jon Kyl introduced a bill to repeal section 224 of the USA PATRIOT Act. *See S. 2476*, 108th Cong. (2004).
33. § 216(a), 115 Stat. at 288 (amending 18 U.S.C. § 3121(c) (2000)).

¶9 The section 216 amendments are quite vague; the section merely inserts the words “routing, addressing” after “dialing,” and replaces “call processing” with “the processing and transmitting of wire or electronic communications so as not to include the contents of any wire or electronic communications.”<sup>34</sup> The statute does not address how this is to be accomplished and does not define content. By simply conflating e-mail headers and Web site addresses with telephone numbers, and conflating a particular technology for telephones with the full range of computer interception devices (including the FBI’s Carnivore program), the potential range of information retrievable has been exponentially increased.

¶10 So why is this different from what libraries could expect prior to the passage of the USA PATRIOT Act? Before the Act, the term *pen register* was expressly applied to “a device which records or decodes electronic or other impulses which identify the *numbers dialed* or otherwise transmitted on the telephone line to which such device is attached.”<sup>35</sup> There was no possibility that patron information about reading or other information seeking activity could be recovered from telephone numbers on a telephone in a library. After the passage of the USA PATRIOT Act, however, a pen register using a Carnivore-type of computer program attached to a library computer or computer network could easily recover patron information—such as Web sites visited, pages downloaded, online order forms accessed, and pictures viewed—otherwise formally protected by state statute,<sup>36</sup> state constitution,<sup>37</sup> or informally protected by the American Library Association’s Code of Ethics.<sup>38</sup> This type of information is content, and it now can be recovered without a showing of probable cause.<sup>39</sup>

¶11 Whether or not the government is actively monitoring Web sites visited by library patrons is not the critical issue, however. Rather, it is the potential for

34. *Id.*

35. 18 U.S.C. § 3127(3) (2000) (emphasis added). If federal magistrates were applying the statute to computer systems, despite the express “telephone line” language, it was not common knowledge. In any event, the passage of the USA PATRIOT Act ended any debate base on statutory interpretation. See Stephen A. Osher, *Privacy, Computers and the PATRIOT Act: The Fourth Amendment Isn’t Dead, but No One Will Insure It*, 54 FLA. L. REV. 521, 527 (2002).

36. Forty-eight states and the District of Columbia have express laws protecting the privacy of library records; the remaining two states (Kentucky and Hawai’i) have opinions from their attorneys general that library records are confidential. MARY MINOW & TOMAS A. LIPINSKY, *THE LIBRARY’S LEGAL ANSWER BOOK* 200–10 (2003).

37. Eleven state constitutions have privacy provisions. JENNIFER FRIESEN, *STATE CONSTITUTIONAL LAW: LITIGATING INDIVIDUAL RIGHTS, CLAIMS, AND DEFENSES* 2-95–2-96 (3d ed. 2000).

38. See AM. LIBRARY ASS’N, *CODE OF ETHICS* (1995), available at <http://www.ala.org/ala/oif/statementspols/codeofethics/codeofethics.pdf> (Principle 3 provides: “We protect each library user’s right to privacy and confidentiality with respect to information sought or received and resources consulted, borrowed, acquired or transmitted.”); AM. LIBRARY ASS’N, *POLICY ON CONFIDENTIALITY OF LIBRARY RECORDS* (1986), available at <http://www.ala.org/ala/oif/statementspols/otherpolicies/policyconfidentiality.pdf>.

39. The government has taken the position that it will try not to recover content, but it will retain content once recovered, and will use that content in case of a national emergency. See *infra* ¶¶ 18–23.

abuse that chills First Amendment rights. The holding in *Keyishian v. Board of Regents* that “(t)he threat of sanctions may deter almost as potently as the actual application of sanctions” to chill speech protected by the First Amendment,<sup>40</sup> applies equally to the library patron who does not ask for material on a book about Al Qaeda or on the construction of dams in the Western states for fear of investigation by the FBI.<sup>41</sup> The potential for abuse exists with pen registers. Even in the context of telephone lines, technological advances in the ability of pen registers to capture content have, in some jurisdictions, raised the constitutional bar on issuing pen register orders.<sup>42</sup> Where the pen register attached to a telephone line mechanically evolved so that it was possible, at the flip of a switch, to record content and not just telephone numbers, courts have held the government to a higher standard than the statutory standard that “the information likely to be obtained by such information and use is relevant to an ongoing criminal investigation.”<sup>43</sup> As noted in *People v. Bialostok*:

In light of . . . the potential for abuse embodied in the technology used here, we distinguish this more sophisticated technology from earlier pen registers. The traditional pen register considered in *Smith v. Maryland* was, to large extent, self-regulating. *Neither through police misconduct nor through inadvertence could it reveal to anyone any information in which the telephone user had a legitimate expectation of privacy. The same is not true of the device used here.* This is a technology that has the capacity, through willful use or otherwise, to intrude on legitimately held privacy, and it is the warrant requirement, interposing the Magistrate’s oversight, that provides to citizens appropriate protection against unlawful intrusion.<sup>44</sup>

¶12 The pen register as it exists post–September 11 is certainly not self-regulating. It is capable of being used improperly either by deliberate misconduct or by inadvertence. To understand the problem, a brief discussion of the difference between telephone numbers and computer numbers may be helpful.

---

40. 385 U.S. 589, 604 (1967) (involving a statutory plan allowing firing of teachers who advocated or taught the doctrine of forceful overthrow of the government).

41. These fears are not baseless. In the post-September 11 world, actions as innocent as criticizing President Bush during a conversation in a San Francisco gym warranted a visit by the FBI. Emil Guillermo, *The FBI’s House Calls*, S.F. GATE (Dec. 18, 2001), at <http://sfgate.com/cgi-bin/article.cgi?file=/gate/archive/2001/12/18/eguillermo.DTL>. And the ACLU recently filed suit on behalf of a number of community groups who allege that their members have curtailed their political speech, religious activities, or civic participation for fear of investigation by the FBI. *Muslim Community Ass’n v. Ashcroft*, No. 03-72913 (E.D. Mich. 2003), available at <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13248&c=206>.

42. See *People v. Bialostok*, 610 N.E.2d 374, 376–77 (N.Y. 1993). Later courts have looked on a case by case basis at the ease with which the technology can be altered to capture content. See, e.g., *People v. Kramer*, 706 N.E.2d 731, 737 (N.Y. 1998) (“*Bialostok* should be understood and applied as a more fact specific, adaptable legal guidepost for sophisticated modern technologies. It should require scrutiny and examination of the pen register technology as used in a given investigation and situation.”). “The pen register devices . . . had the capacity to intercept and record either digital or aural transmissions, depending on whether they were set for ‘audio off’ or ‘audio on.’ The switch from one mode to the other could be accomplished by a technician adjusting a switch. . . .” *Id.* at 733.

43. 18 U.S.C. §3123(a) (2000).

44. *Bialostok*, 610 N.E.2d at 376–78 (emphasis added).

### *Telephone Lines and Packet Technology*

¶13 There is a basic difference between telephones and computers. Computers use a technology known as packet switching, where data is broken down into small packets of information which are then “transmitted and reassembled in the correct order at the destination computer. The packets are encoded at the source for correct reassembly, permitting them to utilize the most efficient routing along the way.”<sup>45</sup> Telephone numbers can be collected at the source, without any difficulty in separating the noncontent or address information from the telephone call or the content. Because e-mail and Web site information is “transmitted in packets, whoever intercepts the message must separate the address from the contents of the e-mail. The FBI responds to invasion of privacy concerns by asserting that they can be trusted to separate address from content and retain only the former.”<sup>46</sup>

¶14 Web site addresses give substantially more information than a telephone number. Just knowing that someone accessed a certain page provides access to all of the content on that page. The FBI’s computer program, Carnivore, allegedly has the ability to capture Web addresses, including “specific pages visited, sites visited, or even items that have been purchased or browsed on the Internet.”<sup>47</sup> If library computers are the target of a pen register order utilizing Carnivore, then all the information accessed by everyone using the computer, not just the target, is accessible to FBI review.<sup>48</sup>

¶15 The FBI interprets what is content and what is not. In the case of computer information, the entire packet is decoded, and the noncontent information must be selected. FBI agents must contact the Department of Justice if they do not know what information is *noncontent* and what information is *content*.<sup>49</sup>

---

45. Osher, *supra* note 35, at 528 (citations omitted).

46. *Id.* (citations omitted).

47. “Carnivore” Controversy: *Electronic Surveillance and Privacy in the Digital Age: Hearing before the Senate Comm. on the Judiciary*, 106th Cong. 38 (2000) (statement of Michael O’Neill, associate professor, George Mason University School of Law). Information released after 2000 by the Department of Justice about Carnivore supports the finding that content is captured by the FBI’s programs; the FBI’s remedy is to try to configure the programs to collect only needed information and to refrain from using “accidentally” collected content. See Memorandum from Larry D. Thompson, Deputy Attorney General, U.S. Dep’t of Justice, to Assistant Attorney General, Criminal Division, et al., Avoiding Collection and Investigative Use of “Content” in the Operation of Pen Registers and Trap and Trace Devices 4 (May 24, 2002), available at <http://www.house.gov/judiciary/attachD.PDF>. However, to prevent immediate danger of death, serious physical injury or harm to the national security, the accidentally collected information may be used. *Id.* To avoid overcollection requires operator skill and operator trustworthiness.

48. See Gina Tufaro, Note, *Will Carnivore Devour the Fourth: An Exploration of the Constitutionality of the FBI Created Software*, 18 N.Y.L. SCH. J. HUM. RTS. 305, 310–11 (2002) (“When an officer receives a warrant for a wiretap, he has access to the suspects [sic] phone call conversations, and only that suspect’s. The ACLU points out that Carnivore, in contrast, is capable of reading millions of messages per second, not just those involving the criminal suspect. Although the FBI may hone in on a specified suspect, everyone on the ISP, theoretically, is an equal target.”).

49. “Agents and prosecutors with questions about whether a particular type of information constitutes content should contact the Office of Enforcement Operations in the telephone context (202-514-6809) or the Computer Crime and Intellectual Property Section in the computer context (202-514-1026).” Computer Crime & Intellectual Prop. Section, U.S. Dep’t of Justice, Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001, at <http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm> (last updated Nov. 5, 2001).

### Government Guidelines

¶16 In the guidelines established by the Department of Justice after the passage of the USA PATRIOT Act, agents are informed that information in the subject line of an e-mail is considered content, and that the pen register order does not authorize the interception of content. “Pen/trap orders cannot, however, authorize the interception of the content of a communication, such as words in the ‘subject line’ or the body of an e-mail.”<sup>50</sup> However, if the subject line is filled in, it will be intercepted as part of the packet. You can’t unring the bell.

¶17 The government’s own guidelines make it clear that while Carnivore may be intended to capture content, it does not always work and that there is no bright line on what content is. The Department of Justice’s guidelines directly address the subject of “content” in the context of e-mail headers, but not in the context of Web site addresses.<sup>51</sup> The Department of Justice has avoided discussing the collection of Web site addresses for the very good reason that there is no way to view the same page a person has been looking at and not see the content of the page. If you collect the Web address, you collect the content shown at that address as well.

¶18 When Viet H. Dinh, an assistant attorney general in the Justice Department was asked whether or not URLs were content or noncontent at a Senate Judiciary Committee hearing, he evaded a direct response by replying, “With respect to URLs, the deputy attorney general has issued a memorandum which has been provided to this committee on the use of post-cut-through intercepts in the analog world and also content information in the digital world.”<sup>52</sup> The document referred to would appear to be Deputy Attorney General Thompson’s Memorandum on “Avoiding Collection and Investigative Use of ‘Content’ in the Operation of Pen Registers and Trap and Trace Devices,” which merely requires agents to call a specified number if they have a question, leaving the final say on what is and what is not content entirely within the Department of Justice’s discretion.<sup>53</sup>

¶19 The Thompson memorandum on overcollection does call for the assistant attorney general to issue new guidelines,<sup>54</sup> and that appears to have happened. Post-USA PATRIOT Act guidelines for electronic surveillance in the *United States Attorneys’ Manual* provide that “use of pen registers to collect all or part of a URL is prohibited without prior consultation with CCIPS [Computer Crime and Intellectual Property Section of the Criminal Division of the U.S. Department of Justice].”<sup>55</sup>

---

50. *Id.*

51. Memorandum from Larry D. Thompson, *supra* note 47, at 4.

52. *Anti-Terrorism Investigations and the Fourth Amendment After September 11, 2001, Hearing Before the Subcomm. on the Constitution of the House Comm. on the Judiciary*, 108th Cong. 41 (2003) [hereinafter *Anti-Terrorism Investigations Hearing*] (testimony of Viet D. Dinh, Assistant Attorney General, U.S. Dep’t of Justice), available at <http://www.house.gov/judiciary/87238.PDF>.

53. Memorandum from Larry D. Thompson, *supra* note 47, at 5. The memorandum confirms that programs in place do capture content, which is supposed to be subject to the FBI’s retention and use policies for content information.

54. *Id.*

55. U.S. DEP’T OF JUSTICE, UNITED STATES ATTORNEYS’ MANUAL § 9-7.500 (2003), available at [http://www.usdoj.gov/usao/eousa/foia\\_reading\\_room/usam/title9/7mcrmm.htm#9-7.500](http://www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/7mcrmm.htm#9-7.500).

However, this “policy does not apply to applications for pen register orders that would merely authorize collection of Internet Protocol (IP) addresses, even if such IP addresses can be readily translatable into URLs or portions of URLs.”<sup>56</sup> The exception would seem to overwhelm the rule: you can expressly get Web pages if you ask, and you can indirectly get Web pages even if you don’t ask.

¶20 Content in the form of Web pages visited is easily recoverable with a pen register order issued only on a showing of relevance. Since content is precisely what the Fourth Amendment strives to protect, any attempt to intercept content must be governed by a higher standard than “likely to be relevant.”<sup>57</sup> Recognizing that it can only use “technology reasonably available to it,”<sup>58</sup> the Department of Justice’s policy means that the program can only seek to minimize any overcollection, and that if:

despite the use of “technology reasonably available to it,” an agency’s deployment of a pen register does result in the incidental overcollection of some portion of “content,” it is the policy of this Department that such “content” may not be used for any affirmative investigative purpose, except in a rare case in order to prevent an immediate danger of death, serious physical injury, or harm to the national security.<sup>59</sup>

¶21 Allowing the FBI authority to devise a program that inadvertently captures both noncontent and content, and then to retain the latter for use “in a national emergency” is allowing one agency too much discretion.<sup>60</sup> Even Republicans are showing signs of concern about the USA PATRIOT Act’s constitutional implications. Robert Barr of Georgia emphasized that the FBI contends that it has the authority to harvest large amounts of data and then to filter out the unwanted information. “Those are two very, very large steps that we are taking here . . . I don’t think that this has been well thought out.”<sup>61</sup>

### *FISA Pen Registers*

¶22 Section 216 was not the only section of the USA PATRIOT Act that addressed pen registers. Section 214 of the USA PATRIOT Act amends the FISA provisions regarding pen register and trap and trace devices. All the government has to cer-

56. *Id.*

57. See Chris Katopis, “Searching” Cyberspace: The Fourth Amendment and Electronic Mail, 14 TEMP. ENVTL. L. & TECH. J. 175, 198–99 (noting that heightened scrutiny is necessary where content is being recovered).

58. Memorandum from Larry D. Thompson, *supra* note 47, at 3 (citing 18 U.S.C. § 3121(c), as amended by the USA PATRIOT Act, § 216(a), 115 Stat. 272, 288).

59. *Id.* at 4.

60. See Jerry Berman & James X. Dempsey, *CDT’s Guide to the FBI Guidelines: Impact on Civil Liberties and Security—The Need for Congressional Oversight* (June 26, 2003), at <http://www.cdt.org/wiretap/020626guidelines.shtml>.

61. Tufaro, *supra* note 48, at 315 (quoting Barr) (citation omitted); see also Dan Eggen & Jim VandeHei, *Ashcroft Taking Fire from GOP Stalwarts; More Wish to Curb Anti-Terror Powers*, WASH. POST, Aug. 29, 2003, at A1; *LCHR Rebuts Attorney General’s Speech on USA PATRIOT Act*, Lawyer’s Committee on Human Rights, at [http://www.lchr.org/media/2003\\_alerts/0825.htm](http://www.lchr.org/media/2003_alerts/0825.htm) (Aug. 25, 2003) (reporting negative comments of Republican senators and representatives on both the USA PATRIOT Act and the FBI’s desire for new powers).

tify is that the information likely to be obtained through use of the device is “foreign intelligence information not concerning a United States person<sup>62</sup> or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.”<sup>63</sup>

¶23 Section 214 would apparently only be required if there were no criminal investigative component to the FBI’s request, as a section 216 order would cover any investigation of a person, suspected of a crime or not, where it might be relevant to a criminal investigation. Since most terrorist activities have a criminal component,<sup>64</sup> section 216 would appear to cover the majority of investigations, without even invoking the jurisdiction of the FISA court or its cold protection that “United States persons” cannot be the subject of a section 214 pen register order if the entirety of their activities were protected by the First Amendment.<sup>65</sup>

¶24 Section 216 appears to be the primary focus of the Department of Justice and its congressional interrogators. In recent House Judiciary hearings, the focus of the entire inquiry was section 216.<sup>66</sup> Nevertheless, FISA courts also have authority to issue pen register orders.

### *Roving Wiretaps*

¶25 The USA PATRIOT Act changed the requirements for wiretap orders for real-time interception of the content of electronic communications. Section 218 amended the standard to be met in issuing a FISA wiretap order from “the purpose” of the order is to gather foreign intelligence to “a significant purpose” of the order is to gather foreign intelligence.<sup>67</sup> The scope of *significant purpose* was the subject of a FISA Court of Review case.<sup>68</sup> While the Court of Review did not accept the government’s argument that it could use a FISA wiretap warrant if the primary purpose of the investigation was prosecuting an agent for a nonforeign intelligence crime, it did approve authorizing a warrant where the government

---

62. The Foreign Intelligence Surveillance Act defines a “United States person as . . . a citizen of the United States, an alien lawfully admitted for permanent residence. . . , an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power. . . .” 50 U.S.C. § 1801(i) (2000).

63. USA PATRIOT Act, Pub. L. No. 107-56, § 214(a)(1), 115 Stat. 272, 286 (amending 50 U.S.C. § 1842(a)(1) (2000)).

64. *Anti-Terrorism Investigations Hearing*, *supra* note 52, at 9, available at <http://www.house.gov/judiciary/87238.PDF>; see also *In re Sealed Case*, 310 F.3d 717, 736–39 (Foreign Int. Surv. Ct. Rev. 2002).

65. See *supra* note 63 and accompanying text.

66. *Anti-Terrorism Investigations Hearing*, *supra* note 52. It would not appear to be that difficult, even without the avenue provided by section 216, to argue that an activity had a component besides protected First Amendment activities; section 216 obviates the need for any such rationalization.

67. § 218, 115 Stat. at 291 (amending 50 U.S.C. § 1823(a)(7)(B), 50 U.S.C. § 1804(a)(7)(B) (2000)).

68. *In re Sealed Case*, 310 F.3d 717. This is the first and only published decision of the FISA Court of Review.

asserted any measurable foreign intelligence purpose.<sup>69</sup> This leaves a lot of scope for investigating ordinary crime,<sup>70</sup> and the Department of Justice has interpreted this section to mean that FISA wiretaps can be used primarily for criminal investigation purposes.<sup>71</sup>

¶26 Section 206 made the scope of FISA warrants nationwide and anonymous; a roving wiretap order under section 206 does not need to identify the third party who has to provide assistance “to accomplish the surveillance.”<sup>72</sup> A FISA order is directed at content and every page viewed by a patron at a library computer terminal as well as the content of any e-mails would be recovered by the wiretap. The wiretap will intercept the computer usage of every patron at the terminal and no one will know since the recipient of the order cannot disclose the existence of the order or the content of a communication.<sup>73</sup>

¶27 The library community should be concerned about the ease with which these orders can be issued. The knowledge that there is a court that is required to rubber stamp<sup>74</sup> government requests to access real-time content in library computers for crimes only tangentially related to terrorism will have a chilling effect on First Amendment rights. As Erwin Chemerinsky pointed out, “[t]he experience with other broad statutes is that they are often used in contexts far beyond what the drafters intended.”<sup>75</sup> The USA PATRIOT Act has already been used for purposes unrelated to terrorism, such as drug, fraud, and bank theft cases.<sup>76</sup> And Senator Patrick Leahy is also concerned that the Department of Justice is using the Act in cases that do not involve terrorism, then reporting the results as successes against the war on terrorism.<sup>77</sup>

---

69. *Id.* at 736–39.

70. “The Court of Review’s decision leaves the proverbial fox guarding the henhouse.” While the court must determine if a significant purpose of the investigation is to collect foreign intelligence information before it issues an order, the court is required to grant the application if the government certifies that it has any measurable foreign intelligence purpose for the investigation. John E. Branch III, *Statutory Misinterpretation: The Foreign Intelligence Court of Review’s Interpretation of the “Significant Purpose” Requirement of the Foreign Intelligence Surveillance Act*, 81 N.C. L. REV. 2075, 2077 (2003).

71. *The USA PATRIOT Act in Practice: Shedding Light on the FISA Process: Hearing Before the Senate Comm. on the Judiciary*, 107th Cong. 20 (2002) (statement of Professor William C. Banks, Professor of Law, Syracuse University, Syracuse, New York), available at <http://www.access.gpo.gov/congress/senate/senate14ch107.html>.

72. § 206, 115 Stat. at 282 (amending 50 U.S.C. § 1805(c)(2)(B) (2000)).

73. Electronic Privacy Info. Ctr., *Analysis of Provisions of the Proposed Anti-Terrorism Act of 2001 Affecting the Privacy of Communications and Personal Information* 6 (Sept. 24, 2001), available at [http://www.epic.org/privacy/terrorism/ATA\\_analysis.pdf](http://www.epic.org/privacy/terrorism/ATA_analysis.pdf).

74. FISA judges have no discretion; once the government makes the necessary certifications, the warrant must issue. 50 U.S.C. § 1805(a) (2000).

75. Chemerinsky, *supra* note 13, at 30. Chemerinsky was referring to Title III warrants, but the observation applies to any broadly drafted statute.

76. Dan Eggen, *PATRIOT Act Not Just Used Against Terror, Report Says; The Powers Granted in the USA PATRIOT Act Were Used in Drug, Fraud, and Bank-Theft Cases, a Report to Congress Shows*, GRAND RAPIDS PRESS, May 21, 2003, at A1.

77. See *Protecting Our National Security from Terrorist Attacks: A Review of Criminal Terrorism Investigations and Prosecutions, Hearing before the Senate Comm. on the Judiciary*, 108th Cong. (Oct. 21, 2003) (Statement of Senator Patrick Leahy) (“I am concerned that the Department of Justice

### *Turning Over Tangible Records—Sections 215 and 505*

¶28 Library patrons come and go, and unless the government knows who was sitting at the computer at a certain time, the Web sites visited can't be connected to a certain person. This is where sections 215 and 505 come in. They give new teeth to the ability of the government to view Web site activity at library computer terminals with a pen register order. Section 215 is arguably the section of the USA PATRIOT Act that has drawn the most outcry from librarians; it expanded the range of businesses that could be the subject of a FISA order "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities."<sup>78</sup> Prior to the passage of the USA PATRIOT Act, only the records of common carriers, public accommodation facilities, physical storage facilities, or vehicle rental facilities were subject to an order to turn over tangible items.<sup>79</sup>

¶29 Section 215 expands that authority to cover any business or entity, which would of course include libraries. The business can be required to turn over tangible items "including books, records, papers, documents, and other items."<sup>80</sup> The government only has to state that the records contain foreign intelligence information "not concerning a U.S. citizen or permanent resident" *or* that the records "are needed to protect against international terrorism or clandestine intelligence activities."<sup>81</sup> If the application contains such a statement, the FISA court must issue the warrant.<sup>82</sup> The section also provides that "[n]o person shall disclose to any other person (other than those persons necessary to produce the . . . things) that the Federal Bureau of Investigation has sought or obtained tangible things under this section."<sup>83</sup>

¶30 Although section 215 might appear circumscribed by its terms, the section provides that the government conduct section 215 investigations "under guidelines approved by the Attorney General under Executive Order 12333."<sup>84</sup> This has potentially serious consequences for privacy, because the order requires the attorney general to set guidelines for surveillance, but the procedures, once established, are not subject to review.

The Order allows the Attorney General to authorize "any technique for which a warrant would (ordinarily) be required . . . (upon a unilateral judgment) that the technique is

---

may be exaggerating its success in fighting terrorism, by classifying cases as 'terrorism' related even when they have little or nothing to do with terrorism."), available at [http://judiciary.senate.gov/member\\_statement.cfm?id=965&wit\\_id=2629](http://judiciary.senate.gov/member_statement.cfm?id=965&wit_id=2629).

78. § 215, 115 Stat. at 287 (amending 50 U.S.C. § 1861(a)(1) (2000)).

79. 50 U.S.C. § 1862 (2000).

80. § 215, 115 Stat. at 287 (amending 50 U.S.C. § 1861(a)(1) (2000)).

81. *Id.*

82. *Id.*

83. *Id.*, 115 Stat. at 288 (amending 50 U.S.C. § 1861(d)).

84. *Id.*, 115 Stat. at 287 (amending 50 U.S.C. § 1861(a)(2)(A)). The FBI has used executive orders in the past as ostensible authority, augmented by Director J. Edgar Hoover's order, to monitor dissidents on the right and the left. See Athan G. Theoharis, *Dissent and the State: Unleashing the FBI, 1917–1985*, 24 HIST. TCHR. 41, 43 (1990).

directed against a foreign power or an agent of a foreign power.” The lack of a definition for the term “agent of a foreign power” means that the characterization of the target falls exclusively within the discretion of the Attorney General as well.

While the FBI must apply for an order to the special FISA court, the court will grant the order on less than probable cause. The government need only certify that it seeks the records for an authorized investigation conducted pursuant to the Attorney General’s procedures, and that the investigation intends to obtain foreign intelligence information, a very broadly defined term. Since the Attorney General has the sole discretion to define the parameters of the investigation, the government obtains access to a broad range of private records in potential violation of the individual’s privacy.<sup>85</sup>

Section 215 does prohibit a warrant where the investigation is “conducted solely upon the basis of activities protected by the first amendment to the Constitution.”<sup>86</sup> This may be cold comfort, as FISA court orders are rarely reviewed.<sup>87</sup> FISA establishes a secret court that does not have to make its proceedings public.<sup>88</sup>

¶31 There is another provision of the USA PATRIOT Act that could require a library to turn over records of computer use to the government. Section 505 expanded the ability of the FBI to administratively—without court review—issue national security letters.<sup>89</sup> A national security letter may now be used to obtain information from a library<sup>90</sup> by certifying that “the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.”<sup>91</sup> This section has the same limited protection for First Amendment activities as Section 215.<sup>92</sup> National security letters have always had a gag order provision.<sup>93</sup>

### Library Records and Government Efforts to Secure Them

¶32 Armed with a FISA section 215 order, the government can request library records, including records of computer use. National security letters can also be used to secure records of computer use. This raises several interesting issues for

85. Patricia Mell, *Big Brother at the Door: Balancing National Security with Privacy Under the USA PATRIOT Act*, 80 DENV. U. L. REV. 375, 418 (2002) (citations and footnotes omitted).

86. § 215, 115 Stat. at 287 (amending 50 U.S.C. § 1861(a)(1)).

87. Although FISA was enacted in 1978, this happened for the first time in *In re All Matters Submitted to Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611 (Foreign Int. Surv. Ct. 2002), reviewed by *In re Sealed Case*, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002).

88. See 50 U.S.C. §§ 1803, 1822(c) (2000).

89. § 505(a), 115 Stat. at 365 (amending 18 U.S.C. § 2709(b) (2000)).

90. Libraries providing Internet access come within the statutory definition of an “electronic communication service” required to comply with a national security letter under § 2709(b): “‘electronic communication service’ means any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15) (2000).

91. § 505(a)(3)(B), 115 Stat. at 365 (amending 18 U.S.C. § 2709(b)(2) (2000)).

92. See *supra* note 86 and accompanying text.

93. 18 U.S.C. ¶ 2709(c) (2000) (“No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.”). A bill has just been introduced in Congress to criminalize the violation of a national security letter gag order; the proposed penalty is from one to five years in prison. H.R. 3179, 108th Cong. (2004).

libraries. Pikowsky has suggested that, because librarians do not as a rule keep records of patron name, identification, and times of use, the information accessed on a library computer is actually more private than information accessed on a home computer, and that perhaps such a situation is not appropriate.<sup>94</sup> The government could not agree more. Although the USA PATRIOT Act does not require librarians to keep records of computer use, there has been some criticism of librarians who quickly shred records or refuse to keep them.<sup>95</sup>

¶33 One important use of law libraries is to provide access to government documents, both in print and online formats. Many law libraries are members of the Federal Depository Library Program (FDLP), which provides government documents to the libraries for free in exchange for, *inter alia*, the member library's agreement to allow access to the materials according to FDLP guidelines. In law libraries, computers are routinely used by public patrons to access government documents. Libraries that are otherwise private or semiprivate provide this access as part of the FDLP Program. The FDLP Internet Use Policy Guidelines formerly stated that "patrons cannot be required to present identification."<sup>96</sup> The prohibition against requiring identification was removed when the guidelines were revised in 2003; the new rules enable librarians to keep records.<sup>97</sup>

¶34 Shortly after September 11, 2001, the University of Illinois sent libraries a survey on responses to the event. According to the survey, 4.1% of all libraries responding reported that the FBI or police had already requested information about their patrons.<sup>98</sup> In a University of Illinois study seeking information for the year after September 11, 2001, 10.7% of responding libraries reported that the FBI or police had requested information about their patrons.<sup>99</sup> Until September 2003,

94. Pikowsky, *supra* note 6, at 619–20, ¶¶ 67–70.

95. "If I'm a terrorist and I need to use a computer system to e-mail my buddies, guess where I'm going to go. I'm going to go right to the libraries that have refused to keep any kind of records of who is using the computers." *NewsHour: Libraries and Liberties* (PBS television broadcast, June 18, 2003) (remarks of Victoria Toensing, former Justice Department attorney who established the Justice Department's Terrorism Unit) (transcript available at [http://www.pbs.org/newshour/bb/law/jan-june03/library\\_6-18.html](http://www.pbs.org/newshour/bb/law/jan-june03/library_6-18.html)). This is also Pikowsky's point. Libraries that do not keep records, however, are the only ones where patrons can access information on the Internet free of the fear that their reading habits are being monitored; it is freedom from that fear that the First Amendment protects. See *United States v. Rumely*, 345 U.S. 41, 57–58 (1953) (Douglas, J., concurring).

96. See FDLP Internet Use Policy Guidelines (effective Jan. 15, 1999), at [http://web.archive.org/web/20021019160935/http://www.access.gpo.gov/su\\_docs/fdlp/mgt/iupolicy.html](http://web.archive.org/web/20021019160935/http://www.access.gpo.gov/su_docs/fdlp/mgt/iupolicy.html). The old guidelines did allow time limits and the use of sign-up sheets.

97. See FDLP Internet Use Policy Guidelines (rev. March 2003), at [http://www.access.gpo.gov/su\\_docs/fdlp/mgt/iupolicy.html](http://www.access.gpo.gov/su_docs/fdlp/mgt/iupolicy.html).

98. Library Research Ctr., Univ. of Ill. at Urbana-Champaign, Public Libraries' Responses to September 11, 2001, at 6 (survey results, 1028 libraries responding), available at <http://alexia.lis.uiuc.edu/gslis/research/national.pdf> (last visited June 3, 2004).

99. Library Research Ctr., Univ. of Ill. at Urbana-Champaign, Public Libraries' Response to the Events of 9/11/2001: One Year Later [2] (survey results, 906 libraries responding), available at <http://alexia.lis.uiuc.edu/gslis/research/finalresults.pdf> (last visited May 20, 2004); see also LEIGH ESTABROOK, PUBLIC LIBRARIES AND CIVIL LIBERTIES: A PROFESSION DIVIDED, at [http://alexia.lis.uiuc.edu/gslis/research/civil\\_liberties.html](http://alexia.lis.uiuc.edu/gslis/research/civil_liberties.html) (last updated Jan. 22, 2003) [hereinafter CIVIL LIBERTIES SURVEY II].

Attorney General John Ashcroft had adamantly maintained that the number of libraries served with section 215 orders was classified information and could not be revealed.<sup>100</sup> Apparently provoked by librarians' attacks on section 215, Mr. Ashcroft recently declassified the information on library visits and revealed that the number of times section 215 had been used was zero.<sup>101</sup> David Cole, a Georgetown law professor, said that "although the government did not appear to have seized any records under the Patriot Act, the law had had a 'substantial chilling effect.'"<sup>102</sup>

¶35 Attorney General Ashcroft's announcement that section 215 had been used "zero" times may not be correct. At least one librarian responding to the University of Illinois follow-up survey stated the library had received a court order referencing section 215 or 50 U.S.C. § 1862, and at least two librarians reported that they had received court orders prohibiting them from telling patrons that authorities requested information.<sup>103</sup> Two librarians indicated that they did not answer some of the questions about service of an order because they believed they were legally prohibited from doing so.<sup>104</sup> The survey effort is being continued in Illinois. Two academic and twelve public libraries recently reported that they did not answer questions on the survey "because they believe the provisions of the USA PATRIOT Act prohibit them [from doing so]."<sup>105</sup>

¶36 Many libraries have changed their record-keeping habits since September 11, 2001. According to the second Illinois survey, 40.5% of the 906 responding libraries reported that they have started to require identification of patrons to use the Internet and that this is a policy change since September 11; 56.8% have started keeping a sign-up sheet for users of the computer terminals.<sup>106</sup> After the passage of the USA PATRIOT Act, the Department of Justice released information

---

100. Eric Lichtblau, *Government Says It Has Yet to Use New Power to Check Library Records*, N.Y. TIMES (San Francisco ed.), Sept. 19, 2003, at A16.

101. *Quoted in id.*

102. *Quoted in id.* "There's real concern about the scope of the government's unchecked powers," [Mr. Cole] said. "And it's the things the government is doing that we can see that has us worried about what we can't see."

103. CIVIL LIBERTIES SURVEY II, *supra* note 99. Leigh Estabrook, who conducted the survey, stated: "We recognize that many requests for information about users have nothing to do with national security. We also recognize that the current environment creates a chilling effect that can make librarians justifiably hesitant to answer questions about whether they have received requests under the USA PATRIOT Act. The percent and numbers of libraries receiving court orders to provide information about users is small, but our data show that it is not zero." E-mail from Leigh Estabrook, Professor and Director of the Library Research Center, University of Illinois at Champaign-Urbana, to Susan Nevelow Mart, Reference Librarian, UC Hastings College of the Law (Sept. 25, 2003) (on file with the author).

104. CIVIL LIBERTIES SURVEY II, *supra* note 99.

105. Library Research Ctr., Univ. of Ill. at Urbana-Champaign, *The PATRIOT ACT and Illinois Libraries: A Report for the Illinois State Library* (2003) (discussing results of survey in which 587 libraries responded), available at <http://lrc.lis.uiuc.edu/web/PA.html>.

106. CIVIL LIBERTIES SURVEY II, *supra* note 99. It is not clear from the responses how much information about each patron is required on the sign-up sheets. And 32.5% of the responding libraries have stopped keeping a sign-up sheet for computer terminal users since September 11.

on unclassified library visits, stating that agents had visited about fifty libraries in the course of investigations (not specifically terrorism investigations).<sup>107</sup> Librarians believe the number is much higher.<sup>108</sup>

¶37 The attorney general's office was so concerned about the attacks mounted by groups like the American Library Association and the American Civil Liberties Union (ACLU) that it started a publicity campaign, which the ACLU later characterized as "disinformation."<sup>109</sup> The ACLU did so after reviewing newspaper quotes from Justice Department officials in which they incorrectly stated that the government needs a search warrant and probable cause to review library records or that the Act only applies to terrorists.<sup>110</sup> Unfortunately, the FBI's past is replete with examples of abuses of investigatory authority.<sup>111</sup> The FBI has

investigated people because of their ethnic or racial background, or because of their political viewpoint. For example, during the late 1960s and early 1970s, it conducted the COINTELPRO investigation, an effort to spy upon and disrupt the anti-Vietnam War and pro-civil rights movements. During the 1980s, the FBI launched a 27-month "intelligence" investigation of the Committee In Solidarity With the People of El Salvador (CISPES) because its members opposed U.S. policy of aiding repressive regimes in Central America. . . . The new intelligence surveillance authorities authorized by the USA PATRIOT Act may well trigger the same kinds of conduct.<sup>112</sup>

¶38 There have been previous attempts to monitor the reading habits of the American public. In the 1980s, the public found out that the FBI had a program called the Library Awareness Program.<sup>113</sup> The FBI went into libraries and requested help from librarians to monitor suspicious behavior in the library, particularly the behavior of foreign nationals, and then report their observations to the

107. *Anti-Terrorism Investigations Hearing*, *supra* note 52, at 39 (testimony of Viet D. Dinh, Assistant Attorney General, U.S. Dep't of Justice, stating that number of section 215 visits to libraries was classified, but that "libraries had been contacted approximately 50 times, based on articulable suspicion or calls—voluntary calls from librarians regarding suspicious activity"), *available at* <http://www.house.gov/judiciary/87238.PDF>.

108. CIVIL LIBERTIES SURVEY II, *supra* note 99.; Eric Lichtblau, *Surveillance, Secret Warrants Used In Terror Investigations: Justice Department Portrays Use of Patriot Act As Restrained*, SAN DIEGO UNION TRIB., May 21, 2003, at A1 ("Librarians, concerned about the government's ability to pry into the public's reading habits, have said they believe libraries have been contacted much more frequently."), *available at* 2003 WL 6586202.

109. ANN BEESON & JAMEEL JAFFER, AM. CIVIL LIBERTIES UNION, UNPATRIOTIC ACTS: THE FBI'S POWER TO RIFLE THROUGH YOUR RECORDS AND PERSONAL BELONGINGS WITHOUT TELLING YOU 15 (2003), *available at* <http://www.aclu.org/Files/OpenFile.cfm?id=13245>.

110. *Id.* at 15–17. *Unpatriotic Acts* refers to the Department of Justice's own documents, which state that relevance, not probable cause, is the standard for obtaining documents for a section 215 order issued by the FISA court. In addition, many of the provisions of the USA PATRIOT Act apply to crimes other than terrorism.

111. The abuse goes back to the beginning of the FBI's history. Between 1917 and 1921, with World War I as the precipitating excuse, the FBI targeted a host of radical and liberal activists and officials, from union leaders to liberal senators and judges, to critics of the FBI. Theoharis, *supra* note 84, at 52.

112. Am. Civil Liberties Union, *How the USA PATRIOT Act Enables Law Enforcement to Use Intelligence Authorities to Circumvent the Privacy Provisions Afforded in Criminal Cases* (Oct. 23, 2001), *at* <http://archive.aclu.org/congress/1102301i.html>.

113. FOERSTEL, *supra* note 10, at 2.

FBI.<sup>114</sup> The FBI was trying to prevent foreigners from getting access to *unclassified* information available to the general public. This is not unlike the administration's current removal of material from the Internet and requests to recall information from FDLP libraries.<sup>115</sup>

¶39 In the 1980s, librarians resisted. At that time, Senator Paul Sarbanes stated: "I don't think this sort of thing should occur without a court order. . . . It should never be a fishing expedition."<sup>116</sup> The FBI practice at that time was to approach staff members at a public desk; many felt intimidated and made to believe that their refusal to comply would be a sign of disloyalty or lack of patriotism.<sup>117</sup> This is a familiar refrain today. Furthermore, despite claims to the contrary, the FBI had in fact gone on fishing expeditions and asked for lists of books borrowed by foreign nationals.<sup>118</sup>

¶40 In 1988, in the wake of the hearings on the nomination of Judge Robert Bork and the release of his video rental records, Senator Robert W. Kastenmeier introduced the Video and Library Privacy Protection Act.<sup>119</sup> The FBI was opposed to protection of library records in the bill, which required getting a court order based on clear and convincing evidence that the subject was engaging in criminal activity, a finding that the evidence was highly probative, granting the subject time to appear and contest the court order, and precluding unlawfully obtained material from being used in a court proceeding.<sup>120</sup> The FBI tried to introduce a national security letter exemption; the ensuing political battle between the library privacy protection proponents and the FBI resulted in the deletion of the library portion of the bill's protection.<sup>121</sup>

¶41 The FBI's interest in libraries was addressed in Attorney General John Ashcroft's new surveillance guidelines, which freed the FBI to monitor Internet sites, libraries, churches, and political organizations. Ashcroft had characterized restrictions on domestic surveillance as "a competitive advantage for terrorists who skillfully utilize sophisticated techniques and modern computer systems to compile information for targeting and attacking innocent Americans"<sup>122</sup>

¶42 It is not just the fact of abuse, but the potential for abuse that is so troubling about the powers that the government has been given. The FBI's history of creating

114. *Id.*

115. See generally ACCESS TO GOVERNMENT INFORMATION POST SEPTEMBER 11TH, at <http://www.ombwatch.org/article/articleview/213/1/104/> (page last updated on May 3, 2002).

116. Quoted in FOERSTEL, *supra* note 10, at 12.

117. *FBI Counterintelligence Visits to Libraries, Hearings Before the Subcomm. on Civil And Constitutional Rights of the House Comm. on the Judiciary*, 100th Cong. 4 (1988) [hereinafter *FBI Counterintelligence Hearings*] (statement of Duane Webster, Executive Director, Association of Research Libraries).

118. *Id.* at 23 (testimony of James C. Schmidt, Executive Vice President, Research Libraries Group).

119. FOERSTEL, *supra* note 10, at 125.

120. *Id.* at 127 (referring to a Counterintelligence Division's secret internal memorandum).

121. *Id.* at 125–33. Ironically, today video rental records have more privacy protection than library records.

122. Quoted in Brad Knickerbocker, "Fishing Expeditions"—or Security Linchpin? *CHRISTIAN SCI. MONITOR*, June 6, 2002, at 3.

personal files on people, by means both legal and illegal, is well known.<sup>123</sup> Senator Patrick Leahy told National Geographic Television that “[t]he ability of the FBI to learn more about you than you probably even know about yourself can be very, very frightening.”<sup>124</sup> When FBI files on prominent Republicans were about to be released to the Clinton administration, allegedly as part of a review of more than four hundred former White House pass-holders, John P. Sears, who was Ronald Reagan’s campaign manager in 1976 and 1980, called for Congress “to force the FBI to destroy all of its files that don’t pertain to ongoing criminal investigations. Criminal and political blackmail are not proper enterprises for presidents or the FBI.”<sup>125</sup> Sears questioned the sincerity and credibility of the FBI’s promise that it no longer indulged in the excesses of the 1960s and 1970s, when “a sordid picture of attempts to discredit civil rights leaders and anti-Vietnam War demonstrators, of burglary to secure privileged information on individuals, of wire-taps under the guise of ‘national security’ and of a general pattern of violating the constitutional rights of American citizens” were discovered.<sup>126</sup> This history cannot be ignored.

¶43 Although the government has downplayed its substantial efforts to obtain records from libraries, and has insisted that they are necessary to fulfill the mandate to win the war on terrorism, library records are not normally the stuff of thrillers, where time is so critical and the evidence is so vital that the moments lost in securing a court order based on probable cause will be determinative of the outcome of a case. In fact, in a recent recounting of FBI successes, Assistant Attorney General Christopher A. Wray testified that:

[H]istorically, terrorists and spies have used libraries to plan and carry out activities that threaten our national security. For example, Brian Patrick Regan, who was convicted last February of offering to sell U.S. intelligence information to Iraq and China, used a computer at a local public library to look up addresses for Iraqi and Libyan embassies overseas. Similarly, in a recent domestic terrorism criminal case, a grand jury served a subpoena on a bookseller to obtain records showing that a suspect had bought a book giving instructions on how to build a particularly unusual detonator that had been used in several bombings. This was important evidence identifying the suspect as the bomber.<sup>127</sup>

¶44 This testimony raises several issues. Brian Patrick Regan’s use of a library computer to look up embassy addresses must have been only a very small

---

123. See Brian Handwerk, *National Geographic Goes Inside the FBI*, at [http://news.nationalgeographic.com/news/2003/07/0723\\_030723\\_fbi.html](http://news.nationalgeographic.com/news/2003/07/0723_030723_fbi.html) (July 23, 2003) (“[FBI Director J. Edgar] Hoover created secret files on many Americans, which were meant to intimidate his enemies and silence his critics.”).

124. *Id.*

125. John P. Sears, *The FBI Should Not Keep Personal Files*, ST. LOUIS POST-DISPATCH, June 20 1996, at 7B.

126. *Id.*

127. See *Protecting Our National Security from Terrorist Attacks: A Review of Criminal Terrorism Investigations and Prosecutions*, *supra* note 77 (Statement of Christopher A. Wray, Assistant Attorney General, Chief of Criminal Division, U.S. Dep’t of Justice), available at [http://www.senate.gov/~judiciary/testimony.cfm?id=965&wit\\_id=2740](http://www.senate.gov/~judiciary/testimony.cfm?id=965&wit_id=2740).

piece of the evidence of his crime. The FBI knew that Regan used a library computer and knew what he looked up on the computer, so it was able to secure the information without, according to Attorney General Ashcroft, using a section 215 order.<sup>128</sup> In the “recent domestic terrorism criminal case” mentioned by Christopher Wray, the government was able to secure a subpoena to get the bookstore records. It did not, in that case, need to resort to a section 215 FISA order, with its lower standards.

¶45 Library records of what a patron has read or viewed do not, without more, prove anything; you cannot infer that the book was read, the information was completely viewed, or that the person agreed or disagreed with the material. But the FBI has always fought for the right to fish for information.<sup>129</sup> The agency has fished for information before,<sup>130</sup> and, because of the technology involved, cannot avoid both overcollection of information and collecting information on innocent computer users.

¶46 Even in the recent past, the Department of Justice has demonstrated its willingness to make inaccurate statements to achieve its aims. In *In re All Matters Submitted to Foreign Intelligence Surveillance Court*, the FISA court made a factual finding regarding misstatements of fact in government applications which remains undisturbed: the FBI made over seventy-five misstatements or omissions of material fact related to major terrorist attacks and has never satisfactorily explained how the errors occurred.<sup>131</sup>

¶47 In another instance, involving a federal computer crime investigation, the FBI admitted making false statements to obtain warrants which it then used to seize all of a company’s business and private communications generated on the company’s electronic bulletin board.<sup>132</sup> Although the search was supposed to be directed at one employee, the entire company’s records were seized.<sup>133</sup>

¶48 Library patrons are worried about the government looking over their shoulder while they read and surf the Internet. Because of the broad provisions of the USA PATRIOT Act, the lack of judicial and legislative oversight, and the possibilities of content overcollection and overaggressive applications for pen register and section 215 orders or national security letters, these fears cannot be dismissed. And it is fear that is the problem.

---

128. See *supra* note 101 and accompanying text.

129. See *supra* note 116 and accompanying text.

130. *Id.*; see also *Fourth Amendment Issues Raised by the FBI’s “Carnivore” Program*, Hearing of the Subcomm. on the Constitution of the House Comm. on the Judiciary, 107th Cong. 47–48 (2000) (testimony of Barry Steinhardt, Associate Director, ACLU, discussing the FBI’s recent history with the Communications Assistance to Law Enforcement Act in which the FBI promised not to use the new law to turn cellular phones into location tracking devices, but within a year its policy was to use cellular phones as tracking devices), available at <http://www.house.gov/judiciary/stei0724.htm>.

131. 218 F. Supp. 2d 611, 620–21 (Foreign Int. Surv. Ct. 2002).

132. Katopis, *supra* note 57, at 186–87.

133. *Id.*

### **Congressional Revolt**

¶49 The USA PATRIOT Act limits both congressional and judicial oversight of surveillance, altering the normal checks and balances between the executive, judicial, and legislative branches. Attempts to redress this imbalance are in the works. As of this writing, seven pieces of legislation have been introduced in either the House or the Senate that address the USA PATRIOT Act:

- the Freedom to Read Protection Act<sup>134</sup> and its companion bill, the Libraries, Booksellers and Personal Records Protection Act,<sup>135</sup> would withdraw library and bookseller records from the effects of section 215;
- the Benjamin Franklin True Patriot Act<sup>136</sup> will sunset many USA PATRIOT Act provisions within ninety days of passage unless during the ninety-day period congressional hearings conclude that one or more sections should not be subject to the sunset provision;
- the Surveillance Oversight and Disclosure Act of 2003<sup>137</sup> would add reporting requirements and improve congressional oversight of certain USA PATRIOT Act provisions;
- the Reasonable Notice and Search Act<sup>138</sup> would alter the delayed notice provisions of the “sneak and peak” warrants authorized by section 213 and require the authority to issue the warrants to sunset;
- the Security and Freedom Ensured (SAFE) Act<sup>139</sup> would address perceived constitutional defects in the roving wiretap and record subpoena authority created by the USA PATRIOT Act; and
- the SAFE’s companion act in the House, the Security and Freedom Ensured (SAFE) Act,<sup>140</sup> mirroring SAFE and further limiting the definition of domestic terrorism in the USA PATRIOT Act to “acts dangerous to human life,” clearly excluding political protests. The current definition is so broad it could include political protest.

¶50 All of these efforts are directed at either restoring the checks and balances between the judicial, legislative, and executive branches of government that were impaired by the USA PATRIOT Act, restoring civil liberties guaranteed by the Constitution that were eroded by the USA PATRIOT Act, or both. However, not one of these bill has yet made it out of committee, so to date the revolt has been more a matter of form than substance.

---

134. H.R. 1157, 108th Cong. (2003).

135. S. 1507, 108th Cong. (2003).

136. H.R. 3171, 108th Cong. (2003).

137. H.R. 2429, 108th Cong. (2003).

138. S. 1701, 108th Cong. (2003).

139. S. 1709, 108th Cong. (2003).

140. H.R. 3352, 108th Cong. (2003).

### Probative Value of Library Records and the Right to Receive Information

¶51 The First Amendment protects the right of free speech.<sup>141</sup> In addition, the First Amendment protects those rights that are necessary to make the right of free speech meaningful.

It is well established that [the First Amendment] safeguards a wide spectrum of activities, including the right to distribute and sell expressive materials, the right to associate with others, and, most importantly to this case, the right to receive information and ideas. These various rights, though not explicitly articulated in either the Federal or Colorado Constitution, are necessary to the successful and uninhibited exercise of the specifically enumerated right to “freedom of speech.”<sup>142</sup>

¶52 Receiving information is not the same as believing or promoting the content of the information. It has been judicially acknowledged that just reading material does not mean one advocates the ideas contained within.<sup>143</sup> If one is to be investigated for reading, the range of ideas people are willing to investigate will necessarily shrink. The right to receive information and ideas has a long history in First Amendment jurisprudence.<sup>144</sup> While the mere fact of reading or looking up material does not prove much, the fact that someone could monitor what people are reading may scare off readers.<sup>145</sup> And where it is ideas, or *expressive rights*, that are the subject of the search, the Supreme Court has held that a search warrant must comply with the particularity requirements of the Fourth Amendment with “scrupulous exactitude.”<sup>146</sup> The First Amendment “prohibits the state from interfering with the communicative processes through which its citizens exercise and prepare to exercise their rights of self-government.”<sup>147</sup>

¶53 The changes made by section 216 to the pen register statute do not meet the scrupulous exactitude required where the First Amendment and the Fourth Amendment meet. A log of Web sites visited shows the subject of a user’s search history which of necessity includes content. If, as this writer has done recently, a

---

141. U.S. CONST. amend. I.

142. *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1051 (Colo. 2002) (citations omitted).

143. *Keyishian v. Board of Regents*, 385 U.S. 589, 600–01 (1967) (“university librarian who recommends the reading of such materials” does not “thereby advocate the propriety of adopting the doctrine contained therein”).

144. *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) (“It is now well established that the Constitution protects the right to receive information and ideas.”).

145. “Anything that chills the desire, the interest of Americans . . . in going to libraries is a very serious matter.” *FBI Counterintelligence Hearings*, *supra* note 117, at 72 (statement of Representative Don Edwards).

146. *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978) (holding that warrant to search offices of student newspaper for pictorial evidence of identity of protesters can only issue where requirements of Fourth Amendment are met with “scrupulous exactitude”); *Stanford v. Texas*, 379 U.S. 476, 485 (1965) (holding that the requirement that warrants “must particularly describe the ‘things to be seized’ is to be accorded the most scrupulous exactitude when the ‘things’ are books, and the basis for their seizure is the ideas which they contain”).

147. *Herbert v. Lando*, 441 U.S. 153, 184–85 (1979) (Brennan, J. dissenting in part) (footnote omitted).

user visits ten Web sites on terrorism, nothing can be assumed about the user based solely on visits to those sites. The point of the search could be doing research for an article on the war against terrorism. The searcher could be compiling information on the hosts of such sites. The searcher could be morbidly attracted to reviewing bad news on the Internet. The list is endless. But no one can decipher a user's intent merely by looking at the sites that he or she has visited.

¶54 No case has yet determined whether or not government seizure of the records of Web sites visited by patrons while at the library is subject to the warrant requirement protection of the Fourth Amendment, but the jurisprudence on the First Amendment right to receive information in a library and on the protection of content in traditional Fourth Amendment analysis are about to collide.

¶55 In *Tattered Cover, Inc. v. City of Thornton*,<sup>148</sup> a case where the constitutionality of a search warrant for bookstore records was at issue, the Colorado Supreme Court had some interesting things to say about the competing values of the right to freely receive information and the need to prosecute criminals and prevent crimes. *Tattered Cover* involved the Colorado Constitution, which has broader protection for First Amendment rights than the United States Constitution.<sup>149</sup> A Colorado bookseller was served a search warrant seeking to discover customer purchase records relating to two books on how to set up clandestine drug labs. Because even the district attorney who issued the warrant was troubled by the First Amendment implications of the warrant, which requested third-party records of reading material, all of the parties to the action agreed to let the court decide if the warrant met constitutional muster.<sup>150</sup> The court's discussion of the First Amendment right to read in private and the chilling effect on that right if innocent third party reading records are easily made public is grounded in United States Supreme Court jurisprudence. *Tattered Cover* is the first case to explicitly hold that the United States Constitution (and Colorado's Constitution) "protect[s] an individual's fundamental right to purchase books anonymously, free from governmental interference,"<sup>151</sup> that there is a constitutional right to receive ideas and information, and that the "citizen is entitled to seek out or reject certain ideas or influences without Government interference or control."<sup>152</sup> The court, citing United States Supreme Court cases, held that "[a]nonymity is often essential to the successful and uninhibited exercise of First Amendment rights, precisely because of the chilling effects that can result from disclosure of identity."<sup>153</sup>

¶56 The court then addressed the collision of this First Amendment right with the Fourth Amendment right to be free from unreasonable searches and seizures,

---

148. 44 P.3d 1044 (Colo. 2002). Although *Tattered Cover* does not involve terrorism or the USA PATRIOT Act, the case was decided in the political and emotional aftermath of September 11, 2001.

149. *Id.* at 1053–54.

150. *Id.* at 1049–50.

151. *Id.* at 1047.

152. *Id.* at 1052 (quoting *United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 817 (2000)).

153. *Id.* (citations omitted).

discussing both probable cause and the requirement that the place to be searched and the objects to be turned over be particularly described.<sup>154</sup> Under federal law, warrants directed at expressive activity must comply with Fourth Amendment requirements with “scrupulous exactitude.”<sup>155</sup> The court discussed a 1998 grand jury subpoena case in which the Office of Independent Counsel sought the records of two bookstores related to purchases by Monica Lewinsky. The district court in that case formulated a balancing test for a subpoena directed to bookstore records, requiring the government to show a compelling interest in or need for the information sought and a sufficient connection between the information sought and the criminal investigation.<sup>156</sup> Under *Tattered Cover*’s analysis, seeking bookstore records because the content of a book is probative is the most chilling and least worthy basis for granting a warrant.

However, we note that, in most situations, there is a lesser danger of harm to constitutionally protected interests when the customer purchase record is sought for reasons entirely unrelated to the contents of the materials purchased by the customer. The chilling effect that results from disclosure of customer purchase records occurs because of the general fear of the public that, if the government discovers which books it purchases and reads, negative consequences may follow. However, if the government seeks a purchase record to prove a fact unrelated to the content or ideas of the book, then the public’s right to read and access these protected materials is chilled less than if the government seeks to discover the contents of the books a customer has purchased.

For example, if the police were to find a book about baseball with a *Tattered Cover* price sticker on it in the vicinity of an illegal drug lab, and they wished to find out who purchased the baseball book in order to place that person at the scene of the crime, the harm to constitutional interests caused by forced disclosure of the *Tattered Cover*’s book records might well be permissible under the balancing test we describe. Similarly, if law enforcement officials seek to discover a book purchase record to disprove a suspect’s alibi, on the theory that the bookstore record proves that the suspect was at the bookstore at a particular time, the contents of the books bought are not significantly at issue and the harm to the public caused by the seizure of the record is less than if the facts were otherwise.<sup>157</sup>

¶57 The *Tattered Cover* court went on to hold that Colorado’s constitution requires more than scrupulous exactitude.<sup>158</sup> But even scrupulous exactitude will be glaringly absent from any USA PATRIOT Act pen register order, which need not describe either the place or the objects to be seized with particularity, and which may be issued without any demonstration of probable cause.

¶58 “Because First Amendment freedoms need breathing space to survive, government may regulate in the area only with narrow specificity.”<sup>159</sup> To the extent that

---

154. *Id.* at 1054 (citation omitted).

155. *Id.* at 1055 (citing *Zurcher v. Stanford Daily*, 436 U.S. 547, 564 (1978); *Stanford v. Texas*, 379 U.S. 476, 485 (1965)).

156. *Id.* at 1056–57 (citing *In re Grand Jury Subpoena to Kramerbooks & Afterwords, Inc.*, 26 Med. L. Rptr. 1599, 1601 (D.D.C. 1998)).

157. *Id.* at 1059 (footnote omitted).

158. *Id.*

159. *NAACP v. Button*, 371 U.S. 415, 433 (1963) (citing *Cantwell v. Connecticut*, 310 U.S. 296, 311 (1940)).

the content of reading material is at issue, library records, like bookstore records, normally have limited probative value in proving a crime. Under current state laws, records are generally available with a subpoena.<sup>160</sup> Indeed, the government seems to have used the subpoena process to access library records since September 11, 2001.<sup>161</sup> Use of the subpoena process allows both notification that the records are being sought and an opportunity for judicial review prior to implementation of the order. It will not unduly burden investigative powers for the government to conform to the due process requirements of the Fourth Amendment when seeking pen register orders for library computers and securing subpoenas for written records of computer use or circulation records.<sup>162</sup> The provisions of the USA PATRIOT Act that allow electronic surveillance of library computers and the seizure of library records do not meet the “least restrictive means requirement” which assures that the government action will not chill the exercise of fundamental expressive rights any more than absolutely necessary to advance the government’s interest.<sup>163</sup>

### Conclusion

¶59 The original drafters of the Constitution “undertook to secure conditions favorable to the pursuit of happiness. . . . They sought to protect Americans in their beliefs, their thoughts, their emotions and their sensations. They conferred, as against the government, the right to be let alone. . . .”<sup>164</sup> The jurisprudence of the Fourth Amendment is still seeking to reach some kind of balance between the increasing ability of the government to use technology to erode the concept of privacy and the belief that there are, in fact, zones of privacy that are still worthy of protection. The USA PATRIOT Act tips the balance in favor of decreasing the right to be let alone by the government. By allowing the FBI to use section 216 to secure content without the usual protection granted by the probable cause requirement necessary for a warrant to issue, and by allowing the FBI to be the arbiter of what happens to the content that is overcollected, no one is protected from a potential invasion of privacy. The past history of the FBI in abusing the power to investigate makes it clear that concerns about the lack of checks and balances on implementing the provisions of the USA PATRIOT Act are not unfounded. In determining what records to keep and what policies to implement, librarians should do their best to ensure that libraries remain neutral, private places to investigate ideas.

---

160. MINOW & LIPINSKY, *supra* note 36, at 174–75.

161. *See supra* ¶¶ 43–44.

162. Subpoenas are not immediately executable, and librarians served with a subpoena have an opportunity to review the matter with counsel and move to quash the subpoena if it has a chilling effect. MINOW & LIPINSKY, *supra* note 36, at 195–97.

163. *Buckley v. Valeo*, 424 U.S. 1, 68 (1976).

164. *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

