Libraries as ISPs - Yes
Libraries as Electronic Service Providers – No

Grayson Barber
July 17, 2006

This memorandum analyzes recent state and federal legislation to determine whether public libraries are Internet Service Providers (ISPs) or Electronic Service Providers. I conclude that public libraries enjoy special status with respect to wiretapping and other forms of surveillance. Congress reauthorized the USA Patriot Act with special provisions for libraries, and a substantial body of case law recognizes the constitutional guarantees that attach to libraries.

The New Jersey Legislature enacted new legislation in December 2005, which at first glance appears to be inconsistent with the New Jersey Library Confidentiality statute.[1] The new legislation amends the state wiretapping law to expand the information which a provider of electronic communication or remote computing service is required to disclose to a law enforcement agency that has obtained a grand jury or trial subpoena. P.L. 1995, Chap. 270, amends N.J.S.A. 2A:156A-29.

Taken literally and in isolation, this new state statute commands all providers of "electronic communication service or remote computing service" to disclose information to law enforcement in response to a grand jury subpoena or trial subpoena. I do not believe libraries fall within the definition of "electronic communication service or remote computing service" for purposes of this statute.

Further, I believe libraries have very strong grounds to resist subpoenas – including trial subpoenas and grand jury subpoenas - that have not been "issued by a court," i.e., signed by a judge. These grounds include 1) reauthorization of the USA

[1] The New Jersey Library Confidentiality Statutes is codified at N.J.S.A. 18A:73-43.2.

Patriot Act, which specifically exempted public libraries from subpoena power, 2) the Library Confidentiality statute; 3) the First Amendment to the US Constitution and 4) the Fourth Amendment to the US Constitution.

Reauthorization of the USA Patriot Act[2]

The Patriot Improvement Reauthorization Act specifically exempts public libraries from a species of subpoena called a national security letter (NSL),[3] unless the library acts as a provider of "electronic communications service," as defined under 18 U.S.C. § 2510(15). The legislative history of this provision makes it clear that libraries have a special status with respect to searches by law enforcement:

> What we did in this legislation is add clarifying language that states that libraries operating in their traditional functions: lending books, providing access to digital books or periodicals in digital format, and providing basic access to the Internet would not be subject to a national security letter. There is no National Security Letter statute existing in current law that permits the FBI explicitly to obtain library records. But, . . . librarians have been concerned that existing National Security Letter authority is vague enough so that it could be used to allow the Government to treat libraries as they do as they do communication service providers such as a telephone company or a traditional Internet service provider from whom consumers would go out and get their access to the Internet and send an receive e-mail.

[2] U.S.A. Patriot Act, 115 Stat. 272 (2001). NSL's are not issued by courts. Before 9-11-2001, NSL's were governed by the Electronic Communications Privacy Act (18 U.S.C. § 2710 et. seq.), the Right to Financial Privacy Act (12 U.S.C. § 3401 note) and the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.). The Patriot Act provided two expansive elements to the issuance of a NSL: First, an NSL may be authorized by Senior FBI officials as well as Special Agents in Charge (SAC's). Second, the Patriot Act eliminated the previous requirement that the NSL be aimed at a foreign power or its agents. Essentially, therefore, the FBI is empowered to issue NSL's to itself. 18 U.S.C. § 2701 et. seq. is directed to communications providers.

[3] There are NSL provisions in three federal statutes, each of which was modified by the USA Patriot Act. Electronic Communications Privacy Act, 18 U.S.C. § 2709 (FBI can compel communications companies to disclose customer information); Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5) (FBI can compel financial institutions to disclose customer information); Fair Credit Reporting Act, 15 U.S.C. § 1681u (FBI can compel credit reporting agencies to disclose records on individuals).

152 Cong. Rec. S1390, (daily ed. Feb. 16, 2006).[4]

Libraries Are ISP's But Not "Electronic Service Providers"

Libraries often serve as a portal to Internet services such as Yahoo or Hotmail. This does not transform libraries into electronic service providers, for purposes of federal law. The New Jersey statute was enacted to conform to federal law, suggesting that the state would similarly exempt libraries from the definition.

The statutory definitions are not particularly illuminating. The federal statute defines an electronic service provider as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). The language of the state wiretap statute is identical. N.J.SA. 2A:156A-2.

Under both federal and state law, libraries enjoy special status. The colloquy in the federal legislative history makes this clear. As Senator Durbin stated, "A gas station that has a pay phone isn't a phone company." 15 Cong. Rec. S1390 (daily ed. Feb. 16, 2006). Providing access to the internet is not the same as operating an interned-based web hosting service for e-mail. Again, the legislative history recognizes the distinction:

> **Mr. Durbin:** So if I understand it correctly, your bill clarifies that libraries, simply because they provide basic internet access, are not communications service providers under the law and are not subject to national security letters as a result. . . . [I]s that a correct conclusion?
>
> **Mr. Sununu:** I absolutely believe the conclusion of the Senator from Illinois is correct. A library providing basic Internet access would not be subject to a National Security Letter as a result of that particular service and other services that are very much in keeping with the traditional role of libraries.
>
> Some have noted or may note that basic Internet access gives library patrons the ability to send and receive e-mail by, for example, accessing an Internet-based e-mail service. But in that case, it is the

[4] Senator Sununu's amendment proceeded unchanged through the approval process and became part of the revised 18 § 2709. Special thanks to Prof. Carol Roehrenbeck for sharing a research memo prepared by her law student, Thomas Madden.

> Web site operator who is providing the communication service- the Internet communication provider itself- and not the library, which is simply making available a computer with access to the Internet.

15 Cong. Rec. S1390, (daily ed. Feb. 16, 2006).

For purposes of the federal statute reauthorizing the USA Patriot Act, therefore, libraries are NOT "electronic service providers". For purposes of the New Jersey state wiretap statute, this understanding should be imported from federal law. This would be consistent with the legislative history of the 2005 amendments to the state wiretap law, which indicate that the purpose of the amendments was to conform to federal law. It would also be consistent with the New Jersey Library Confidentiality statute, N.J.S.A. 18A:73-43.2.

By contrast, libraries ARE internet service providers, "ISPs," under federal law. The Communications Decency Act ("CDA"), contains the following grant of immunity:

> No State or local government may impose any liability for commercial activities or actions by commercial entities, **nonprofit libraries**, or institutions of higher education in connection with an activity or action described in subsection (a)(2) [obscenity] or (d) [sending or displaying offensive material to persons under 18].

47 U.S.C. §223(f)(2). This immunity provision recognizes that librarians should enjoy immunity from prosecution, civil or criminal, regardless of what patrons may view on the Internet. For example, if a library customer uses Hotmail for purposes of defamation or extortion, the library cannot be held responsible.

The term "interactive computer service" specifically includes the Internet access libraries provide. 47 U.S.C. §230(f)(2). The CDA specifically provides that if a third party (e.g. a library patron) uses an Internet terminal to view or disseminate obscene

material, the "interactive computer service" (i.e., the library) will not be considered the "publisher" of the material:

> No provider or user of interactive computer service shall be treated as the publisher or speaker of information provided by any other information content provider.

47 U.S.C. § 230(c)(1). "By its plain language, §230(c)(1) creates a federal immunity to any cause of action that would make service providers liable for information originating with a third party user of the service." Zeran v. America Online, 129 F.3d 327, 330 (4th Cir. 1997), cert. denied, 524 U.S. 937 (1998).

Section 230(e)(3) prohibits any state law cause of action, civil or criminal, that would be inconsistent with the immunity granted to public libraries. It specifies the circumstances under which §230 preempts state law claims, and confirms that immunity is not limited to tort claims. "No cause of action may be brought and no liability may be imposed under any state or local law that is inconsistent with this section."

Thus, if patrons access illegal material on library Internet terminals, the library cannot be held liable. Mainstream Loudoun v. Board of Trustees of the Loudoun County Library, 24 Fed. Supp.2d 552, 565 n.15 (E.D. Va. 1998), citing Zeran.

In Zeran, supra, the court held that even though AOL controls a private network, section 230(c)(1) preempted state law. Even if the ISP has knowledge of the content of material disseminated by a third party, the ISP cannot by held liable for the third party's publication. This means that even if a library knows that one of its customers has sent inappropriate e-mail messages, the library cannot be held liable for its customer's speech.

The New Jersey Library Confidentiality Statute

State law prohibits public librarians from disclosing library records that identify patrons, except under certain limited circumstances. Specifically, N.J.S.A. 18A:73-43.2 provides that

> Library records which contain the names or other personally identifying details regarding the users of libraries are confidential and shall not be disclosed except in the following circumstances:
>
> a. The records are necessary for the proper operation of the library;
> b. Disclosure is requested by the user; or
> c. Disclosure is required pursuant to a subpoena issued by a court or court order.

Under state law, therefore, libraries may not disclose records that contain names, addresses or other personally identifiable information about library customers. A library record is defined under the statute as "any document ... the primary purpose of which is to provide for control of the circulation or other public use of library materials." N.J.S.A. 18A:73-43.1. This means that if the police want access to the computers to check patrons' e-mail, review borrowing records, or track websites, the police must first get a subpoena signed by a judge or a court order signed by a judge.

Legislative History

The legislative history of the library confidentiality statute reveals that the New Jersey Legislature specifically intended to limit the kinds of subpoenas that could be used to obtain customer information. The legislation, as originally introduced in 1984, permitted disclosures in response to "subpoena or court order." The bill was then amended on November 19, 1984, to limit "the type of subpoena" to "*a* subpoena

*_issued by a court_* or court order." As amended, the bill passed both houses of the Legislature unanimously.[5]

The First Amendment Right to Read Privately

The First Amendment guarantees freedom of speech and of the press. It embraces an individual's right to read whatever she wants to read, without fear that the government will take steps to discover which books she buys, reads, or intends to read. Customers have a First Amendment right to receive information in public libraries. Kreimer v. Bureau of Police for Town of Morristown, 958 F.2d 1242, 1252 (3d Cir. 1992). To disclose customers' records without notice and without a court order would have a substantial chilling effect on their willingness to use public libraries. Customers would not feel at ease perusing, borrowing, reading or using other library resources, such as computers.

Libraries are places where anyone can receive information and explore ideas. When a person uses library resources, he engages in activity protected by the First Amendment because he is exercising his right to read. Any governmental action that interferes with the willingness of customers to use the library thus implicates First Amendment concerns. See, e.g., 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."); Griswold v. Connecticut, 381 U.S. 479, 482 (1965) ("The right of freedom of speech and press includes not only the right to utter or to print, but the right to distribute,

[5] The legislative history includes no reports, no hearings and no signing statements. The bill was pre-filed in 1984 and passed in 1985. The statement accompanying the bill noted that library confidentiality was a national concern, and that 16 states had similar statutes. Today 47 of the 50 states have library confidentiality statutes, and two states (Kentucky and Hawaii) have advisory opinions from their attorneys general, stating that library records should be confidential. See http://tinyurl.com/2bb6x

the right to receive, the right to read . . . and freedom of inquiry . . . ."); Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 64-65 n.6 (1963) ("The constitutional guarantee of freedom of the press embraces the circulation of books as well as their publication."); Smith v. California, 361 U.S. 147, 150 (1959) (stating that "the free publication and dissemination of books and other forms of the printed word furnish very familiar applications" of the First Amendment); Martin v. City of Struthers, 319 U.S. 141, 143 (1943) ("The right of freedom of speech and press has broad scope. . . . This freedom embraces the right to distribute literature . . . and necessarily protects the right to receive it."); Lovell v. City of Griffin, 303 U.S. 444, 452 (1938) (circulation of expressive material is constitutionally protected).

Privacy In Public Places

Inevitably, the question will arise whether patrons have a reasonable expectation of privacy in a public library. The answer is that the police still need a warrant even if they are gathering evidence from a publicly accessible place. The U.S. Supreme Court ruled in Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979), that law enforcement officers must obtain a warrant to take allegedly obscene publications off bookshelves in stores that are open to the public.

Fourth Amendment Search and Seizure

The library confidentiality law places an obstacle between law enforcement officers and the evidence they are trying to obtain. This has always been a source of frustration for the police, but it is exactly what the New Jersey legislature contemplated when it enacted the statute. It is consistent with Fourth Amendment search and seizure

law, which similarly frustrates law enforcement officers in their pursuit of evidence. The Fourth Amendment provides that

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

It is without question a burden to the police that they cannot freely seize evidence, intercept phone calls, or use electronic evidence for surveillance of individuals without probable cause. The framers of the Constitution, apprehensive of prosecutorial abuses, created a balance of powers that placed a judge between the authority of the state and the rights of citizens. "The basic purpose of this Amendment … is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials." Berger v. New York, 388 U.S. 41, 53 (1967).

There are numerous cases dealing with the interaction between the Fourth Amendment guarantee against unreasonable searches and seizures and the First Amendment freedom of expression.[6] In United States v. Rumely, 345 U.S. 41 (1953), a bookseller was convicted of contempt of Congress for refusing to divulge to the House Select Committee on Lobbying Activities the names of those who made bulk purchases of political books for further distribution. The Court held, 7-0, that Congress had no authority to demand the identities of book purchasers. "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, book stores, and homes of the land. Through

[6] Historically the struggle for freedom of speech and press in England was bound up with the issue of the scope of the search and seizure power. See Marcus v. Search Warrant, 367 U.S. 717, 724 (1961).

the harassment of hearings, investigations, reports, and subpoenas government will hold a club over speech and over the press." Id. at 57-58 (Douglas, J., concurring).

In Stanford v. Texas, 379 U.S. 476 (1965), a search warrant authorized the search for and seizure of "books, records, pamphlets, cards, receipts, lists, memoranda, pictures, recordings and other written instruments concerning the Communist Party of Texas" at a mail order bookseller. A subsequent search removed over 2,000 books from Stanford's home, and Stanford petitioned for the books' return. The Court held, 9-0, that the warrant purported to authorize an unconstitutional general search. "The constitutional 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." Stanford, 379 U.S. at 485.

The Colorado State Supreme Court invalidated a search warrant, even though it had been signed by a judge. In Tattered Cover v. City of Thornton, 44 P.3d 1044 (Colo. 2002), law enforcement officials wanted to find out who purchased an instruction book on how to make methamphetamine. The Colorado Supreme Court held that special precautions must be taken before such a search could be authorized. If the police could obtain a bookstore's customer purchase records, the court reasoned, the result would be to chill people's willingness to read a full panoply of books and be exposed to diverse ideas. Law enforcement officials can obtain a warrant for such records only upon notice and after an adversarial hearing.

A federal district court in Washington D.C. determined that subpoenas directed to innocent bookstores implicated First Amendment concerns. When the Office of Independent Counsel investigated Monica Lewinsky, it subpoenaed a bookstore where

she had purchased a book for President Clinton. The bookstore moved to quash the subpoena, and won. The court held that, in order to demonstrate the enforceability of the subpoena, the government must show: (1) a compelling interest in or need for the information sought; and (2) a sufficient connection between the information sought and the criminal investigation. In re Grand Jury Subpoena to Kramerbooks & Afterwards, 26 Med. L. Rptr. 1599 (D.D.C. 1998).

Conclusion

For the reasons set forth in this memorandum, I conclude that public libraries ARE ISPs, but ARE NOT "electronic service providers" for purposes of state and federal wiretap laws. In response to investigative subpoenas, librarians should move to quash unless the subpoenas have been reviewed by a court of competent jurisdiction.