PATRIOT IN THE LIBRARY: MANAGEMENT APPROACHES WHEN DEMANDS FOR INFORMATION ARE RECEIVED FROM LAW ENFORCEMENT AND INTELLIGENCE AGENTS

LEE S. STRICKLAND*
MARY MINOW**
TOMAS LIPINSKI***

A. INTRODUCTION

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (the "USA PATRIOT Act")[1] has focused our attention as never before on the expansive world of judicial means by which the government may seek any tangible information regarding the violation of our criminal laws or threats to our national security.[2] While that legislation expanded government authorities, a certain perspective is important: U.S. educational institutions and libraries are in possession of information relevant to the enforcement of our laws and have, in fact, in the past been recipients of various forms of judicial process. What has changed, due in part to the USA PATRIOT Act and in part to technology, is the complexity of the law, the level of public and professional awareness of it, and the concern as to the balance between privacy and national security. What has not changed is the basic rule that, although librarians and educators are required by state law to protect patron[3] and

* J.D., College of Information Studies, University of Maryland. With thanks to Robert Bickal and Cicely Wilson.

** J.D., A.M.L.S., LibraryLaw.com.

*** J.D., Ph.D., L.L.M, School of Information Studies, University of Wisconsin, Milwaukee.

1. Pub. L. No. 107-56, 115 Stat. 272 (2001) (to be codified in scattered sections of 5, 8, 12, 15, 18, 20, 21, 22, 28, 31, 42, 47, 49, 50 U.S.C.) [hereinafter USA PATRIOT Act].

2. While libraries and educational institutions are the focus of this article, the discussion here applies generally to any business entity or individual with the exception of the statutory limitations discussed *infra* notes 3, 4.

3. These laws generally provide that confidentiality extends to records of information sought or received, and materials consulted, borrowed or acquired, and includes database search records, reference interviews, circulation records, interlibrary loan records, and other personally identifiable uses of library materials, facilities, or services—unless disclosure is required by court order. By way of example, the Maryland state statute for library patron confidentiality, set forth at MD. CODE. ANN., EDUC. § 23-107 (2001), is similar to that of most states and provides:

student confidentiality[4] in general, librarians and educators are nevertheless required to disclose relevant records as required by appropriate judicial process. But that is the question—what is appropriate judicial process? Is it a generic term that represents any form of government legal demand to produce documents or information? As we consider in detail below, the term encompasses a range of documents: court orders signed by judges or magistrates, directives signed by clerks of the court (most often in blank without consideration of the merits), or demands signed by executive branch officers (e.g., an inspector in a federal agency) that is authorized to be issued by specific statute and that may thereafter be enforced by court order through the inherent civil and criminal contempt authority.

In this article, we examine university libraries in the context of academic freedom, the text of USA PATRIOT Act provisions most relevant to libraries, and the universe of judicial demands and the specific limitations on their authority, as well as the management options and policies for responding to these demands. This article offers a conservative approach suggesting that patron and student privacy are not absolutes—with respect to government demands—and that libraries and schools may decide on management approaches that balance such privacy with the obligation to protect their information assets from misuse and misappropriation and thus protect their institutions from the newly burgeoning world of cyber liability. This article also offers some progressive suggestions to consider for institutions that wish to take a stronger stance in protecting student privacy.

B. UNIVERSITY LIBRARIES IN THE CONTEXT OF ACADEMIC FREEDOM

In September 2003, in response to increasing pressure from the library community and others to release the number of times that controversial Section 215 of the USA PATRIOT Act had been used to get patron records,[5] Attorney

> Subject to the provisions of subsection (b) of this section, a free association, school, college or university library in this State shall prohibit inspection, use, or disclosure of any circulation record or other item, collection, or grouping of information about an individual that: (1) Is maintained by a library; (2) Contains an individual's name or the identifying number, symbol, or other identifying particular assigned to the individual; and (3) Identifies the use a patron makes of that library's materials, services, or facilities.
>
> The exception provided at part (b) permits disclosure in the course of the library's ordinary business and only for the purposes for which the record was created. Also note that the provisions here are also included in the Maryland Public Information Act (FOIA equivalent) as an exemption from required disclosure under that Act.

4. The release of "educational records" is defined and governed by the Family Educational Rights and Privacy Act of 1974 ("FERPA"), Pub. L. No. 93-380, 88 Stat. 571 (1974) (codified at 20 U.S.C. § 1232g (2000)), also known as the "Buckley Amendment." More specifically, 20 U.S.C. § 1232(g)(b)(2)(B) provides that an educational institution must notify students and former students in advance of complying with any judicial process for the release of their student records. While FERPA does not mandate a specific time frame for notice, most institutions provide a period of ten working days. At the end of that time, unless legal action is initiated by the student and the school is so informed, the records are disclosed.

5. *See* Plaintiff's Motion for Preliminary Injunction, ACLU v. U.S. Dep't of Justice, 265 F. Supp.2d. 20 (D.D.C. 2003) (No. CIV.A.-02-2077 ESH) ("requiring the immediate processing and

General John Ashcroft declassified the number: zero.[6] Rather than alleviate concerns, however, it may be characterized as a blank check that has not yet been cashed.

The fragile nature of academic freedom causes it to wither under *chilling effects*; that is, not knowing when and where surveillance and search provisions will be used. In the setting of higher education, this legislation has particular importance, as that environment is one in which free expression by the members of the university community is historically paramount. This freedom of inquiry, to speak and to receive, is at the heart of the concept of academic freedom. Within this setting, the library, whether physical or virtual, is the natural axis of support for that inquiry. Use of the "library" is the starting point for academic inquiry (the right to receive), as faculty and students access the store of knowledge, whether in print, database, interlibrary loan, or other form. To some extent use of the "library" is also the end of the inquiry, as items such as books, articles, conference proceedings, etc. (the right to speak) become accessible to subsequent scholars through the library's points of access.

This inquiry is set in the broader context of the campus environment and in the virtual setting of university computing and network facilities. Of concern to the library community are the surveillance and search provisions of the USA PATRIOT Act and the impact such provisions may have on the principles of intellectual freedom. The concept of free speech and free inquiry are part and parcel of the American landscape.[7] While the concept of academic freedom is to a large extent undefined by the courts[8] and by scholars alike,[9] it is nonetheless a

release of agency records identified in a request submitted by plaintiffs under the Freedom of Information Act on August 21"). Three hundred and forty-one pages of "responsive records" documents have been released, heavily redacted. *See* ACLU, The Government's Response, *available at* http://www.aclu.com/patriot_foia/foia3.html (last visited Mar. 31, 2004).

6. "[T]he number of times section 215 has been used to date is zero." CNN, *Justice document: Patriot Act provision never used* (Sept. 17, 2003), *at* http://www.cnn.com/2003/LAW/09/17/ashcroft.patriot/index.html. Section 215 refers to USA PATRIOT Act § 215, 115 Stat. at 287–88 (codified at 50 U.S.C.A. §§ 1861–1863 (2003)).

7. *See* Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 65 n.6 (1963) ("freedom of the press embraces the circulation of books as well as their publication"); Griswold v. Connecticut, 381 U.S. 479, 482 (1965) ("not only the right to utter or to print, but the right to distribute, the right to receive, the right to read . . . and freedom of inquiry" (internal citation omitted)); Watchtower Bible & Tract Soc'y v. Vill. of Stratton, 536 U.S. 150 (2002).

8. See *Urofsky v. Gilmore*, 216 F.3d 401 (4th Cir. 2000) (en banc), discussing the concept of academic freedom as a constitutional right, citing *Regents of the University of Michigan v. Ewing*, 474 U.S. 214, 226 (1995), among other cases, and observing that "[d]espite these accolades, the Supreme Court has never set aside a state regulation on the basis that it infringed a First Amendment right to academic freedom." *Urofsky*, 216 F.3d at 412. "Significantly, the Court has never recognized that professors possess a First Amendment right of academic freedom to determine for themselves the content of their courses and scholarship, despite opportunities to do so." *Id.* at 414. *See also* Kate Williams, *Loss of Academic Freedom on the Internet: The Fourth Circuit's Decision in* Urofsky v. Gilmore, 21 REV. OF LITIG. 493, 503 (2002) ("Though Sweezy [*v. New Hampshire*, 453 U.S. 234 (1957)] was the first Supreme Court case to constitutionalize academic freedom, it was also the first to lay the grounds for what continues to be a confusing doctrine.").

9. *See* W. Stuart Stuller, *High School Academic Freedom: The Evolution of a Fish Out of*

matter of professional practice in higher learning.[10] The "university is a traditional sphere of free expression . . . fundamental to the functioning of our society."[11] Because the "essentiality of freedom in the community of American universities is almost *self-evident*[,] [n]o one should underestimate the vital role in a democracy that is played by those who guide and train our youth."[12] While the USA PATRIOT Act is causing controversy and concern in the American public library community, as the vocal sparring match between the Attorney General and the library community demonstrates,[13] the principles of the First Amendment may be heightened even more in the context of the university:

> Our Nation is deeply committed to safeguarding academic freedom, which is of transcendent value to all of us and not merely to the teachers concerned. That freedom is therefore a special concern of the First Amendment, which does not tolerate laws that cast a pall of orthodoxy over the classroom.[14]

This concept underlies the charge that the USA PATRIOT Act, through its increased capacity of surveillance at the university level, in the university library, and in the virtual library of the Internet, poses a threat to the future climate of freedom of inquiry in higher education.[15] The chilling effect of such surveillance is the antithesis of academic freedom.

C. USA PATRIOT ACT: STATUTORY LANGUAGE

Although Section 215 has received much of the press attention, a number of provisions in the USA PATRIOT Act are of concern to libraries in higher education. The USA PATRIOT Act amends several federal statutes relevant to law enforcement and intelligence access to library records.

Water, 77 NEB. L. REV. 301, 302 (1998); J. Peter Byrne, *Academic Freedom: A "Special Concern of the First Amendment"*, 99 YALE L.J. 251, 253 (1989); Amy H. Candido, *Comment, A Right to Talk Dirty?: Academic Freedom Values and Sexual Harassment in the University Classroom*, 4 UNIV. OF CHICAGO LAW SCHOOL ROUNDTABLE, 85, 86 (1996–97).

10. *Urofsky*, 216 F.3d at 411 n.12 ("In view of this history, we do not doubt that, as a matter of professional practice, university professors in fact possess the type of academic freedom asserted by Appellees."). *See also* Damon L. Krieger, *May Public Universities Restrict Faculty from Receiving or Transmitting Information via University Computer Resources? Academic Freedom, the First Amendment, and the Internet*, 59 MD. L. REV. 1398 (2000) (an excellent review of the right to receive information and the right of academic freedom).

11. Rust v. Sullivan, 500 U.S. 173, 200 (1991).

12. Sweezy v. New Hampshire, 354 U.S. 234, 250 (1957) (emphasis added).

13. "According to these breathless reports and baseless hysteria, some have convinced the American Library Association that under the bipartisanly-enacted Patriot Act, the FBI is not fighting terrorism. Instead agents are checking how far you've gotten in the latest Tom Clancy novel." *Remarks of Attorney General John Ashcroft to the National Restaurant Association Conference*, FED. NEWS SERVICE, Sept. 15, 2003, *available at* LEXIS, Federal News Service.

14. Keyishian v. Bd. of Regents, 385 U.S. 589, 603 (1967).

15. Krieger, *supra* note 10, at 1423 ("The express free speech guarantee of the First Amendment includes the right of the people to make use of the Internet to receive information without unwarranted governmental regulation which impinges upon the flow of ideas.").

1. Section 215 Amends Title 50

Section 215 of the USA PATRIOT Act amends the Foreign Intelligence Surveillance Act ("FISA")[16] by deleting current sections 1861 to 1863 of Title 50, U.S. Code, and replacing them with new sections 1861 and 1862.[17] Section 215 reduces the traditional Fourth Amendment requirements for probable cause, and now allows the Federal Bureau of Investigation ("FBI") to obtain personal records by certifying that they are sought for an investigation to prevent terrorism;[18] the FBI need not suspect the person holding the records of any wrongdoing.

New section 50 U.S.C. § 1861(a) authorizes the Director of the FBI or his or her designee to "make an application for an 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."[19] This would include any record, whether digital or analog, not only from the university library, but from campus network and computing centers as well. A proviso to retain First Amendment protections requires that an "investigation of a United States person is not conducted *solely* upon the basis of activities protected by the First Amendment to the Constitution."[20]

New section 50 U.S.C. § 1861(b)(2) specifies that "[e]ach application under this section . . . shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) . . . ."[21] To get the court order, government officials must specify that the records are sought for foreign intelligence investigations, conducted to protect against international terrorism or clandestine intelligence activities. Once the FBI makes that showing, the law says the court "shall enter an . . . order."[22] Once granted, the order entitles the FBI to procure any library records including book circulation, Internet use, patron registration, and even virtual reference records.

New section 50 U.S.C. § 1861(c)(2) provides that "[a]n order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a)."[23] In other words, the order cannot disclose that it is issued in conjunction with or for a § 1861(a) purpose (i.e., an investigation to protect against international terrorism or clandestine intelligence activities).

The library receiving such an order is prohibited from disclosing its occurrence. New section 50 U.S.C. § 501(d) states that "[n]o person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the FBI has sought or obtained tangible things under this

16. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered sections of 18 and 50 U.S.C.A.) [hereinafter FISA].

17. USA PATRIOT Act § 215, 115 Stat. at 287–88 (codified at 50 U.S.C.A §§ 1861–1863 (2003)).

18. *See id*.

19. 50 U.S.C.A. § 1861(a)(1) (2003).

20. *Id.*

21. *Id.* § 1861(b)(2) (emphasis added).

22. *Id.*

23. *Id.* § 1861(c)(2).

section."[24]

The constitutionality of Section 215 has been challenged by the Muslim Community Association of Ann Arbor.[25] The complaint for declaratory relief claims that it is facially invalid in violation of the First, Fourth, and Fifth Amendments to the Constitution.

2. Additional Provisions

The following tables show additional provisions and citations to the amended laws of interest to libraries:[26]

USA PATRIOT ACT PROVISIONS AND LIBRARY RECORDS
Court Order: Intercept Orders (Wiretaps)

Type of information: Real Time Content: Voice, data, keystrokes, phones, computers, etc.
Legal standard (listed in descending level of threshold): Probable cause that target committed one of list of serious crimes, now including *terrorism and computer crimes*. Other options tried or unlikely to succeed.
Legal authority: Federal Wiretap Statute (codified at 18 U.S.C.A. § 2516 (2000 & West Supp. 2003))
Notes and sample orders: ▪ Also known as "Title III" orders. ▪ Broader list of crimes.[27] ▪ The Act does not impose any additional requirement on service providers to furnish facilities or technical assistance beyond permitting the authorized interception. ▪ Given the obligation to implement a court order, however, the applicability of this assurance against reconfiguration is uncertain in those cases where implementation of a court order would in fact require reconfiguration.[28] For example, Carnivore or related tools may be

24. *Id.* § 501(d).

25. *Muslim Cmty. Assoc. of Ann Arbor v. Ashcroft,* Complaint for Declaratory and Injunctive Relief, Civil Action No. 03- 72913 (E.D. Mich. July 7, 2003), Complaint *available at* http://news.findlaw.com/hdocs/docs/aclu/mcaa2ash73003cmp.pdf (last visited Mar. 31, 2004).

26. *See* Mary Minow, *Library Records Post-Patriot Act (Federal Law)* (Sept. 16, 2002) *available at* http://www.llrx.com/features/libraryrecords.htm. *See also* Wiley Rein & Fielding LLP, *The Search & Seizure of Electronic Information: The Law Before and After the USA Patriot Act* (Jan. 18, 2002), *available at* http://www.arl.org/info/frn/other/matrix.pdf.

27. USA PATRIOT Act § 202, 115 Stat. 272, 278 (codified at 18 U.S.C.A. § 2516 (2000 & West Supp. 2003)).

28. *Id.* § 222, 115 Stat. at 292–93 (not codified, but published as 18 U.S.C.A. § 3124 note (2000 & West Supp. 2003).

29. *See* Donald P. Delaney et al, Wiretap Laws and Procedures: What Happens When the U.S. Government Taps a Line (Sept. 23, 1993), *available at* http://www.cpsr.org/cpsr/privacy/communications/wiretap/denning_wiretap_procedure_paper.txt (last visited Mar. 31, 2004).

installed by the Government. ▪ FBI agents must follow procedures that go well beyond the legal requirements imposed by Title III and which involve extensive internal review. In preparing the affidavit, the FBI agent in the field works with the field office principal legal advisor and also with an attorney in the local U.S. Attorney's Office, revising the documentation to take into account their comments and suggestions. After the documents are approved by field office management, they are submitted to the Department of Justice.[29]

Legal standard: Target is a foreign power or an agent of a foreign power; and a significant purpose is to gather foreign intelligence.
Legal authority: Foreign Intelligence Surveillance Act ("FISA") (codified at 50 U.S.C.A. § 1805 (2003 & West Supp. 2003))
Notes and sample orders: ▪ Determined by FISA Court (50 U.S.C. § 1803); records sealed. ▪ Allows FISA "roving" intercepts of target's wire and electronic communications regardless of the location. Court order need not specify name of library (previously had to specify parties who were required to provide assistance).[30] ▪ Wiretaps of non-U.S. persons who are agents of a foreign power 120 days with extensions up to one year.[31]

Court Order: Search Warrant

Type of information: Past Content: Any tangible thing including computers and computer files.
Legal standard: Affidavits filed with complaint that there is probable cause to believe that a crime has been committed and that the information sought is material to that defense; may be based upon hearsay evidence in whole or in part, with sufficient indicia of reliability.
Legal authority: Search Warrants (codified at 18 U.S.C.A. § 3103 (2000), § 3103a (2000 & West Supp. 2003)). Federal Rule of Criminal Procedure 41.
Notes and sample orders: ▪ See sample search warrant at http://www.cybercrime.gov/s&sappendix2002.htm#_F_ (last visited Mar. 31, 2004). ▪ *Immediately executable* with or without library's cooperation.

30. USA PATRIOT Act § 206, 115 Stat. at 282 (codified at 50 U.S.C.A. § 1805 (2003 & West Supp. 2003)).

31. *Id.* § 207, 115 Stat. at 282 (codified at 50 U.S.C.A. §§ 1805, 1824 (2003 & West Supp. 2003)).

- "Single jurisdiction search warrants": Terrorism investigation warrants may be issued by a Federal magistrate judge in any district in which activities related to the terrorism may have occurred, for a search anywhere in country.[32]
- "Sneak and peek": If the court finds reasonable cause to believe that notification of the execution of the warrant may have an adverse result; reasonable necessity for seizure.[33]
- On July 23, 2003, the House voted 309–118 in favor of the Otter Amendment to prohibit any funds from being used to carry out Section 213.[34]

Type of information:
Past Content: E-mail, voicemail.

Legal standard:
Probable cause—standards vary depending on whether the e-mail has been opened, how long the e-mail has been in storage, and whether or not the e-mail is held by a third party.

Legal authority:
18 U.S.C.A. §§ 2703(a)–(c) (2000 & West Supp. 2003).
18 U.S.C.A. §§ 2510(1)–(4) (2000 & West Supp. 2003).

Notes and sample orders (Section numbers refer to USA PATRIOT Act):
- See sample search warrant at http://www.cybercrime.gov/s&sappendix2002.htm#_F_ (last visited Mar. 31, 2004), and at 18 U.S.C.A. § 2703(a) (2000 & West Supp. 2003)).
- A court with jurisdiction over the offense may issue warrants for providers anywhere in country.[35]

Type of information:
Past Content: Physical searches.

Legal standard:
Probable cause to believe that:

> (A) the target of the physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and (B) the premises or property to be searched is owned, used, possessed by, or is in transit to or from an agent of a foreign power or

32. *Id.* § 219, 115 Stat. at 291 (codified at FED. R. CIV. P. 41).

33. *Id.* § 213, 115 Stat. at 285–86 (codified at 18 U.S.C.A. § 3103a (2003 & West Supp. 2003).

34. *See* The Library of Congress, Bill Summary, *at* http://www.congress.gov/cgi bin/bdquery/z?d108:H.A.292 (last visited Mar. 31, 2004).

35. USA PATRIOT Act § 209, 115 Stat. at 283 (codified at 18 U.S.C.A. §§ 2510, 2703 (2000 & West Supp. 2003)); § 220, 115 Stat. at 291–92 (codified at 18 U.S.C.A. §§ 2703, 2711 (2000 & West Supp. 2003)).

a foreign power; . . . .
Legal authority: FISA (codified at 50 U.S.C.A. § 1824 (2003 & West Supp. 2003)).
Notes and sample orders: ▪ Up to ninety days unless agent of foreign power (120 days) extend up to one year. ▪ Must keep secret. ▪ Compensation for expenses.

Court Order: § 2703(d) Court Order

Type of information: Past Content: E-mail stored more than 180 days.
Legal standard: Specific and articulable facts relevant to an ongoing criminal investigation.
Legal authority: 18 U.S.C.A. § 2703(d) (2000 & West Supp. 2003)).
Notes and sample orders: ▪ See sample § 2703(d) court order at http://www.cybercrime.gov/s&sappendix2002.htm#_B_ (last visited Mar. 31, 2004). Although this is a court order, provider may promptly move to quash or modify order if unusually voluminous or undue burden.

Court Order: Pen Trap Orders; Real-time Collection Transaction Records

Type of information: Non-Content: E-mail "To/From" headers; top level URLs; phone numbers dialed out or received.
Legal standard: Court must grant (no discretion) if government certifies reasonable grounds that facts are relevant to ongoing criminal investigation.
Legal authority: Federal Pen Register and Trap and Trace Statute (codified at 18 U.S.C.A. §§ 3121–3127 (2000 & West Supp. 2003)).
Notes and sample orders: ▪ See sample Pen-Trap court orders at: http://www.cybercrime.gov/s&sappendix2002.htm#_D_ (last visited Mar. 31, 2004). Installation issued nationwide; orders must specify initial provider, but need not name other providers.[36] ▪ Provider may request written or electronic certification that the order applies to the provider.[37]

36. *Id.* § 216, 115 Stat. at 288–90 (codified at 18 U.S.C.A. §§ 3121–3127 (2000 & West Supp. 2003)).

37. 18 U.S.C.A. § 3123(a)(1) (2000 & West Supp. 2003).

38. *Id.* § 3123(c) (2000 & West Supp. 2003).

39. *Id.* § 3123(d)(2) (2000 & West Supp. 2003).

- Sixty days and may be extended for additional sixty day periods.[38]
- Provider may not disclose existence of pen/trap "to any . . . person, unless or until otherwise ordered by the court."[39]

Legal standard:
Concerns foreign intelligence and does not concern a U.S. citizen or concerns U.S. citizen and protects against terrorism or intelligence activities.

Legal authority:
FISA Pen Registers and Trap and Trace Devices for Foreign Intelligence Purposes (codified at 50 U.S.C.A. § 1842 (2003 & West Supp. 2003)).

Notes and sample orders:
Dropped requirement of foreign agents or those engaged in international terrorist or clandestine intelligence activities; it is enough that the order is sought as part of an investigation to protect against international terrorism or clandestine intelligence activities. Must not be motivated solely by an American's exercise of his or her First Amendment rights. Order remains at ninety days.[40]

Court Order: Subpoenas[41]

Type of information: Varies.

Legal standard: Administrative Subpoenas—Issued for lawfully authorized purpose and information is relevant to inquiry; reasonableness standard.

Legal authority: Various federal statutes.[42]

Notes and sample orders:

- See sample subpoena language at: http://www.cybercrime.gov/s&sappendix2002.htm#_E_ (last visited Mar. 31, 2004). Library may move to quash or modify in court. Library has burden of proof to show agency failed to meet standard; generally subject to contempt if refusal to comply after court order.

Type of information:
Non-Content: Subscriber name, session time, network address.

Legal standard: ECPA Subpoenas—Relevant to investigation.

Legal authority:
ECPA (codified at 18 U.S.C.A. § 2703(c) (2000 & West Supp. 2003)).

Notes and sample orders:

- Patron authentication (who use library databases from home/office) may be at risk; library may move to quash or modify.

40. USA PATRIOT Act § 214, 115 Stat. at 286–87 (codified at 50 U.S.C.A. §§ 1842, 1843 (2003 & West Supp. 2003)).

41. A subpoena is not a court order unless signed by a judge.

42. U.S. DEP'T OF JUST., APPENDICES A, B, AND C ACCOMPANYING REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH EXECUTIVES AND AGENCIES, *available at* http://www.usdoj.gov/olp/appendixa1.pdf (last visited Mar. 31, 2004).

Court order: FISA Court Order, "Section 215 Business Records"

Type of information: Content: Any tangible thing (including books, records, papers, documents and other items).
Legal standard: Investigation to protect against international terrorism or clandestine intelligence activities; formal pleading to FISA Court. Provides that investigation of a U.S. person is not conducted solely upon the basis of activities protected by the First Amendment.
Legal authority: FISA (codified at 50 U.S.C.A.§§ 1861–1863 (2003)).
Notes and sample orders: ▪ Sealed proceedings; orders will not state their purpose. ▪ No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the FBI has sought or obtained tangible things under this section. ▪ Requires Attorney General to inform select congressional committees on semiannual basis of total number of requests granted, modified, and denied. Classified. ▪ Declassified in 2003 by Attorney General Ashcroft.

OTHER MEANS OF GETTING LIBRARY RECORDS

Not Court Orders: National Security Letters

Type of information: Telephone and electronic communications; financial records; credit records.
Legal standard: Authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment.
Legal authority: ECPA (codified at 18 U.S.C.A. § 2709 (2000 & West Supp. 2003)) (telephone and electronic communications records); Right to Financial Privacy Act ("RFPA"), (codified at 12 U.S.C.A. § 3414(a)(5)(A) (2001 & West Supp. 2003)) (financial records); Fair Credit Reporting Act ("FCRA"), 15 U.S.C.A. § 1681u (1998 & West Supp. 2003) (credit records).
Notes and samples: ▪ Intelligence corollary to the administrative subpoena. ▪ Although these are not court orders, institutions are instructed by law to comply.

Not Court Orders: Notification to Preserve Evidence[43]

Type of information:

43. This is not a court order, but must be adhered to pending court proceedings.

Records and other evidence.
Legal standard: Government requests provider preserve (not turn over) records and other evidence.
Legal authority: 18 U.S.C.A. § 2703(f) (2000 & West Supp. 2003)).
Notes and samples: ▪ See sample 2703(f) letter at http://www.cybercrime.gov/s&sappendix2002.htm#_C_ (last visited Mar. 31, 2004). Only for information already in provider's possession, not future information. Must take all necessary steps to preserve records. Fax or phone call okay; library should request confirmation letter for its own protection, and for clarification of request. Request lasts ninety days, may be extended ninety days.

Not Court Orders: No Warrant Search and Seizures

Type of information: Computers, electronic evidence.
Legal standard: Consent, exigent circumstances, plain view, search incident to a lawful arrest emergency authority also given in statutes such as FISA and ECPA.
Legal authority: Supreme Court decisions interpreting Fourth Amendment.[44]
Notes and samples: ▪ Department of Justice, Computer Crime and Intellectual Property Section, Criminal Division, July 2002, Searching and Seizing Computers without a Warrant, available at: http://www.cybercrime.gov/s&smanual2002.htm (last visited Mar. 31, 2004).

Not Court Orders: Voluntary Disclosure of Records

Legal standard: Communications services provider have "good faith" belief that emergency involving danger of death or serious physical injury.
Contents may be disclosed to a federal, state or local entity.
Legal authority: ECPA (codified at 18 U.S.C.A. § 2702 (2000 & West Supp. 2003). Computer Fraud and Abuse Act ("CFAA") (codified at 18 U.S.C.A. § 1030(a)(5) (2000 & West Supp. 2003)).
Notes and samples: ▪ The Cyber Security Enhancement Act, Section 225 of the Homeland Security Act, amended Section 212 of the USA PATRIOT Act, lowering the threshold for voluntary disclosure from "reasonable" belief to "good

44. *See, e.g.,* California v. Ciraolo, 476 U.S. 207 (1986) (holding that observations from low-flying airplanes present no Fourth Amendment issue.

faith," from "immediate danger" to an emergency involving danger of death or serious physical injury; and allowing disclosure to a federal, state or local government entity instead of law enforcement.

D. FACTUAL BACKGROUND

Our consideration of the law of judicial process draws factually on a number of actual cases and incidents that presented government information demands. We discuss the spectrum of those demands (some judicial and some merely requests) and the potential management responses in that context. Some have also been reported in the media, for example, the government approach information demand to the Hartford Public Library in late 2002. The libraries allegedly attached monitors to library computers,[45] but it was later confirmed that the computers had been used to hack into business computers in California in criminal violation of the federal Computer Fraud and Abuse Act[46] and that a limited search warrant had been served and executed.[47] Previously, search warrants had been executed against various public libraries in an effort to locate the Unabomber,[48] and in many more incidents as detailed in a recent survey by the University of Illinois.[49]

Almost all of these incidents and cases began in unexpected ways but often touch upon the information technology resources of the involved institution. Given cases may involve a fraudulent computer transaction using a stolen credit card or check, a child pornographer peddling images over the Internet, or a patron launching a proxy attack against other computers. Or there may be more drama in that a federal agent and local police officer working together on a joint terrorism

45. Such software records keystrokes, can be surreptitiously installed on systems, and has been used in industry and in criminal investigations in the past. The government version is often referred to in the media as "Magic Lantern." ABCNews.com, *Shedding Light on Magic Lantern* (Dec. 21, 2001), *available at* http://abcnews.go.com/sections/scitech/CuttingEdge/cuttingedge011221.html.

46. Counterfeit Access Device and Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213 (1986) (codified as amended at 18 U.S.C.A. § 1030 (2000 & West Supp. 2003)).

47. The Hartford Courant initially reported that the FBI had installed software to monitor the Internet activity of patrons at the Hartford Public Library. Bill Olds, *FBI Searched Library Computer, Didn't Install Monitoring Program*, THE HARTFORD COURANT, Nov. 7, 2002, at B1. It subsequently acknowledged that the report was incorrect after Michael J. Wolf, the state's most senior FBI agent, disputed what he called the "outrageously fallacious column" and stated that the FBI had used a search warrant to seize evidence from a specific library computer that had been used to "hack" into a business computer system in California "for criminal purposes" but had not installed any monitoring program. *Id*.

48. Jennifer Auther, *Kaczynski the bookworm: FBI pores over Unabomb suspect's library* (Apr. 24, 1996), *available at* http://www.cnn.com/US/9604/24/unabom.books (last visited Mar. 31, 2004).

49. The January 2003 University of Illinois survey narrative and data may be found, respectively, at The Graduate School of Library and Information Science, Library Resource Center, Public Libraries and Civil Liberties: A Profession Divided, at http://www.lis.uiuc.edu/gslis/research/civil_liberties.html (last updated Jan. 22, 2003); and The Graduate School of Library and Information Science, Library Resource Center, Public Libraries and Civil Liberties—Questionnaire: Public Libraries' Response to the Events of 9/11/2001: One Year Later, at http://www.lis.uiuc.edu/gslis/research/finalresults.pdf (last visited Mar. 31, 2004).

task force arrive and advise that the Foreign Intelligence Surveillance Court has issued a court order requiring a search and absolute secrecy. Some instances may involve a telephone call from a law enforcement officer in a neighboring state who advises that he or she is investigating a crime involving threatening e-mails that have been traced to an Internet Provider ("IP") address associated with your institution. The law enforcement officer may ask to confirm your IP address, to secure all system usage records maintained on your library computers, and to secure all messages or other traffic that might be relevant to the crime remaining on the hard drive of the noted personal computer ("PC") and/or the library servers. Of course, there are many other permutations of this scenario—often involving the official making the request or the court issuing the request. Instead of the detective in a neighboring state, a detective in another county in your state or a federal court across the country, or even an employee from an administrative or regulatory agency with a demand issued by that agency, may make the request. What does one do when the demand is in the form of an oral request and not a judicial document? Perhaps, simply, a federal officer requests to inspect public use workstations including portable PCs used by students and patrons.

Each of these incidents reflect the fact that while our schools and libraries are bastions of intellectual freedom, they nevertheless exist in a dangerous world—threats to our institutional assets, domestic crime, and international challenges to our national security. As such, there is a clear obligation on the part of a university's management to understand judicial process in terms of rights and obligations and to adopt comprehensive institutional policy to interact successfully with the government. In the following section we first examine the universe of judicial process given the differences in the type of evidence sought (e.g., electronic communications or documentary records), the form of judicial process (e.g., search warrant or subpoena or otherwise), the interest (e.g., law enforcement or intelligence or even civil), and, of course, the authority involved (e.g., local, state or federal—and where). Second, we consider a number of management initiatives in this arena including the importance of records schedules, the need for a published privacy policy, the options for reserving the right to electronically monitor users, and the potential authority to make voluntary disclosures. Of course, this article should not be considered legal advice and is intended only to provide a starting point for legal inquiry.

E. UNDERSTANDING THE FORMS OF CRIMINAL-RELATED JUDICIAL PROCESS

We begin our discussion with the forms of judicial process—–a question relating to the title of the document, the identity of the issuer, the type of information sought, and hence the authority of the document. While judicially-compelled production of information of any form is generally controlled by the Fourth Amendment (and also state constitutional equivalents that may provide any greater citizen protection), federal and state governments have adopted a range of statutes to more specifically regulate the process. Indeed, it is important to remember the courts have determined that the Fourth Amendment protects only a

"reasonable expectation of privacy" that "society is prepared to accept;"[50] there are many exceptions, including, for example, customer records held by businesses,[51] observations from low-flying airplanes, [52] recordings of telephone numbers dialed,[53] or trained dog sniffs of luggage.[54] In such areas, therefore, government demands simply do not constitute searches for purposes of the Fourth Amendment and may be regulated by statute if at all.

1. Regular Business or Personal Records (Electronic or Paper)

In many criminal investigations, the primary concern is documentary evidence in the form of typical business records. In the library environment, documentary evidence could include circulation records, Internet sign-up records, reference records (including digital reference interviews), and other records. Not included in this discussion is a separate category of information—electronic communications records—that will be addressed subsequently in Part E.4 of this article.

2. The World of Search Warrants

Our understanding today of search warrants comes generally from judicial decisions—many of relatively recent vintage. We know, although not conclusively established until 1967, that search warrants reach not only *"instrumentalities, fruits, or contraband"* but indeed any item of *"evidential value."*[55] This means that a search warrant may be directed to a library for any information, patron specific or otherwise, provided only that the material sought has evidentiary value.

Although the First Amendment provides no explicit shield to search warrants, the Supreme Court has acknowledged that when expressive rights are implicated, a search warrant must comply with the particularity requirements of the Fourth Amendment with "scrupulous exactitude"[56] and thereafter Congress has provided special rules for the media vis-à-vis search warrants.[57]

50. Katz v. United States, 389 U.S. 347, 361 (1967).

51. *See*, *e.g.*, United States v. Miller, 425 U.S. 435 (1976) (holding that bank records are disclosed information and thus not subject to Fourth Amendment protection).

52. *See*, *e.g.*, Florida v. Riley, 488 U.S. 445 (1989) (holding that police officer's observation of greenhouse from vantage point of helicopter did not constitute a search for which a warrant was required).

53. *See*, *e.g.*, Smith v. Maryland, 442 U.S. 735 (1979) (holding that installation and use of pen register by telephone company does not constitute a search within the meaning of the Fourth Amendment)

54. *See*, *e.g.*, United States v. Place, 462 U.S. 696 (1983) (holding that exposure of luggage to a trained narcotics detection dog is not a search for Fourth Amendment purposes).

55. Warden v. Hayden, 387 U.S. 294 (1967) (emphasis added).

56. Zurcher v. Stanford Daily, 436 U.S. 547 (1978) (internal citations omitted). In point of fact, *Hayden*, *supra* note 55, set the stage for *Zurcher* by allowing law enforcement to use search warrants for evidence of crime that may have been collected during news gathering efforts—here student newspaper photographs of a violent clash between the police and demonstrators at Stanford University. *Id*. at 551.

57. Although not specifically applicable to libraries and educational institutions, Congress, after *Zurcher*, broadened the protection for the media with the enactment of the Privacy

Moreover, although special rules per se are not provided for libraries or bookstores concerning search warrants, in *Tattered Cover, Inc. v. City of Thorton*,[58] the Colorado Supreme Court, relying on the privacy clause in the state's constitution, ruled that a warrant served on a bookstore was not enforceable and should not have been enforceable and should not have been issued.[59]

In *Tattered Cover*, a mailing envelope from the Tattered Cover bookstore had been found in the trash outside a suspected drug lab.[60] Inside the lab were two books that appeared to fit the envelope: the titles were *Advanced Techniques of Clandestine Psychedelic and Amphetamine Manufacture*, by Uncle Fester, and *The Construction and Operation of Clandestine Drug Laboratories*, by Jack B. Nimble.[61] When Denver police tried to execute a local search warrant, owner Joyce Meskis immediately contacted the bookstore's attorney, who in turn contacted the Denver District Attorney's ("Denver DA") office.[62] A Denver DA persuaded the police officers not to execute the warrant until the Tattered Cover could litigate its validity.[63]

The court ruled that an innocent, third-party bookstore must be given an opportunity for a hearing and the court must apply a balancing test, recognizing that a seizure of documents, books, or films is conceptually distinct from a seizure of objects such as guns or drugs.[64] Law enforcement must show a compelling need, no reasonable alternatives (such as identifying clothing on the scene instead), and the warrant must not be unduly broad (e.g., records for thirty days instead of one).[65] Additionally, the court must consider whether or not the purchase records are sought because of the books' content, creating a chilling effect on readers.[66]

The last factor makes the distinction between book purchase records that are sought because of a book's content and those sought merely to prove a fact

Protection Act of 1980 ("PPA"), Pub. L. No. 96-440, 94 Stat. 1879 (1980) (codified as amended at 42 U.S.C. § 2000aa (2000)), that prohibits search warrants directed against media or media employees except in extraordinary circumstances (i.e., reasonably likely that target will destroy or conceal the evidence, that media has committed or are committing a crime; or that death or injury will result if a search warrant is not used). Instead, it mandates the use of subpoenas. Note that the PPA applies to federal and local law enforcement but violations do not result in suppression of the evidence, 42 U.S.C. § 2000aa-6(d), yet may result in civil damages against the involved government agency or individual officers if there is state sovereign immunity, 42 U.S.C. § 2000aa-6(a), (b), (e).

58. Tattered Cover, Inc. v. City of Thorton, 44 P.3d 1044 (Colo. 2002).

59. *Id*. at 1063.

60. *Id*. at 1048.

61. *Id*. at 1049. After the case was over, the actual title sent in the mailer was revealed: *A Guide to Remembering Japanese Characters*, by Kenneth G. Henshall. Dan Recht, attorney for the Tattered Cover said, "I desperately wanted people to know this because of the ironic twist and because, despite their best efforts, the police can be dead wrong." Susan Greene, *Bookseller at last tells secret title*, DENV. POST, Apr. 16, 2003, *reprinted in* NEWSLETTER ON INTELLECTUAL FREEDOM (July 2003), *available at* https://members.ala.org/nif/v52n4/bookseller-reveals.html.

62. *Tattered Cover*, 44 P.3d at 1049.

63. *Id*. at 1050.

64. *Id.* at 1059.

65. *Id.*

66. *Id.*

unrelated to the content. In this case, law enforcement found books about methamphetamine labs and wanted to establish motive. The court weighed this factor against law enforcement. If a book, unrelated to the motive, had been found in the methamphetamine lab, however, the court said it would place its owner at the scene and would not likely produce a chilling effect.[67]

3. The World of Subpoenas

Subpoenas differ from search warrants in many regards, including most importantly the previously discussed right to produce the records rather than have them seized. A criminal subpoena is authorized by court rules[68] and may properly seek any information or thing relevant to the investigation being pursued and thus is broader than a search warrant.[69] Second, because a criminal subpoena is based only on an allegation of relevance—not proven probable cause—the subpoena may be contested through a motion to quash.[70] At least in the federal sphere, however, the showing required to quash is difficult to meet—a criminal grand jury subpoena is deemed valid "unless the district court determines that there is no reasonable possibility that the category of materials the government seeks will produce information relevant to the general subject of the grand jury investigation."[71]

Administrative subpoenas are a category of governmental authority to compel the production of documents or testimony that has been granted by Congress to various federal agencies. Unlike search warrants that are issued by federal courts and require a demonstrated showing of probable cause or grand jury subpoenas that include citizen oversight, administrative subpoenas that are issued by federal agents themselves, without any prior approval by the courts, need only relate generally to the subject matter of the investigation, and may generally be enforced through the civil and criminal contempt powers of the federal courts.[72] Today, there are well over three hundred existing administrative subpoena authorities, and

67. The Colorado Supreme Court looked to state constitutional protections against privacy and innocent third party searches:

> In order for law enforcement officials to prevail, they must demonstrate a compelling governmental need for the specific customer purchase records that they seek. When conducting the balancing test, the court may consider whether there are reasonable alternative methods of meeting the government's asserted need, whether the search warrant is unduly broad, and whether the law enforcement official seek the purchase records for reasons related to the content of the books bought by any particular customer.

Id. at 1047.

68. *See, e.g.,* FED R. CRIM. PROC. 17.

69. *See, e.g.,* United States v. Gurule, 437 F.2d 239 (10th Cir. 1970).

70. As discussed earlier, this was the essence of the recent noted litigation, *Tattered Cover*, involving a rather limited warrant for bookstore records in a criminal drug prosecution. The Colorado Supreme Court held that, under Colorado constitutional law, when a search warrant implicates Constitutional values, the *ex parte* warrant process should not apply in cases of innocent third parties. *Tattered Cover*, 44 P.3d at 1060.

71. United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991).

72. *See, e.g.,* United States v. LaSalle Nat'l Bank, 437 U.S. 298 (1978); United States v. Powell, 379 U.S. 48 (1964); Okla. Press Publ'g Co. v. Walling, 327 U.S. 186 (1946).

the Department of Justice describes them as a "complex proliferation" of law with varying enforcement methods and varying provisions for the protection of individual rights including privacy in each of the enabling statutes.[73]

In *Tattered Cover*, in addition to the local search warrant, the Drug Enforcement Agency ("DEA") served an administrative subpoena on the bookstore, requesting the title of the books corresponding to information listed on the mailer.[74] Of note to administrative subpoena recipients, in an aside, the court wrote: "Using such a subpoena was ordinarily a successful technique for DEA officers, though such a subpoena lacks any legal force or effect."[75]

4. Electronic Communications Information

Beyond the basics of Fourth Amendment law for documentary evidence in federal criminal law enforcement investigations, the Electronic Communications Privacy Act ("ECPA")[76] controls access to electronic communications records and has an interesting history. Indeed, the issue of electronic searches is even more complex than the law of physical searches for documentary records because of the evolution of technology and the statutory overlay to the Fourth Amendment. The Supreme Court first addressed the issue in 1928, holding that a telephone wiretap was not covered by the Fourth Amendment.[77] Justice Brandeis in his dissent, however, was eloquent as to the issue:

> The evil incident to invasion of the privacy of the telephone is far greater than that involved in tampering with the mails. Whenever a telephone line is tapped, the privacy of the persons at both ends of the line is invaded and all conversations between them upon any subject, and although proper, confidential and privileged, may be overheard. Moreover, the tapping of one man's telephone line involves the tapping of the telephone of every other person whom he may call or who may call him. As a means of espionage, writs of assistance and general warrants are but puny instruments of tyranny and oppression when compared with wire-tapping.[78]

As a result, Congress first addressed the issue in the Communications Act of 1934[79] that, *inter alia*, proscribed any person, not authorized by the sender, to

73. U.S. DEP'T OF JUST., OFFICE OF LEGAL COUNSEL, REPORT TO CONGRESS ON THE USE OF ADMINISTRATIVE SUBPOENA AUTHORITIES BY EXECUTIVE BRANCH AGENCIES AND ENTITIES (2002), *available at* http://www.usdoj.gov:80/olp/intro.pdf.

74. *Tattered Cover*, 44 P.3d at 1049.

75. *Id.*

76. Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.A.) [hereinafter ECPA]. *See* 18 U.S.C.A. § 2510 (2000 & West Supp. 2003) for real time provisions and 18 U.S.C.A. § 2701 (2000 & West Supp. 2003) for other access provisions.

77. Olmstead v. United States, 277 U.S. 438 (1928).

78. *Id.* at 475–76 (Brandeis, J., dissenting).

79. Pub. L. No. 73-416, 48 Stat. 1064 (1934) (codified as amended in scattered sections of 47 U.S.C.A.).

intercept any communication.[80] By 1968, the law had become so complex and confused that Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act[81] to address the specific conditions and procedures under which wiretaps would be authorized. Congress revisited the issue in 1986 with the ECPA as electronic communications became prevalent.[82]

The ECPA has a four-tier approach to acquiring the very broad range of electronic communications information[83] that was enlarged somewhat by the USA PATRIOT Act. First, a *real-time intercept order* requires a greater showing than a regular search warrant and must be authorized by the most senior levels of the Department of Justice.[84] It applies to any real-time voice or data transmission,[85] may be used only for specific crimes (e.g., murder, narcotics or terrorism),[86] and only when normal investigative techniques for obtaining the information have failed, are likely to fail, or are too dangerous.[87] The intercept order has two parts—one authorizing the law enforcement agency to conduct the intercept, and the other to an ISP to provide necessary assistance. When the provider cannot comply, this is the circumstance in which Carnivore[88] may be deployed.

Second, a *traditional search warrant* is used for stored electronic

80. 47 U.S.C.A. § 301 (2001).

81. Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C.A. §§ 2510–2522 (2000 & West Supp. 2003)).

82. *Id.*

83. The ECPA is a classic example of a statute that addresses government access to a range of information—some falling within the scope of the Fourth Amendment (e.g., real-time intercepts) and some wholly without (e.g., subscriber information held by the telephone company).

84. ECPA § 105, 100 Stat. at 1855–56 (codified as amended at 18 U.S.C.A. § 2516 (2000 & West Supp. 2003)); § 106, 100 Stat. at 1856–57 (codified as amended at 18 U.S.C.A. § 2518 (2000)).

85. *Id*. § 101, 100 Stat. at 1848–53 (codified as amended at 18 U.S.C.A. § 2510 (2000 & West Supp. 2003)).

86. *Id*. § 105, 100 Stat. at 1855–56 (codified as amended at 18 U.S.C.A. § 2516); § 106, 100 Stat. at 1856–57 (codified as amended at 18 U.S.C.A. § 2518).

87. *Id*. § 105, 100 Stat. at 1855–56 (codified as amended at 18 U.S.C.A. § 2516); § 106, 100 Stat. at 1856–57 (codified as amended at 18 U.S.C.A. § 2518).

88. Carnivore, more recently renamed DCS-1000, is in essence, a special filtering tool that can be inserted into a communication network and configured to gather the information authorized by court order, and only that information. *See* Stephen W. Tountas*, Carnivore: Is the Regulation of Wireless Technology a Legally Viable Option to Curtail the Growth of Cybercrime?*, 11 WASH. U.J. L. & POL'Y 351 (2003). In other words, it is a Local Area Network ("LAN") packet sniffer that identifies and copies those packets (by IP address) so authorized. Its use does not change any Constitutional or statutory requirements for warrants and court orders, but it has been the subject of enormous civil liberties controversy because of the possibility of intentional or accidental misuse. Because of these concerns, however, former Attorney General Reno convened an impartial review by a leading U.S. university. On November 21, 2000, the Illinois Institute of Technology completed its report and verified that the system operates as stated, albeit that proper use relies on the operator's ability to configure the filter correctly and fully. IIT RESEARCH INSTITUTE, INDEPENDENT TECHNICAL REVIEW OF THE CARNIVORE SYSTEM: FINAL REPORT (Dec. 8, 2000), *available at* http://www.cdt.org/security/carnivore/001214 carniv_final.pdf.

communications[89] (e.g., e-mail at a service provider and now voice mail pursuant to the USA PATRIOT Act[90]). It requires a determination by a federal judge that probable cause exists to believe that a crime has been committed and that the information sought is material to that offense.[91]

Third, and less difficult, a *court order* is utilized to obtain transactional records and the content of certain electronic communications.[92] Such orders must be granted automatically if the government certifies that there are "reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation"[93] as supported by specific and facts able to be articulated. Transactional records take three forms: *"*pen register*"* information (i.e., telephone numbers dialed); *"*trap and trace*"* information (i.e., incoming telephone numbers); and, under the USA PATRIOT Act, *"*routing and address*"* information (i.e., electronic communications headers but not content).[94] The content that is available is essentially old messages and requires notice to the subscriber although *"*delayed notice*"* may be authorized by the judge. More specifically, old messages are deemed to be unopened messages held by an *"*electronic communications service*"* provider for over 180 days or opened mail held by a *"*remote computing service*"* provider.[95]

Least difficult of all is an *administrative or grand jury subpoena* that is issued by the government itself, without judicial assistance, to obtain information. Typically, in the electronic arena, such subpoenas are used to identify the subscriber including addresses and, under the USA PATRIOT Act, the means of payment, session times and temporary IP addresses assigned.[96]

It should also be noted that most, if not all, states have similar laws addressing the acquisition of electronic communications information, some of which are even more protective of privacy. For example, Maryland's statute includes a more restrictive provision than most on the taping of telephone calls by private

89. ECPA § 201, 100 Stat. at 1860 (codified as amended at 18 U.S.C.A. § 2701 (2000 & West Supp. 2003)).

90. USA PATRIOT Act § 209(2), 115 Stat. 272, 283 (codified at 18 U.S.C.A. § 2703 (2000 & West Supp. 2003)).

91. Although a regular criminal search warrant (issued under FED R. CRIM. PROC. 41) and an ECPA search warrant are identically termed and issued under the same legal basis of probable cause, they are somewhat different in practice. Ordinarily, an ECPA search warrant is served on a provider and the provider then produces the information described in the warrant.

92. 18 U.S.C.A. § 2703(b), (c).

93. 18 U.S.C.A. § 2703(d).

94. USA PATRIOT Act § 216(a)(2), 115 Stat. at 288 (codified at 18 U.S.C.A. § 3121 (2000 & West Supp. 2003)).

95. ECPA § 105, 100 Stat. at 1861 (codified as amended at 18 U.S.C.A. § 2703(a)). The arcane nature of these terms that underlay the entire ECPA framework comes from the early days of computing services when the ECPA was passed. Essentially, Congress likened an electronic communications service to the U.S. Post Office and required a higher standard for access while a remote computing service provider was likened to a third party and required a lower standard (i.e., a subpoena) for access.

96. USA PATRIOT Act § 210, 115 Stat. at 283 (codified at 18 U.S.C.A. § 2703(c)(2)).

citizens—requiring consent of both parties but providing a defense of lack of knowledge of the law.[97] Linda Tripp was prosecuted under this statute during the Clinton administration. Her prosecution failed, however, when the state was precluded from utilizing specific testimony of Monica Lewinsky that would have established the requisite knowledge.[98]

5. The Specific USA PATRIOT Act Amendments to the ECPA

As detailed in the preceding section, the USA PATRIOT Act made some changes to the ECPA scheme that supporters say accommodate advances in technology or remove inconsistencies in the protection of information based on its particular format. Other changes (a) expanded the authority for issuance of intercept orders to crimes related to terrorism[99] and computer fraud;[100] (b) expanded the roving wiretap authority by allowing search warrants for stored messages (email and voice) and court orders for transactional records (e.g., "pen register") to be valid everywhere in the nation and without naming specific common carriers;[101] (c) broadened the scope of orders for transactional records to include any form of electronic communication (e.g., e-mail or web surfing) not just telephone communications;[102] (d) allowed stored voice mail messages to be acquired by the slightly easier search warrant process, thus harmonizing the law for stored voice mail and stored e-mail;[103] (e) broadened slightly the scope of the subpoena authority for subscriber information by allowing for access to payment and type of service information rather than merely current name and address;[104] (f) changed the rules on dissemination of criminal investigation information by allowing the automatic sharing with intelligence (the reverse took place under pre-USA PATRIOT Act law);[105] (g) authorized, but only if requested, assistance by law enforcement to ISPs or businesses under computer attack (but only where a person is trespasser and not in an existing contractual arrangement, and limited intercepts to communications to/from the attacker);[106] and (h) broadened and

97. *See* MD. CODE ANN., CTS. & JUD. PROC. §§ 10-402, 410 (2002).

98. *See* Court's Ruling on State's Motion, Maryland v. Tripp, No. K-99-038397 (Md. Cir. Ct. May 22, 2000), *available at* http://www.freerepublic.com/forum/a39298f5f61de.htm (last visited Mar. 31, 2004); CNN, *Prosecutors drop wiretapping charges against Tripp* (May 24, 2000), *available at* http://www.cnn.com/2000/ALLPOLITICS/stories/05/24/trippcase.cnn/ (last visited Mar. 31, 2004).

99. USA PATRIOT Act §§ 101–106, 115 Stat. at 276–78 (codified in scattered sections of 18 and 50 U.S.C.A.); § 201, 115 Stat. at 278 (codified at 18 U.S.C.A. § 2516 (2000 & West Supp. 2003)).

100. *See* USA PATRIOT Act § 206, 115 Stat. at 282 (codified at 50 U.S.C.A. § 1805 (2003 & West Supp. 2003)).

101. *Id*. §§ 201–202, 115 Stat. at 278 (codified at 18 U.S.C.A. § 2516).

102. *Id*. § 209, 115 Stat. at 283 (codified at 18 U.S.C.A. § 2703 (2000 & West Supp. 2003)).

103. *Id*. § 210, 115 Stat. at 283 (codified at 18 U.S.C.A. § 2703).

104. *Id*. § 203, 115 Stat. at 280–81 (codified at 18 U.S.C.A. § 2510 (2000 & West Supp. 2003)); 50 U.S.C.A. § 403-5d (2003 & West Supp. 2003)).

105. *See id*. § 210, 115 Stat. at 283 (codified at 18 U.S.C.A. § 2703).

106. *Id*. § 217, 115 Stat. at 285–86 (codified at 18 U.S.C.A § 3103a (West Supp. 2003)).

clarified the rules for voluntary disclosure of information by an ISP.[107]

6. The Functional Implications of Receiving Search Warrants or Subpoenas

To the extent that law enforcement is concerned with electronic communications (e.g., e-mail or the records concerning e-mail) then one of the four types of ECPA orders will be received. To the extent documentary records (paper or electronic) are sought, then either a regular search warrant or subpoena would be received depending largely on the discretion of law enforcement. As such, while as legal counsel you might argue that a search warrant is not appropriate for an innocent third party, a search warrant could certainly be issued and executed. Indeed, as we have considered, federal precedent permits the use of search warrants for the search and seizure of evidence in the possession of innocent third parties. This permitted use of search warrants is the law in the vast majority of states, with Colorado, given the *Tattered Cover* decision in 2002, being the primary exception.

A second implication of receiving search warrants or subpoenas is government-mandated secrecy for criminal judicial process. Although not frequently used, the USA PATRIOT Act includes a provision that allows a court to delay immediate notification of the execution of any order[108]—generally referred to in the media as "sneak and peek" warrants. More specifically, the use of such delayed notice warrant—the correct legal term—must be authorized if the court finds that there is reasonable cause to believe that providing immediate notice would have an adverse result, as defined in 18 U.S.C. § 2705, that there is a showing of reasonable necessity for the seizure, and that a specified time for ultimately giving notice is specified. In point of fact, this authority is consistent with established case law and is not a substantial change in Constitutional law.[109] But equally in point of fact, it is a deeply unpopular provision as evidenced by the amendment introduced by Representative C.L. "Butch" Otter (R., ID) to H.R. 2799, the 2004 Appropriations Act for the Departments of Commerce, Justice and State, that would prohibit any expenditure of funds for such search warrants. This amendment passed in the House by a vote of 309 to 118, representing the clearest sign of growing bipartisan opposition to certain provisions of the USA PATRIOT Act.[110]

A third implication involves the process that takes place when law enforcement arrives at the door with a warrant that involves computer searches—exactly how are computer searches conducted and are the stories of rampant hardware seizures realistic? The answer begins with the management rule that all library staff should receive instruction on library policy as to receipt of judicial process and that the library director and counsel are the individuals authorized to act in this regard,

107. *Id*. § 212, 115 Stat. at 284–85 (codified at 18 U.S.C.A. §§ 2702, 2703 (2000 & West Supp. 2003)).

108. *See id*. § 213, 115 Stat. 272, 285–86 (codified at 18 U.S.C.A. § 3103a).

109. *See, e.g.,* United States v. Villegas, 899 F.2d 1324 (2d. Cir. 1990); United States v. Freitas, 800 F.2d 1451 (9th Cir. 1986).

110. Press Release, Dennis J. Kucinich, *House Takes Historic Step against Patriot Act* (July 23, 2003), *available at* http://www.house.gov/apps/list/press/oh10_kucinich/030724Patriot.html.

noting, however, that junior staff are often most likely to be involved upon arrival of law enforcement. Given this circumstance, library staff must be prepared to oversee and maintain notes as to the execution of the warrant, which includes being prepared to discuss the specifics of the execution with the officers.

It is critical to remind library and university staff that the most effective approach to judicial process is not adversarial, but rather through cooperation and negotiation because in our judgment the many stories of "over-reaching" by law enforcement can be attributed at least in part to a breakdown in communications. In doing so, it is important to understand that computer searches may be executed in four basic ways: (a) search the computer and print out a hard copy of particular files at that time (not frequently used because of potential loss of metadata and other information); (b) search the computer and make an electronic copy of particular files at that time; (c) create a duplicate electronic copy of the entire storage device on-site (i.e., a bit-stream copy), and then later recreate a working copy of the storage device off-site for computer forensics review (through commercially-available software); and (d) seize the equipment, remove it from the premises, and review its contents off-site.[111]

Although some believe that option (c) represents the best solution for the library or school and should be acceptable for law enforcement if negotiated and explained, but the ultimate option selected depends significantly on the role of the computer hardware in the offense. If the hardware is itself evidence, an instrumentality, contraband, or a fruit of crime, law enforcement officers will usually plan to seize the hardware and search its contents off-site. An example here would be a computer used by an individual at home to transmit child pornography or a stolen computer; in these cases, the computer is, respectively, an instrumentality of crime and a fruit of a crime; as such, the warrant will describe the hardware and authorize seizure. If the hardware is merely a storage device for evidence, however, officers generally will only seize the hardware if less disruptive alternatives are not feasible. For example, if the probable cause relates to information stored on the computer (e.g., the suspect used a library computer to send a message planning a crime), the warrant should focus on the content of the relevant files rather than on the storage devices which may happen to contain them; in such cases, the warrant should describe the information based on its content and authorize seizure in whatever form the information may be stored.

While these generalities are important to understand and provide a basis for discussions with law enforcement for minimizing intrusion, there are nevertheless other drivers that may require broader police action. First, although the warrant may speak in terms of information, and it is generally the policy of law enforcement to proceed in the least intrusive manner possible, the commingling of target information with much other information can justify the seizure of a larger body of records whether in physical or electronic form. Second, the execution of a

111. U.S. DEP'T OF JUST., CRIMINAL DIV, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION 42 (July 2002) [hereinafter SEARCHING AND SEIZING COMPUTERS].

search may result in the "plain sight" identification of additional information and seizure if it meets a "probable cause" standard—although the scope of this authority in the computer arena is somewhat confused and variable according to the facts of specific cases.[112] Last, in any circumstance, while the library official on site may object to actions that she believes to be in excess of the terms of the warrant, she can do nothing to prevent the officers from seizing information deemed appropriate.

7. Emergency Situations and Search Warrants

As shown in reported legal cases,[113] anecdotal accounts,[114] and even movies involving both typically criminal as well as terrorism circumstances, [115] government authorities have relied on the exigent circumstances exception to the Fourth Amendment to conduct searches and seizures without benefit of a judicially-entered warrant. This authority can be used against any holder of information, including innocent third parties such as public libraries and educational institutions. The standard? The courts have recognized this exigent circumstances exception to the general requirement for a search warrant and have thus upheld an immediate, warrantless seizure when and where a reasonable person would believe that immediate action "was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."[116]

A somewhat more complex analysis applies for electronic intercept warrants where federal law provides statutory terms for exigent circumstances.[117] Here the law empowers warrantless interception if the law enforcement officer is specially designated by the U.S. Attorney General or the principal prosecuting attorney of any state or subdivision; if there are factual grounds that would authorize an intercept; if there reasonably exists an emergency situation that involves an immediate danger of death or serious physical injury to any person, conspiratorial

112. *See, e.g.*, United States v. Carey, 172 F.3d 1268 (10th Cir. 1999) (holding warrant for computer files relating to drug trafficking did not justify five hour effort opening and inspecting JPEG files containing child pornography).

113. In less than three years of this new century, there are 1,933 reported cases in Lexis involving exigent circumstances, and the Supreme Court has most recently spoken on the issue in *Kirk v. Louisiana*, 536 U.S. 635 (2002), again recognizing the well-settled rule of law that probable cause alone does not equate to exigent circumstance authorizing law enforcement to proceed in the absence of a warrant.

114. To protect confidences, we will note only that public libraries and universities have not infrequently been subject to seizures of equipment and information under exigent circumstances without warrants. This is not to suggest that all or even some actions were improper but it is to note the potential and actual use of this authority.

115. *See, e.g.,* PHONEBOOTH (20th Century Fox 2003) psychological crime drama starring Colin Farrell, Kiefer Sutherland, and Forest Whitaker that involves a serial killer terrorizing the person in and persons surrounding a Manhattan public telephone booth where the police decide they are unable to intercept the ongoing telephone conversation without a warrant.

116. *See, e.g.,* United States v. McConney, 728 F.2d 1195, 1199 (9th Cir. 1984) (en banc).

117. *See* 18 U.S.C.A. § 2518(7) (2000).

activities threatening the national security interest, or conspiratorial activities characteristic of organized crime; and if an order could not be obtained with due diligence.[118] Thereafter, within forty-eight hours of the intercept, an appropriate application must be made and granted or the interception immediately terminated and will be considered illegally acquired.[119] Thus courts have held an emergency to exist in upholding warrantless intercepts in the context of a kidnapping, ransom demand, and ultimate murder given that all three statutory factors were met,[120] but not a bank robbery planned in the next forty days,[121] and not where the requesting officer was a state trooper who had not been designated by the principal prosecuting attorney of county in question.[122]

Since exigent seizures are almost always challenged, the courts look generally to the degree of urgency involved (e.g., the evidence about to be removed or destroyed or a crime is about to be committed) and the amount of time necessary to obtain a warrant.[123] Clearly, the destruction issue plays a prominent role when considering electronic information and to the extent that a library's practice or policy would result in the loss of information, an immediate seizure could result. In every case, however, a finding of exigent circumstances is based on the specific facts, and generalized arguments will not suffice—certainly not if the innocent third party (i.e. the library) makes clear its intention to preserve evidence pending the arrival of appropriate judicial process.[124] Although agreements to preserve evidence may be made orally, written documentation should follow so that both parties are in agreement as to what records are at issue and for how long. The Department of Justice exigent authority extends only so far as necessary to prevent immediate destruction and no further. Accordingly, an exigent seizure would not authorize a subsequent warrantless search since the exigency would typically have ended.[125]

In sum, there are three basic considerations in understanding exigent circumstances. First, exigent circumstances is a very specific and finite exception generally available only when evidence is threatened with loss and there is simply no time for a warrant. Second, exigent circumstances may also be available when any delay may cause grave damage to the community often in terms of permitting a crime to occur, a person to die, or a criminal to escape. Third, and perhaps most importantly, exigent circumstances does not equate to a general crime scene exception to the Fourth Amendment. Other than very limited searches to protect the safety of officers or seizures of evidence in plain sight, there is no authority to

118. *Id*.

119. *Id*.

120. *See, e.g.,* Nabozny v. Marshall, 781 F.2d 83 (6th Cir. 1986).

121. United States v. Crouch, 666 F. Supp. 1414 (N.D. Cal. 1987).

122. Shingleton v. State, 387 A.2d 1134 (Md. Ct. Spec. App. 1978). In addition, in this case, there was no evidence of conspiratorial or organized crime activities; however, even though the intercept was unlawful, the content was not made known to the jury and there was no prejudice.

123. *See, e.g.,* United States v. Reed, 935 F.2d 641 (4th Cir. 1991).

124. *See, e.g.,* United States v. McConney, 728 F.2d 1195, 1206 (9th Cir. 1984) (holding that "unjustified but sincere fear cannot excuse noncompliance").

125. *See*, *e.g*, United States v. David*,* 756 F. Supp. 1395 (D. Nev. 1991).

conduct searches and seizures of crime scenes and law enforcement risks significant harm to any criminal prosecution based on such seizures.[126]

Beyond exigent circumstances, there is an additional little-known circumstance in emergency situations—that of "telephone warrants," or even the potential that officers may proceed without the physical possession of an issued warrant. Specifically in the first instance, Rule 41 of the Federal Rules of Criminal Procedure ("FRCrP") allows for the request and issuance of a warrant by telephone or other electronic means.[127] Essentially, the process is that the law enforcement applicant must prepare a "proposed duplicate original warrant" and place a call to the appropriate magistrate or judge.[128] The judge shall then place the officer (or other persons having the necessary information to establish probable cause) under oath,[129] receive the necessary testimony as well as the verbatim contents of the proposed warrant, make and certify a verbatim record of the conversation,[130] enter the contents of the proposed duplicate original warrant (with amendments, if any) into an original warrant,[131] sign that original warrant with the exact time of issuance,[132] and direct the applicant to sign the judge's name on the duplicate original warrant.[133] Thereafter, that duplicate is executed.

With respect to the second instance—non-possession of a warrant—a number of court decisions have held that the failure to adhere to the specific requirement in FRCrP 41 for the display of a warrant and the provision of a signed inventory does not generally invalidate the search and seizure, provided that a valid warrant did in fact exist. Thus, courts have upheld searches where there was a failure to display and deliver a copy of a search warrant until a day later,[134] where a search was executed after hearing on police radio that a warrant had been issued,[135] or where a search inventory was not completed in the defendant's presence.[136] The logic underlying these decisions is that the failures are technical violations of the FRCrP, and not constitutional violations that would invalidate a proper warrant and otherwise proper search. And while these are not typical situations, it is critical to appreciate that failures may occur and to ensure that your institutional policies reflect that possibility.

8. Some Other Forms of Demands or Circumstances of Disclosure

Beyond warrants, subpoenas, and exigent circumstances, one should also be

126. *See*, *e.g.*, Flippo v. West Virginia, 528 U.S. 11 (1999); Hargraves v. Commonwealth**,** 557 S.E.2d 737 (Va. Ct. App. 2002).

127. FED. R. CRIM. P. 41(d)(3), (e)(3).

128. FED. R. CRIM. P. 41(e)(3)(a).

129. FED. R. CRIM. P. 41(d)(2).

130. FED. R. CRIM. P. 41(d)(3).

131. FED. R. CRIM. P. 41(e)(3)(B).

132. FED. R. CRIM. P. 41(e)(3)(D).

133. *Id*.

134. United States v. Marx, 635 F.2d 436 (5th Cir. 1981).

135. United States v. Charles, 883 F.2d 355 (5th Cir. 1989).

136. United States v. Bassford, 601 F. Supp 1324 (D. Me. 1985), *aff'd*, 812 F.2d 16 (1st Cir. 1987).

aware that the release or potential release of library information (including patron specific information) may become an issue in a number of additional circumstances. First, federal authorities may make a formal request for the preservation of records and other evidence pursuant to 18 U.S.C. §2703(f). This statute obligates the library to preserve the described records for ninety days pending receipt of appropriate legal process that would authorize actual release;[137] moreover, the statute applies only retrospectively and does not require capture and preservation of new information that arises after the date of this request.[138]

Second, it is not unusual to receive verbal requests from law enforcement and other government officials without the benefit of any judicial process. In fact, such requests appear to be substantially more numerous than formal demands.[139] While it may not be improper to request information[140] and to respond, some may wish to consider the arguable anonymity rights of patrons, and all must be cognizant that there is to be no disclosure of information concerning patron (or student) use of the facilities and materials. Otherwise, the result would be a violation of state-specific patron (or student) privacy laws by the staff and the possible exclusion of the acquired evidence from any prosecution.

A third and related rationale for disclosure would be information concerning a witnessed criminal act—there is simply no protectable privacy interest in such circumstances.[141] In these instances, the information should be secured and law enforcement notified immediately.

Last, as libraries and educational institutions possess substantial information beyond patron or student specific information, voluntary disclosure would be appropriate under the state freedom of information ("FOI") statute. For example, information about the public business of a library such as the IP addresses of the library public Internet computers would be releasable but not the IP addresses of sites visited by specific patrons.[142] The caution that should be urged upon library and university staff in these circumstances is that the line between public information and privileged protected information may be difficult to ascertain, hence caution and discussion is encouraged before voluntary disclosure.

137. 18 U.S.C. § 2703(f)(2) (2000).

138. *Id.*

139. For example, the January 2003 University of Illinois survey of judicial process made a number of interesting findings, including a 4-1 ratio between voluntary and mandatory requests and a 50% rate of cooperation on voluntary requests—a point that highlights the risk to patron confidentiality through seemingly innocuous interaction. The scope of the voluntary cooperation was not made clear, however. For the survey narrative and data see *supra* note 49.

140. For example, the most frequent question of this genre is whether an individual pictured in a photograph is or has been in the library. Because there is no cognizable privacy interest vis-à-vis one's presence in a public building, a library staff member may, but is not required to, answer the question.

141. *See, e.g.,* Horton v. California, 496 U.S. 128 (1990).

142. Advisory Opinion (AO) 26-03, Virginia FOI Advisory Council (Dec. 8, 2003), *available at* http://opengovva.org/opinions/ao2603.htm.

F. UNDERSTANDING THE FORMS OF INTELLIGENCE-RELATED JUDICIAL PROCESS

1. The Foreign Intelligence Surveillance Act

If the ECPA for electronic communications and regular search warrants and subpoenas for documentary evidence were not enough, yet another legal mechanism to obtain information exists. It is relatively unknown, it works in total secrecy, and it was substantially broadened in scope by the USA PATRIOT Act. It is the Foreign Intelligence Surveillance Act ("FISA")[143] and it is an authority that was used 1,228 times in 2002.[144] More specifically, FISA is the federal law that regulates warrants for the acquisition of electronic information or physical searches as well as court orders for the production of business records in national security counter-intelligence or counter-terrorism cases in the United States.

Why there is separate law for the same type of intrusion is an intriguing Constitutional question and reflects the fact that the Fourth Amendment has a complicated intersection with the authority of the President to conduct foreign relations, provide for national defense, and collect foreign intelligence. These conflicting considerations have led to judicial recognition that, even with respect to U.S. citizens, there are substantial limitations on Fourth Amendment rights in the context of foreign intelligence—whether in the United States or overseas—if the person is acting on behalf of foreign powers. In essence, there is a "foreign intelligence" exception to the Fourth Amendment warrant requirement as held by most federal courts but never explicitly by the Supreme Court.[145] Fortunately, however, as we know from the lessons of the Nixon Administration, there is no domestic intelligence exception.[146]

---

143. Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified as amended in scattered sections of 18 and 50 U.S.C.A.). Also relevant but beyond the scope of this article is Exec. Order No. 12,333, 3 C.F.R. § 200 (1981), *reprinted as amended in* 50 U.S.C. § 401 (2000). Executive Order 12,333 ("EO"), issued by President Reagan in 1981, remains in effect today and provides Presidential direction for the conduct of intelligence operations in the United States in general and overseas to the extent the operations concern U.S. persons. It should be noted that *outside the United States* neither the ECPA nor FISA have any application. Therefore, if a U.S. citizen or permanent resident alien ("PRA") is to be targeted outside the United States, the EO requires the approval of the Attorney General, who, by internal guidelines, must find that there is probable cause to believe that such person is an agent of a foreign power. Decisions to target and collect against non-U.S. persons overseas are left to the intelligence community.

144. Letter from John Ashcroft, Attorney General, to L. Ralph Mecham, Director, Administrative Office of the United States Courts (Apr. 29, 2003), *available at* http://www.usdoj.gov/04foia/readingrooms/2002annualfisareporttocongress.htm (last visited Mar. 31, 2004).

145. *See, e.g.*, United States v. Bin Laden, 126 F. Supp.2d 264, 277 (S.D.N.Y. 2000) ("[T]his court adopts the foreign intelligence exception to the warrant requirement.").

146. *See* United States v. United States Dist. Court, 407 U.S. 297 (1972). In an anti-Vietnam War protest case involving domestic warrantless electronic surveillance by the FBI, the trial court ordered disclosure and the Justice Department attempted to secure a Writ of Mandamus to compel the District Court to vacate its order. *Id.* at 301. The Supreme Court refused—agreeing the Nixon-era surveillance unlawful in that there was no "domestic security" exception to the Fourth Amendment. *Id.* at 321.

Given these constitutional limitations, Congress in 1978 enacted FISA in order to regulate the collection of "foreign intelligence information"[147] from foreign powers or agents of foreign powers in the United States through a scheme of Attorney General ("AG") procedures and approvals and in most cases applications to the specially appointed Foreign Intelligence Surveillance Court ("FISC") for secret warrants. The FISC is composed of eleven federal district court judges, appointed by the Chief Justice for staggered terms and from different circuits, who review AG applications for electronic surveillance, physical searches, and demands for other information such as business records.[148] The cases are presented *ex parte* and *in camera* by attorneys from the Department of Justice ("DOJ") Office of Intelligence Policy and Review, and the records and files of the cases are secret and sealed and may not be revealed even to persons whose prosecutions are based on evidence obtained under FISA warrants, except to a limited degree set by district judges' rulings on motions to suppress.[149]

But most significant is that the threshold condition for FISA warrants is *not probable cause of criminal activity*, as with traditional Fourth Amendment law, *but rather probable cause that the target is a foreign power or an agent of a foreign power*. In light of the fact that FISA warrants can authorize highly intrusive electronic surveillance and physical searches, may be directed against both aliens and U.S. persons, and may lead to criminal prosecutions, the civil liberties concern has always been that this process should not erode our basic rights under the Fourth Amendment. Moreover, it is important to note that FISA orders, while seeking information about terrorism, can be and often are directed to innocent third parties who are in possession of relevant information—from private entities such as ISPs to state and local government entities such as libraries or schools.

2. The USA PATRIOT Act Amendments to FISA, Including Section 215 Authority

Moreover, FISA was substantially amended by the USA PATRIOT Act. Now, intelligence cases may involve law enforcement aspects (to resolve the practical conundrum that many intelligence cases do in fact develop evidence of a federal crime), all forms of electronic orders are "roving" (i.e., they apply to all applicable

147. FISA defines "foreign intelligence information" as information about (1) an actual or potential attack or other grave hostile acts of a foreign power, (2) sabotage or international terrorism by a foreign power or an agent of a foreign power, (3) clandestine intelligence activities by a foreign power or agent, or (4) concerning a foreign country that is necessary to the national defense or the security of the United States or the conduct of the foreign affairs of the United States. 50 U.S.C.A. § 1801(e) (2003).

148. 50 U.S.C.A. § 1803(a) (2003). Section 208 of the USA Patriot Act increased the number of federal district judges designated to serve on the FISC from seven to eleven and required that no less that three of the judges reside within twenty miles of the District of Columbia. *See* USA PATRIOT Act § 208, 115 Stat. 272, 283 (codified at 50 U.S.C. § 1803(a)).

149. The very secret nature of the proceedings and the very minimal annual report have been the subject of continuing media criticism. *See* U.S. Department of Justice, Office of Intelligence Policy and Review, FOIA Reading Room Records, *available at* http://www.usdoj.gov/04foia/readingrooms/oipr_records.htm (last updated May 2, 2003).

carriers without the necessity to name individuals) and, perhaps most significant, pursuant to Section 215 of the USA PATRIOT Act, the production of business records now may be directed to any entity, for any "tangible thing," based solely on a sworn assertion that the order is for an investigation "to obtain foreign intelligence information not concerning a United States person," or "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."[150] A "United States person" is defined as a citizen of the United States, a permanent resident, or certain associations or corporations.[151]

This new authority vis-à-vis business and financial records has generated substantial controversy given its broader reach and reduction of judicial oversight. Indeed it is this authority that has led to the concern over widespread abuse of patron privacy through the extensive seizure of patron records and perhaps entire databases, as contrasted to records concerning a given person. Critics of the USA PATRIOT Act assert that this is certainly the case and supporters note that it is doubtful, given that precedents to date have invalidated broad, general, non-particularized warrants as well as warrants for seizure of equipment that are not elements of the criminal enterprise. Moreover, it is difficult to contemplate a circumstance where a federal judge would accept the bald assertion that all records maintained, for example, by a library are relevant to a terrorism investigation. Institutions that wish to take an active stand to protect patron privacy might consider drafting a privacy policy that states the institution will comply with court orders for specified patron records, but that orders for fishing expedition requests will not be honored. The institution might then file for declaratory judgment to assure the validity of the policy.

3. National Security Letter Demands

There also exists a little known FISA-related provision known as the National Security Letter ("NSL") for certain electronic communications, transactional records (not content), as well as certain financial records. Essentially, as the intelligence corollary to the administrative subpoena in the law enforcement world, the NSL authority is found in three separate statutes—the Right to Financial Privacy Act,[152] the ECPA that we considered previously,[153] and also the Fair

150. USA PATRIOT Act § 215, 115 Stat. at 287–89 (codified at 50 U.S.C.A. §§ 1861–1863 (2003)).

151. 50 U.S.C. § 1801(i) (2000). As defined in the U.S. Code:

> 'United States person' means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of Title 8 of the Immigration and Nationality Act), 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, as defined in subsection (a)(1), (2), or (3) of this section.

Id.

152. *See* 12 U.S.C.A. § 3414(a)(5)(A) (2001 & West Supp. 2003). This section allows for

Credit Reporting Act ("FCRA").[154] The NSL authority, modified by the USA PATRIOT Act, may now be exercised simply with a certification of relevance to an intelligence or terrorism investigation.[155] Although no challenges to NSLs had been made as of May 2003,[156] the library may consider a challenge as a possible course of action.

4. Secrecy With Respect to All FISA Matters

A major distinction between criminal process and intelligence process—FISA orders and NSL demands—is that all are secret and the recipient is barred from publicly disclosing the existence of the information provided. A frequent question from library and educational management is whether the secrecy provision will prevent their counsel's involvement. The best informed judgment is that the general secrecy provisions of FISA orders should not be interpreted as to prevent the individual library employee receiving the order from fully disclosing the fact and content to library management and legal counsel. Indeed, it is critical that every library establish and communicate a policy statement that no individual employee is authorized to act on or respond to any form of judicial order (whether law enforcement or intelligence) but instead must immediately contact and refer the matter to the library director and legal counsel.

G. THE USE OF NEW AND PROPOSED JUDICIAL PROCESS

As we have considered, public concerns focus on only a minority of the USA PATRIOT Act changes to the law of judicial process. Nevertheless, the concerns are real, both from the perspective of the changes to accepted norms of patron and student privacy and the unknown scope of application that raises fear of untoward use. Indeed, the breadth of opposition has not been insignificant. To date, nearly two hundred local jurisdictions and three states have passed laws opposing the

access to individual specific banking and credit records. The Right to Financial Privacy Act of 1978 is found at Pub. L. No. 95-630, 92 Stat. 3697 (1978) (codified as amended at 12 U.S.C.A. §§ 3401–3422 (2001 & West Supp. 2003)).

153. *See* 18 U.S.C.A. § 2709 (2000 & West Supp. 2003). This section of the ECPA allows for access to certain telephone and electronic communications records—limited to subscriber information and toll billing records.

154. *See* 15 U.S.C.A. § 1681u (1998 & West Supp. 2003). The Fair Credit Reporting Act can be found at Pub. L. No. 90-321, 82 Stat. 146 (1968), as added Pub. L. No. 91-508, 84 Stat. 1127 (1970) (codified as amended at 15 U.S.C.A. §§ 1681, 1681a-1681t (1998 & West Supp. 2003)). This section of the FCRA allows for access to names and addresses of all financial institutions at which a consumer maintains or has maintained an account, and identifying information respecting a consumer—limited to name, address, former addresses, places of employment, or former places of employment. *Id.* Note that the FCRA data provides the input to the RFPA that is the authority by which the FBI can access an individual's institution-specific banking and credit records.

155. USA PATRIOT Act § 505(c), 115 Stat. 272, 366 (codified at 15 U.S.C.A. § 1681u).

156. Letter from Jamie E. Brown, Acting Assistant Attorney General, to Chairman F. James Sensenbrenner, Jr. (May 13, 2003), *available at* http://www.lifeandliberty.gov/subs/congress/hjcpatriotwcover051303final.pdf.

USA PATRIOT Act in various ways,[157] and several Freedom of Information Act[158] and other lawsuits have been filed to learn more about the use of the authorities (but have been generally unsuccessful).[159] Senator Orrin Hatch and Representative James Sensenbrenner, Chairmen, respectively, of the Senate and House Judiciary Committees, have refused to endorse additional powers,[160] the House has passed the Otter Amendment to deny funding to execute any delayed notice (otherwise known as sneak-and-peek) search warrants,[161] and a host of other legislation is pending that would restrict USA PATRIOT Act authorities.[162]

157. Bill of Rights Defense Committee, Local Efforts, *available at* http://www.bordc.org/OtherLocalEfforts.htm (last visited Mar. 31, 2004). Such ordinances banning cooperation with federal officials enforcing the USA Patriot Act are largely symbolic given federal supremacy. Dan Eggen, *Patriot Monitoring Claims Dismissed*, WASH. POST, Sept. 19, 2003, at A2.

158. The FOIA cases include one brought by a group of plaintiffs including the ACLU, Electronic Privacy Information Center, American Booksellers Foundation for Free Expression, and Freedom To Read Foundation. ACLU v. U.S. Dep't of Justice, 265 F. Supp.2d 20 (D.D.C. 2003). The plaintiffs sought the number of subpoenas or other legal demands for bookstore and library records issued under the USA PATRIOT Act. *Id.* at 21. The FOIA request was made in August 2002, and the lawsuit based on failure to respond was filed in October. *Id.* at 25. In May 2003, after the release of a few highly redacted, non-substantive documents, the D.C. District Court granted the DOJ's motion for partial summary judgment and the motion for summary judgment filed on behalf of the Federal Bureau of Investigation ("FBI") by the DOJ were granted; plaintiffs' cross-motion for summary judgment was denied. *Id*. at 35.

In another case, the Center for National Security Studies ("CNSS") and others also sued under FOIA for the names of the September 11 detainees. Ctr. for Nat'l Sec. Studies v. U.S. Dep't of Justice, 331 F.3d 918, 922 (D.C. Cir. 2003). The district judge hearing the case ordered release in August 2002 but stayed his decision pending appeal. *Id.* at 925. In early June 2003, the U.S. Court of Appeals for the D.C. Circuit reversed in a somewhat bitter 2-1 decision with the majority holding that the release "would give terrorist organizations a composite picture of the government investigation" and harm national security. *Id.* at 928. The minority found that the withholding "eviscerates" FOIA and our well-established principles of openness. *Id.* at 937.

159. Primary examples here are the cases concerning the blanket closure of immigration proceedings with divergent opinions. N. Jersey Media Group, Inc. v. Ashcroft, 308 F.3d 198 (3rd Cir. 2002), *cert denied*, 538 U.S. ___, 123 S.Ct. 2215 (May 27, 2003) (finding closure appropriate); Detroit Free Press v. Ashcroft, 303 F.3d 681 (6th Cir. 2002) (finding closure inappropriate). Although arriving at opposite findings, the focus in both was the two-part "experience and logic" test established by the Supreme Court in *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555 (1980), that considered whether specific types of proceedings have traditionally been open to the public and whether openness plays a significant positive role in this process. In these two cases, the U.S. Supreme Court denied review, at the urging of the Department of Justice primarily because most of the immigration cases had been concluded.

160. Eggen, *supra* note 157.

161. As considered previously, there is a long history of such warrants that have been consistently approved by the courts over the years.

162. For example, the Freedom to Read Protection Act of 2003, H.R. 1157, 108th Cong. (2003), would eliminate Section 215 business record FISA orders directed toward libraries and bookstores but would still allow criminal warrants and subpoenas as well as FISA search and intercept warrants. The bill has 129 co-sponsors as of August 2003, but has been excluded from immediate legislative consideration by a procedural move.

The Library, Bookseller, and Personal Records Privacy Act, S. 1507, 108th Cong. (2003), is somewhat similar to H.R. 1157 and would also amend Section 215 by requiring the government to show some individualized suspicion; specifically, the standard would become

The level of public opposition has pressured the Attorney General, in a sharp and politically aggressive speech, to declassify the fact that the Department of Justice has never used Section 215 authority.[163] It is suggested that the speech will do little to quell public opposition given its tone (e.g., *"And so the charges of the hysterics revealed for what they are: castles in the air. Built on misrepresentation. Supported by unfounded fear. Held aloft by hysteria."*).[164] The failure to address related critical issues (it did not comment on use of the NSL or other FISA authority) and the simultaneous Administration proposals for additional powers is discussed below.

1. The New Proposed Authorities

To understand the most recent proposals, we must recall the February 2003 draft legislation prepared by the Department of Justice ("DOJ") that was styled as the Domestic Security Enhancements ("DSE") Act of 2003 (and often referred to as PATRIOT Act II).[165] This proposal was leaked and received substantial media and Congressional criticism. Many of the provisions were extreme, including the authority to revoke citizenship, while others were a panoply of additional authorities that would have substantially increased the power of government surveillance. According to media sources, Representative Sensenbrenner, Chairman of the House Judiciary Committee, and Senator Hatch, Chairman of the Senate Judiciary Committee, *"*deterred*"* the circulation and consideration of this proposed legislation and informed the Attorney General "in no uncertain terms" that such an effort "would be extremely counterproductive."[166]

Nevertheless, certain of the provisions of the abortive DSE Act resurfaced on September 11, 2003, on the second anniversary of the terrorist attacks, when President Bush called on Congress to expand the surveillance powers of the government under the USA PATRIOT Act and "untie the hands of our law enforcement officials."[167] Specifically, the DSE Act sought authority for the

"specific and articulable facts" that warrant an individual being suspected of being "an agent of a foreign power."

The Protecting the Rights of Individuals Act, S. 1552, 108th Cong. (2003), would authorize a substantial roll-back of USA PATRIOT Act authorities by redefining domestic terrorism to protect political protesters, by requiring a higher standard of proof for Section 215 orders, by prohibiting agencies from engaging in data mining without explicit congressional authorization, and by reverting the standard for FISA orders generally to the "primary purpose" of foreign intelligence. *Id.* at 10.

163. Eggen, *supra* note 157.

164. Remarks of Attorney General John Ashcroft, Protecting Life and Liberty, Memphis, Tenn. (Sept. 18, 2003), *available at* http://www.usdoj.gov/ag/speeches/2003/091803memphis remarks.htm.

165. THE DOMESTIC SECURITY ENHANCEMENT ACT OF 2003, draft dated Jan. 9, 2003, *available at* http://www.pbs.org/now/politics/patriot2-hi.pdf (last visited Mar. 31, 2004) [hereinafter DSE ACT].

166. Amy Goldstein, *Fierce Fight over Secrecy, Scope of Law,* WASH. POST, Sept. 8, 2003, at A1.

167. Dana Milbank, *President Asks for Expanded Patriot Act: Authority Sought to Fight Terror*, WASH. POST, Sept. 11, 2003, at A1, *available at* http://www.washingtonpost.com/wp

issuance of administrative subpoenas as well as broadened authority for the denial of bail and the imposition of the death penalty.[168]

While the latter provisions may invoke the most emotional unease, it is the little understood administrative subpoena authority that is most significant to our immediate discussion. With over three hundred existing administrative subpoena authorities it is this breadth of authority and general balance in favor of the government that is of concern with respect to the instant proposal.

The Supreme Court has consistently ruled in favor of a broad interpretation of administrative subpoena usage using a "*reasonableness*" and not a "*probable cause*" analysis that incorporates a substantial deference to the government. The reasonableness or good faith standard requires only that (1) the investigation is conducted for a legitimate purpose, (2) the information requested is relevant to that purpose, (3) the agency does not already have the information sought, and (4) the agency followed its own administrative procedures in issuing the subpoena.[169] As summarized by other courts, the federal judiciary will generally enforce administrative subpoenas unless the information sought is "*plainly incompetent or irrelevant to any lawful purpose of the [requesting official] in the discharge*" of official duties.[170]

This is not to suggest that there are no limits on the authority—although the limits are generally found in the specific enabling statute—and will typically be argued in the context of a Motion to Quash.[171] If there are no violations of the statutory authorization, then the principal opposition would be that the good-faith factors in general were violated by the agency (e.g., there is no legitimate purpose to the underlying investigation) or that the overall requirement of reasonableness was not met because of a failure to balance the public need and personal privacy often given the lack of notice.[172]

While the exact form of the proposed anti-terrorism administrative subpoena authority is unknown at the moment, however, the form provided in the abortive DSE Act at Section 128 would allow the production of any record or tangible item (or the testimony of witnesses), require non-disclosure (i.e., secrecy) by the recipient, and provide for enforcement through the contempt powers of the federal courts.[173] It made no provision for notice to or protection of the privacy of the subject, however. In other words, the proposed administrative subpoena authority would effectively supplant the Section 215 authority (that required at least a perfunctory review by the Foreign Intelligence Surveillance Court) with an equivalent source of power that could be exercised by government law

dyn/articles/A57827-2003Sep10.html.

168. *Id.*

169. United States v. Powell, 379 U.S. 48 (1964).

170. Endicott Johnson Corp. v. Perkins, 317 U.S. 501, 509 (1943) (emphasis added).

171. Of course in the context of a motion to quash there is the baseline question of who has knowledge of the subpoena and thus can mount an opposition. It may well be the case that only the recipient who has the information (and is thus only a custodian for the real person in interest) may have knowledge of the administrative subpoena.

172. Okla. Press Publ'g Co. v. Walling, 327 U.S. 186 (1946).

173. DSE ACT, *supra* note 165.

enforcement or intelligence officers alone.

F. UNDERSTANDING JURISDICTION

1. In General

We have explored, so far, the challenges presented by the daunting array of legal process—intercept orders, search warrants, subpoenas, and even the very obscure National Security Letters—arising under both the law enforcement powers of the government and the intelligence authorities. We now turn to assess the issue of jurisdiction. In this discussion, we will consider the environment of our national capital region—for example, could a Maryland state court (assuming the detective secured a court order of some type) compel a Virginia library to produce evidence? Or could a federal court in Maryland do so if we were concerned with a federal crime? We will see that there is some complexity to the answer depending on the crime at issue, the form of the process, and the specific states involved.

2. Jurisdiction at the Federal Level

The bottom line in our mobile, interconnected society is that a given wrongful activity presents multiple criminal offenses in multiple jurisdictions. This presents opportunities for law enforcement decisions and complexity on the part of those in possession of relevant information.

Assume for the moment in our hypothetical that we have a federal focus. It is U.S. district judges or the appointed magistrates for these districts that hear applications for and issue investigative process. In doing so, there are specific rules as to the reach of its judicial process, some of which were modified by the USA PATRIOT Act.

In general, for documentary evidence such as business records (which may be in paper or electronic form), search warrants are applied for, issued by federal judges, and executed in a given district that has jurisdiction of the offense or property. The first exception with respect to documentary or physical evidence is based on the recognition that we live in a mobile age and hence Rule 41(a) of the Federal Rules of Criminal Procedure permit a federal judge to issue a search warrant for evidence outside the district if "the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed."[174]

The second exception requires that we broaden our consideration of documentary evidence to include electronic communications information and consider the USA PATRIOT Act's several substantive changes within the reach of judicial process. Today, all ECPA-orders for electronic communications information (e.g., search warrants for stored e-mail and voicemail messages as well as court orders for transactional records) are valid nationwide whereas previously,

174. FED. R. CRIM. P. 41(b)(2).

and anachronistically, only wiretap orders were so valid.[175] Additionally, search warrants for documentary or physical evidence in terrorism cases—but only domestic or international terrorism cases (as defined in 18 U.S.C. § 2331)—are now valid nationwide.[176] Both of these enlargements of jurisdiction presume, of course, that the issuing federal court has jurisdiction of the offense. This means that a Maryland federal court could issue an ECPA order valid in Virginia for electronic communications information but not, in general, a search warrant for library business records unless the case involved a terrorism matter.

Moving our discussion from search warrants to subpoenas for documentary evidence (and/or attendance of a witness) in non-terrorism criminal matters, this latter form of process is typically issued by clerks of the court upon application of the government, usually in the context of grand jury proceedings or a trial, or by myriad federal agencies with statutory subpoena authority, or even by defense counsel. The service of such subpoenas are regulated by specific statute, generally with nationwide reach,[177] or by Rule 17 of the Federal Rules of Criminal Procedure.[178] Typically the individual serving a subpoena issued on behalf of the government will be a Deputy U.S. Marshal from your judicial district or a FBI Special Agent. Quite certainly, a federal prosecutor in any state could issue a subpoena for library records in Virginia or anywhere in the United States and require compliance once served on that library. As previously discussed, the choice of the more intrusive search warrant or less intrusive subpoena is left to the discretion of the federal government.

Last, with respect to intelligence investigations, FISA orders of all types are valid nationwide and, in light of USA PATRIOT Act amendments, intercept, pen register, as well as trap and trace orders are "roving" and thus apply to any holder of the information and need not be specifically named.[179] A library or university served with an order under this provision that is not specifically named in the provision may request written or electronic certification from the government attorney that the order applies to the entity.[180]

3. Jurisdiction at the State Level and Inside a Given State

Let us consider examples that represent the two general circumstances of state

175. USA PATRIOT Act § 220, 115 Stat. 272, 291–92 (codified at 18 U.S.C.A. §§ 2703, 2711 (2000 & West Supp. 2003)).

176. USA PATRIOT Act § 219, 115 Stat. at 291 (modifying Fed. R. CRIM. P. 41(b)(3)).

177. *See, e.g.,* 5 U.S.C. app. 3 § 6(a)(4), part of the Inspector General Act, that authorizes the Inspectors general of the various federal agencies to issue administrative subpoenas for any information required for their administrative, civil, or criminal duties; there are approximately three hundred statutes that grant such administrative subpoena authority to various federal agencies and officials.

178. FED. R. CRIM. P. 17.

179. USA PATRIOT Act § 206, 115 Stat. at 282 (codified at 50 U.S.C.A. § 1805 (2003 & West Supp. 2003)), § 214, 115 Stat. at 286–87 (codified at 50 U.S.C.A. §§ 1842, 1843 (2003 & West Supp. 2003)).

180. USA PATRIOT Act § 216, 115 Stat. at 288 (codified at 18 U.S.C.A. § 3123(a)(1) (2000 & West Supp. 2003)).

jurisdiction. Virginia is an example of a state which allows for a wide reach of process in general but also a degree of complexity with respect to electronic communications information. Search warrants may be issued by magistrates who are appointed to given districts as well as general district courts and circuit courts that sit in each county and independent city.[181] While the magistrate or judge may issue a warrant only within his or her geographical jurisdiction, it may be directed to any law enforcement authority—state, city or federal—anywhere in the state of Virginia.[182] For electronic communications search warrants, however, the rules are different: intercept warrants as well as "pen register" and "trap and trace" warrants must be issued by a judge within the jurisdiction where the warrant is to be executed while non-content warrants (e.g., subscriber identifying information) follow the general rule and may be issued by any authority within the state.[183]

Maryland, however, is an example of a state which places certain limitations on the reach of in-state courts. In Maryland there are circuit courts where the jurisdiction and reach of process is limited to the given county. Maryland also has the District where the jurisdiction is state-wide and allows the issuance of a search warrant for execution in any county, however.[184] Thus, a detective located in any Maryland county could secure a valid search warrant for execution on the Eastern Shore, but only from the District Court. As for electronic communications information, the circuit courts are the only courts authorized to issue process for wiretaps,[185] stored communications, and transactional records,[186] as well as "pen register" and "trap and trace" data,[187] and thus geographical limitations apply.

4. Jurisdiction Vis-à-Vis Out-of-State Courts

The enforcement of out-of-state criminal judicial process (e.g., a criminal subpoena for documentary evidence) is often not explicit in state laws and typically proceeds on general common law and constitutional precepts of comity. In numerous cases each year, an out-of-state law enforcement agency must attempt to secure documentary evidence from a witness or institution within another state—in our hypothetical, a Maryland to Virginia reach. In general, the process is that the out-of-state law enforcement agency first obtains a subpoena from a court in its own state, and then requests that the foreign law enforcement agency duplicate the process in a court in the foreign state.[188] In our hypothetical case, the

181. *See* VA. CODE ANN. § 19.2-56 (Michie Supp. 2003)

182. *See id*.; Commonwealth v. Stepp, No. 112 87, 1998 WL 972155 (Va. Cir. Ct. Mar 31, 1998) (holding that a magistrate in Loudoun County where a crime occurred may issue search warrant for execution in Fairfax County).

183. *See* VA. CODE ANN. § 19.2-66 (Michie Supp. 2003) (wiretaps), § 19.2-70.2 (Michie Supp. 2003) (trap and trace), § 19.2-70.3 (2000) (non-content subscriber information).

184. *See, e.g.*, Birchead v. State, 566 A.2d 488 (Md. 1989).

185. *See* MD. CODE ANN., CTS. & JUD. PROC, §§ 10-410–414 (1998).

186. *See id*. §§ 10-4A-01–08 (1989 & Supp. 1994).

187. *See id*. §§ 10-4B-01–05 (2002).

188. *See* Hollis Stambaugh, David Beaupre, Dr. David J. Icove, Richard Baker, Wayne Cassaday, & Wayne P. Williams, *State and Local Enforcement Needs to Combat Electronic Crime*, *in* NAT'L INST. OF JUSTICE, RESEARCH IN BRIEF (Aug. 2000), *available at*

Maryland detective would first seek a court order from a Maryland court in the appropriate county, have that order presented and a similar order entered in Virginia, and have the new Virginia order served by local law enforcement. All in all, the process is tedious but not difficult. In this regard it should be noted that some states are easing this process; for example, in 2003, Delaware enacted a law that permits the Delaware Attorney General to issue a subpoena in any criminal case where the out-of-state agency has obtained a court order from its own state court.[189] It should also be noted that some local law enforcement agencies avoid the complexity of securing out-of-jurisdiction warrants by simply delivering their local warrants to out-of-state businesses. Of course, compliance is voluntary—but it is often successful compliance.

Similar processes—an out-of-state order and application to an in-state court—apply for witnesses in criminal prosecutions but are more explicitly regulated by statute—all U.S. states have adopted a version of the Uniform Act to Secure the Attendance of Witnesses from Without a State in Criminal Proceedings.[190] The Virginia statute is quite typical and provides that when a foreign witness is required by a given state, the authorities in that state shall certify the need under the seal of their court and present that certificate to a court of record where the witness is located and where, after a hearing to determine that the witness is material and necessary and attendance will not cause undue hardship, an appropriate order to appear is issued.[191] A substantially similar process exists in other states.[192]

An interesting question has arisen in several states as to whether this Uniform Act that secures witnesses from outside a state also authorizes the issuance of a subpoena *duces tecum* to compel merely the production of documentary evidence. While principles of comity allow such subpoenas (as we have discussed above), the benefits of statutory authority increase the certainty. Most, if not all, state courts to consider this issue have allowed use of the Uniform Act in this additional manner including those in New York, New Jersey, Massachusetts, West Virginia, Alabama, Florida and Georgia.[193]

---

http://www.ncjrs.org/pdffiles1/nij/183451.pdf; U.S. SEC. AND EXCH. COMM'N, REPORT ON RECIPROCAL SUBPOENA ENFORCEMENT LAWS (Nov. 2000), *available at* http://www.sec.gov/news/studies/subpoenalaw.htm.

189. For example, in 2001, the Delaware legislature enacted SB 142 that streamlines the process by which Delaware law enforcement agencies assist out-of-state law enforcement agencies in gathering documentary evidence in criminal investigations. DEL. CODE ANN. tit. 29, § 2508A (2003). Unlike traditional situations where the out-of-state agency must obtain a warrant or subpoena from a court in its own state, and then have a Delaware police agency duplicate the process in a court in Delaware, the new law will increase efficiency by permitting the Attorney General to issue a subpoena in any criminal case where the out-of-state agency has obtained a court order from its own state court. *Id*.

190. 11 U.L.A. 1 (2003).

191. *See* VA. CODE ANN. §§ 19.2-272–282 (Michie 2000).

192. *See* MD. CODE ANN., CTS. & JUD. PROC. §§ 9-301–307 (1984), as well as *In re California*, 471 A.2d 1141 (Md. Ct. Spec. App. 1984) for a discussion as to how the law and process works.

193. *See, e.g.*, *Ex parte* Simmons, 668 So.2d 901 (Ala. Ct. App. 1995).

H. A NOTE ABOUT CIVIL PROCESS

While our primary focus has been on criminal and intelligence process, we have observed that subpoenas may be issued in civil litigation under the same basic standards—a simple assertion of relevance made by the attorney for a party. Most educational institutions, however, are more likely to receive a civil rather than a criminal demand and thus an understanding of the process in this arena is important. The basic rule is that, as with criminal subpoenas, the receiving party may file a Motion to Quash to seek the approval of a court to not respond.[194]

The critical difference, however, is that in civil process the grounds to object are somewhat more broad than in a criminal context and include: (1) the subpoena seeks privileged information although some privileges are more absolute (e.g., information such as attorney-client communications or public contacting) while others may simply require notice and/or balancing of the equities by a judge based on the terms of the statute establishing the privilege; for schools and libraries this would include student records protected by federal law (i.e., the Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. § 1232g)[195] or patron records protected by state confidentiality statutes;[196] (2) the subpoena is too vague as to what it seeks; (3) the subpoena is overly-broad (i.e., it is a "fishing expedition" and requests information not reasonably calculated to lead to the discovery of admissable evidence); (4) the subpoena is too burdensome (e.g., it would be too costly to fulfill or would require the individual to travel too far); (5) the subpoena does not allow a reasonable time to comply (often set by state statute but argument can also be based on volume, location, or search complexities of the requested records); (6) the person subpoenaed lacks possession of the requested records or the authority to release the records;[197] (7) the subpoena was not properly

194. *See, e.g.,* North Carolina State University Office of Legal Affairs, Guidelines and Forms for Responding to Subpoenas, *available at* http://www.ncsu.edu/legal/legal_topics/subpoenas.php (last visited Mar. 31, 2004).

195. Library records are not specifically mentioned in FERPA, 20 U.S.C. § 1232g, yet many universities interpret these records to be covered as educational records. If requested documents are determined to be educational records (i.e., defined as those records directly related to a student and maintained by an institution or by a party acting for an institution), FERPA requires that the educational institution make a reasonable effort to notify the particular student prior to compliance with a subpoena and give the student an opportunity to assert any legal defense. Although FERPA does not specify the exact amount of notice, decisions have required "sufficient" time and most institutions use a ten business day period. *See, e.g.,* GEORGE MASON UNIV., LEGAL AFFAIRS DEP'T, SUBPOENA GUIDELINES HANDBOOK, 9 (Procedure for Educational Document Requests) (Jan. 22, 1999), *available at* http://www.gmu.edu/facstaff/legal-affairs/handbook.pdf If there is no response (typically the case), the institution responds by releasing the requested records. Non-educational records are not covered by FERPA and must be released immediately unless there is another defense. Such non-educational records include, by way of example, those created or maintained by a law enforcement unit of an educational institution, employee-related records, or policy and administrative-type records.

196. *See*, *e.g.*, 75 ILL. COMP. STAT. ANN. 7011 (2003). In case of library confidentiality statutes, the general practice is to invoke a review of the equities by a judge through filing a motion to quash.

197. Note that many organizations have adopted requlations that specify the processes under

served;[198] and (8) the subpoena was issued by a court without jurisdiction.

In regard to this final objection—jurisdiction—we must also consider the reach of given civil courts and this differs in some respects from our criminal discussion. At the federal level and pursuant to the Federal Rules of Civil Procedure ("FRCP"), civil subpoenas reach anywhere in the state (plus one hundred miles outside) where the specific U.S. District Court sits.[199] It should be noted here that a local federal district court may issue a subpoena relative to a case pending in another federal district. Thus, by way of example in Virginia, a valid subpoena could be received from either the U.S. District Court for the Eastern District of Virginia, the Western District of Virginia and, in some instances (within 100 miles) a neighboring U.S. District Court.[200]

At the state level and within that state, state law controls. Quite typical is the rule in Virginia where civil subpoenas from a given circuit or district court may be directed to the sheriff of and executed in any county, city, or town[201] and, moreover, the sheriff of a given county may serve in any contiguous county or city.[202]

At the out-of-state level, the process is more complicated, but many states, including Virginia and Maryland,[203] have adopted the Uniform Foreign Depositions Act ("UFDA")[204] or similar statutes that generally parallel the equivalent criminal provision—secure the foreign order (to the extent required) and request the local clerk (i.e., file a praecipe) to issue a local subpoena. Additional complexity may arise, however, when the target of the subpoena (e.g., an ISP, an educational institution, or a library) objects to producing the requested records for the out-of-state court. Virginia courts have had some experience in resolving such competing interests. Most recently, the Virginia Supreme Court has decided that four factors must be considered when deciding that the UFDA and principles of comity require enforcement of foreign subpoenas: first, the foreign court must have personal and subject matter jurisdiction of the civil cause of action; second, the procedural and substantive law applied by the foreign court must be reasonably comparable to that of Virginia; third, the foreign court's order must not have been falsely or fraudulently obtained; and, fourth, enforcement of the foreign

which records are released including limitation of that authority to designated senior officials. *See, e.g.,* United States *ex rel*. Touhy v. Ragen, 340 U.S. 462 (1951) (holding that it was appropriate for the Attorney General to prescribe regulations for the production of records in courts pursuant to his statutory responsibility for the custody, use, and preservation of the records, papers, and property of governmental records).

198. *See, e.g.,* FED. R. CIV. P. 4. Generally required is personal service but not always by a law enforcement officer.

199. *See* FED. R. CIV. P. 4(b)(2).

200. *See id.*

201. *See* VA. CODE ANN. § 8.01-292 (Michie 2000).

202. *See id.* § 8.01-295 (Michie 2000).

203. *See id.* §§ 8.01-411, 412 (Michie 2000); MD. CODE ANN., CTS. & JUD. PROC. § 9-401 (2003).

204. The UFDA was approved by the National Conference of Commissioners on Uniform State Laws in 1920 and has been adopted in fourteen states. It was superceded in 1962 by the Uniform Interstate and International Procedures Act (withdrawn 1977), 13 U.L.A. 127 (2004).

court's order must not be contrary to the public policy of Virginia, or prejudice the rights of Virginia or her citizens. These four factors have translated, in cases involving allegedly defamatory statements over the Internet, to decisions that denied enforcement in actions by an anonymous corporation, since there were questions as to the personal jurisdiction,[205] but ordered enforcement in another action by a named corporation where the Virginia court had determined that a valid California cause of action existed and that litigation would not violate Virginia public policy.[206]

J. A NOTE ABOUT PROTECTING ASSETS AND PREVENTING LIABILITY

Beyond judicial process, there are the inextricably intertwined topics of electronic monitoring, authentication, and voluntary disclosure. Views of librarians and education administrators are beginning to change in today's legal climate of growing liability for the misuse of computer resources by patrons, students, and staff. Indeed, this recognition of cybersecurity risk comes from many various sources:

- the news (e.g., eight million credit accounts exposed,[207] thirty thousand financial profiles stolen and sold by insiders,[208] or librarians subject to hostile workplace[209]);
- the expressed legal theories imposing liability (e.g., sexual or racial harassment, negligence based on a duty of due care, negligent hiring, respondent superior, breach of contract, enterprise liability in some

205. AOL v. Anonymous Publicly Traded Co., 542 S.E.2d 377, 383 (Va. 2001).

206. AOL v. Nam Tai Electronics, Inc., 571 S.E.2d 128 (Va. 2002).

207. The accounts included those belonging to Visa, MasterCard, American Express, and Discover, and remains under investigation by the FBI. Fred Katayama, *Hacker hits up to 8M credit cards*, CNN/Money (Feb. 27, 2003), *available at* http://money.cnn.com/2003/02/18/technology/creditcards/.

208. On November 25, 2002, "federal prosecutors charged three men with operating an identity-theft ring that had stolen credit reports of more than 30,000 people—the largest case in history." Alex Salkever, *Some Simple Solutions to Identity Theft*, Business Week Online (Nov. 27, 2002), *available at* http://www.businessweek.com/technology/content/nov2002/tc20021127_4748.htm. The defendants had lawful access to passwords for numerous financial institutions and could thus access, and sell on the side, credit reports in full detail. *Id.* As a result, "the ring allegedly emptied bank accounts, took out loans with stolen identities, and ran up fraudulent charges on credit cards." *Id.* Yet, because of the lack of notice to the parties when their credit records were accessed and new accounts opened, the fraud went undiscovered. *Id*.

209. In May 2002 in a preliminary ruling, the Equal Employment Opportunity Commission ("EEOC") ruled in favor of twelve public librarians in Minneapolis who had filed a complaint alleging that patron downloading of pornography "including bestiality and child molestation" and subjecting librarians and other patrons to view the material "did subject the charging party to a sexually hostile work environment." Lisa Bowman, *Librarians fight porn in their workplace*, CNETNews.com (May 29, 2002), *available at* http://news.com.com/2100-1023-258403.html. The EEOC decision allowed litigation to proceed but the case subsequently settled in August 2003 for a payment of $435,000 and a detailed agreement by the library for Internet use policies including detailed penalties. Steve Brandt, *12 Minneapolis Librarians Settle Internet Porn Case*, MINNEAPOLIS STAR TRIB., Aug. 16, 2003, *available at* http://www.twincities.com/mld/twincities/2003/08/16/news/local/6544664.htm.

states, and, if government, a violation of the federal Privacy Act of 1974 or state equivalents);

- the litigation filed (e.g., the successful action against one of Virginia's largest hospitals[210] as well as the class actions against the Government of Saskatchewan, IBM-Canada,[211] and TriWest Healthcare[212]); and
- the legislation enacted (e.g., effective July 1, 2003, in California, there is required notice to customers of breaches involving credit card, social security, drivers license and bank account numbers[213])

What the above suggests is that all businesses, including libraries and educational institutions, may well incur legal liability for the misuse of their computer facilities by staff or patrons. To mitigate that liability, businesses must exercise due care in securing those assets and preventing harm. While a discussion of the legal theories, including negligence, is beyond the scope of this segment,[214] experts suggest that a requirement of due care can be met by the adoption of appropriate security policies that include "best practices" in the industry, the communication of acceptable use policies with patrons and staff, and the management of both security and acceptable use policies through monitoring and

210. In *Fairfax Hosp. v. Curtis*, 492 S.E.2d 642 (Va. 1997), the Virginia Supreme Court held that a health care provider owes any patient a duty of reasonable care, that such duty includes an obligation to safeguard the confidentiality of information regarding the patient, and that the breach of that duty (in this case by the deliberate acts of the employees) gives rise to an action in tort.

211. The data included 650,000 mutual fund statements including names, addresses, and client account numbers; 180,000 insurance accounts including passwords, social insurance numbers, names, addresses, and other details of life, an unknown number of records of the Saskatchewan Workers' Compensation Board; 10,000 accounts of SaskPower including personal financial information; 3,000 records from the Saskatchewan Ministry of Health including provincial health card numbers and related personal information; 3,000 records of the Saskatchewan Ministry of Transportation containing drivers' license information; and an unknown number of records from the Saskatchewan Ministry of Finance including government employee information. Paul Waldie and Jacquie McNish, *Missing Computer Disk Spurs Suit; Class Action Alleges Defendants Negligent*, TORONTO GLOBE AND MAIL, Feb. 3, 2003, at B1.

212. The class action lawsuit, alleging violations of the Privacy Act, breach of contract and negligence, charges that hard drives and laptops containing personal information were stolen from TriWest containing personal information on 500,000 military personnel was stolen. Dennis Wagner, *Lawsuit Accuses TriWest Healthcare of Negligence,* ARIZONA REPUBLIC, Jan. 30, 2002, at B5.

213. *See* CAL. CIV. CODE §§ 1798.29, 1798.82 (West Supp. 2004). Note that Sen. Dianne Feinstein (D-CA) has introduced S.1350, the Notification of Risk to Personal Data Act, in the U.S. Congress that is substantially similar to the California law and that would require government agencies, commercial entities or individuals that own or license electronic databases containing personal information to notify individuals whose information is stored in those databases when the security of the database is breached. *See* Notification of Risk to Personal Data Act, S.1350, 108th Cong. (2003).

214. Essentially, negligence is defined as a failure to exercise the standard of care that a reasonably prudent person would have exercised in a similar situation. BLACK'S LAW DICTIONARY 1056 (7th ed. 1999). Negligence is a tort grounded in the following elements: duty, breach of duty, causation, and damages. *Id*. In this day of widespread knowledge of the facts and effects of cybercrime, negligence may be ever easier to establish.

authentication.[215] The essential fact is that the facilities of a library or other institution may be used for criminal or other wrongful activity, and the institution must have the legal authority to acquire (on terms they deem appropriate), to act on, and to disseminate such information in order to avoid liability.[216] In the words of Donald Pipkin at Hewlett Packard:

> Dependence on computerized information systems is integral to all aspects of an organization. Information-related problems must be understood and managed, the same as any other business resource. Management must recognize the importance of setting policies, standards, and procedures for the protection of information and allocation of resources to achieve it.[217]

If we accept that visual or electronic monitoring may be a management obligation, several immediate questions are presented including the authority and policies to monitor as well as to make voluntary disclosures of information regarding wrongful acts, and the appropriate notice that should be provided to staff, students, and employees.

The legal authority to monitor and voluntarily disclose flows from the ECPA. The ECPA, as amended, permits a provider to the public to monitor its system for management purposes and to make voluntary disclosures of content and other information (1) as necessary to protect the property of the provider, (2) if related to the commission of a crime, or (3) if related to an emergency involving immediate danger of death or serious physical injury.[218] It should be noted that this last factor—the emergency authority—was broadened by the USA PATRIOT Act and has been expanded further by the Homeland Security Act. Disclosure is now allowed under the following standards: first, the "immediacy" requirement is eliminated and thus the emergency may be at any point in time and thus more hypothetical; second, the "reasonable belief" requirement is reduced to "good faith" and thus the factual basis can be any information that is perceived as a threat so long as the motivations for the disclosure are not an ill intent; and third, the disclosures may be made to any local, state or federal government entity, not just law enforcement agents.[219]

An institution's policy on monitoring and voluntary disclosure is largely a

215. Chris Mullins, Webcast: Legal Liability for Security Breaches and Minimum Standards of Due Care (2003), *available at* http://archives.neohapsis.com/archives/sans/2003/0026.html.

216. For an excellent survey of electronic monitoring and privacy policy and practices, see U.S. GENERAL ACCOUNTING OFFICE, COMPUTER-USE MONITORING PRACTICES AND POLICIES OF SELECTED COMPANIES (Sept. 2002), *available at* http://www.gao.gov/new.items/d02717.pdf.

217. DONALD PIPKIN, INFORMATION SECURITY: PROTECTING THE GLOBAL ENTERPRISE (2000).

218. The ECPA allows for voluntary disclosure of stored content by public service providers to protect property at § 201, 100 Stat. 1848, 1861 (codified as amended at 18 U.S.C.A. § 2702(b)(5) (2000 & West Supp. 2003)); for crime at § 201, 100 Stat. at 1861 (codified as amended at 18 U.S.C.A. § 2702(b)(6) (2000 & West Supp. 2003)); and for emergency at 18 U.S.C.A. § 2702(b)(7) (West Supp. 2003)).

219. *See* Homeland Security Act of 2002, Pub. L. No. 107-296, § 225(d), 116 Stat. 2135, 2157 (2002) (codified as amended at 18 U.S.C.A. § 2702(b) (2000 & West Supp. 2003)) (Section 225 is known as the Cyber Security Enhancement Act of 2002).

matter of management discretion and decision. One middle ground is to adopt a policy that balances the institution's respect for the privacy of patrons pursuant to a state's library confidentiality statute but also recognizes the responsibility of the library to protect its electronic systems from unauthorized or criminal use by making appropriate referrals to federal and state law enforcement authorities. In essence, such a policy would embody a rule that the institution does not monitor on a routine basis but does reserve the right (1) to monitor as necessary to manage and to protect its systems from unauthorized or criminal use, and (2) to make voluntary disclosures to federal and state law enforcement and national security authorities as deemed appropriate by library management and counsel.

In any event, several additional points are critical with respect to monitoring and disclosure. Private providers and public institutions, with respect to electronic systems provided to employees, may generally monitor and disclose without limitation.[220] As such, privacy, monitoring, and acceptable use policies often differ for employees as compared to public users, such as patrons or students. Moreover, the law and various court decisions have repeatedly emphasized the importance of providing notice as to monitoring for both public and private providers since notice implements the statutory provision of consent.[221] Examples of such notice, which should take the form of both written notice as well as electronic notice (referred to as "bannering" in the sense of an electronic message that appears on user logon and requires "click-through" agreement), follow.

> *Patron Electronic Privacy, Monitoring, and Disclosure Policy*
>
> This public library computer workstation and network ("system") is for authorized members of the public and is subject to the rules specified on our Acceptable Use Policy ("AUP"). As noted, this is a public machine utilizing the unsecured Internet and as such, there should be no expectation of privacy with respect to communications on or use of this system.
>
> In addition, you should note that this library does not routinely inspect, monitor, or disclose content or other user information but may do so in the course of system management and maintenance. Accordingly, your use of this system constitutes consent to monitoring and you are advised that any evidence of criminal activity identified by the monitoring process, including communications content and transmission details, will be disclosed to law enforcement and national defense agencies as appropriate. Any individuals found to be using the network in excess of their authority or contrary to the library AUP are subject to the penalties stated in the AUP and may have all of their activities on the system monitored and recorded to ensure subsequent compliance with policy.
>
> [OPTIONAL] Last, in order to facilitate the management of this

220. *See* ECPA § 201, 100 Stat. at 1860 (codified as amended at 18 U.S.C.A. § 2702(a)(1)–(3) (2000 & West Supp. 2003)).

221. See 18 U.S.C.A. § 2511(2)(c)–(d) (2000) for consent for real-time monitoring; and 18 U.S.C.A. § 2702(b)(1), (c)(1) (2000 & West Supp. 2003) for consent for access to stored content.

computer system, the library has adopted a system of authentication for public users. This step, identical in concept to our materials check-out system, is intended not to ascertain the content of your computer usage but rather to protect our assets and prevent improper usage that may give rise to legal liability. Please refer to the AUP for prohibited activities.

Alternative version with emphasis on privacy:

Patron Electronic Privacy, Monitoring, and Disclosure Policy

This public library computer workstation and network ("system") is for authorized members of the public and is subject to the rules specified on our Acceptable Use Policy ("AUP").

The library's privacy policy respects your use of library resources, and will not release that information unless required to do so by law.

The library does not routinely inspect, monitor or disclose content or other user information but may do so in the course of system management and maintenance. Accordingly, your use of this system constitutes consent to monitoring and you are advised that any evidence of criminal activity identified by the monitoring process, including communications content and transmission details, will be disclosed to law enforcement and national defense agencies as appropriate. In addition, any individuals found to be using the network in excess of their authority or contrary to the library AUP are subject to the penalties stated in the AUP and to having all of their activities on the system monitored and recorded to ensure subsequent compliance with policy.

Employee Electronic Privacy, Monitoring, and Disclosure Policy

This computer workstation and network ("system") is the property of this library and may be used only by designated and authenticated library staff and volunteers. It is the intent of the library that the system be used primarily for library business, although limited personal use primarily during non-duty time is permitted as more fully detailed in our Staff Acceptable Use Policy. In no event is staff authorized to access sexually explicit sites, to conduct commercial activities, or to further any civil or criminal violation of law.

The library reserves the right to monitor use of this system to ensure network security and adherence to library policy as well as to respond to allegations or evidence of suspected employee misuse or misconduct. Your use of this system constitutes consent to monitoring for such purposes as well as to disclosure of results of such monitoring to appropriate federal and state authorities. As such, you should have no expectation of privacy as to any communications on or information stored within this system.

K. MANAGEMENT RESPONSES TO JUDICIAL PROCESSES

Having considered the complex world of legal process, we turn to the issue of the development of a management policy to direct an institutional response to any received judicial process. In other words, whenever judicial process is received, certain questions inevitably are voiced. The first tier relates to the information itself: *Do we collect this information? Have we preserved this information? Must we preserve this information?* The second tier relates to the mechanics of response: *Who should be notified? Are there legal defenses? Who should act on the request? What records should be maintained on the response process?* And beyond judicial process, how should we address the requirement to protect our electronic assets—an effort that may require monitoring and voluntary disclosure of information?

As we shall see, these questions are answered by adopting the following: first, an adequate and proper records management program; second, detailed policy guidance on the process of responding to judicial process that must be communicated well to all employees—realizing that it is often junior personnel who man the front lines; and third, an adequate electronic monitoring and disclosure policy for public and private users.

1. The USA PATRIOT Act and Records Management

We begin our discussion by noting that neither the USA PATRIOT Act nor any other law requires a provider to change its current data retention practices or to reconfigure its system to collect information if presented with judicial process. That said, several factors should be noted. First, the FBI could insist on deployment of its Carnivore system if the provider could not comply with the judicial process. Second, federal authorities may make a formal letter request for the preservation of records and other evidence pursuant to the ECPA at 18 U.S.C. § 2703(f) for electronic communications records. This statute obligates the recipient to preserve the described records ninety days pending receipt of appropriate legal process that would authorize actual release.[222] This statute applies only retrospectively and does not require capture and preservation of new information that arises after the date of this request.[223] The term "obligated," however, should be interpreted as "required" given that the law generally prohibits the destruction of information once notice is given, or one has reason to believe that it has evidentiary value.

2. Developing the Legal and Operational Basis for Library Business

The luxury not to change our data systems does not mean that libraries are free to maintain few, if any, records or, even more, to destroy records on an *ad hoc* or arbitrary basis. We must remember that a library is a business, and often a government entity, and that one critical concept provides the needed foundation for almost every legal and operational activity of a business—an adequate records

222. ECPA § 111(a), 100 Stat. 1848, 1859 (not codified, but published as 18 U.S.C.A. § 2510 note (2000 & West Supp. 2003)).

223. *Id.*

management program ("RMP"). The questions that we have considered thus far present the realization that all too often institutions have neglected to adopt the key element of a RMP—detailed *records control schedules ("RCS")* or *records retention plans* to ensure that records are kept for, and only for, as long as they are needed for operational, legal, fiscal, or historical purposes. Without a RCS, your institution is in legal jeopardy for many reasons—from keeping records too long and endangering patron confidentiality to destroying records on an *ad hoc* basis and risking charges of illegal destruction. Without a detailed RCS, both preserving and destroying records is risky business. Creating a RCS begins with appraisal which is the process by which we evaluate the totality of our physical and electronic records in order to determine their final disposition. Typically, the records are designated as either permanent (so determined by historic value), or temporary where they may be destroyed when no longer needed or after a time period certain (e.g., from one week to sometimes as long as seventy-five years). Also, typically, records that are yet unapprised are treated as permanent—in order to avoid inappropriate destruction—and all appraisal decisions should be approved by the appropriate state archivist.

Essential to the appraisal process are several specific activities. First is the *records inventory*—a review of the agency functions as reflected in its program responsibilities, structure, and authorities. Second, is the designation of *records series*—a convenient way of grouping files to permit their management as a group because they relate to a particular subject or function or have some other relationship arising out of their creation, receipt, or use. Third is the creation of a *file plan*—a day-to-day tool for records managers, as well as program and administrative personnel, to ensure that records are organized and retained as they are created and/or received. And fourth is *scheduling*—the determination and recording of the business and historic value of each record series in terms of time that the records will be retained (i.e., the retention period). The key point in this discussion is that a RCS is not optional administrative overhead, but rather a requirement of law as well as a critical facet of asset management because records are a business asset. Moreover, as we have noted, a RCS is the predicate to responding effectively and legally to any judicially compelled disclosure of records.

All too often, a library believes it maintains a certain level of patron-specific data only to discover its reports reflect more detailed levels of data. Two information technology facts are critical to remember in building an RCS: first, a report (on paper or computer screen) reflects only what a programmer instructed the system to write or display—it does not reflect the totality of the system holdings. Indeed it may not accurately reflect the system holdings given that reports are merely compiled summaries of raw system data and are no more accurate than the work of the programmer that created the report. Second, unless data is overwritten, it can often be recovered even if linkages have been broken and both criminal investigations and civil cases can reach such data. In sum, the RCS is the authority by which every information professional interacts with the information in their charge.

3. A Staff Policy for Judicial Process

We turn to the second management process that is of critical import—a policy to guide staff in the receipt and handling of judicial process. Employees should not be placed in a position of interpreting and responding to process, yet that is exactly what may happen if management does not promulgate a clear and unequivocal policy that only senior management (e.g., the library director) and legal counsel are authorized to receive and act on received judicial process. We also suggest, based on the evidence of best practices, the importance of having a designated "library duty officer" who may be reached by cellular telephone or pager at all times. Such policies have the following key elements: First, no employee is authorized to release library information in response to oral requests by law enforcement officers. Second, to the extent that an officer requests non-confidential and non-library information (e.g., requests whether a person in a photograph has been in your library), the employee may, but is not required to, respond. Third, all written demands for library information (i.e., judicial process of any form) shall be communicated immediately to the site supervisor or, after hours, to the library duty officer. Fourth, any employee who receives or gains access to information that reasonably presents evidence of a past, present, or future crime shall immediately secure that information and inform the site supervisor or, after hours, the library duty officer, and, if such information reasonably suggests an immediate danger of death or serious physical injury, and library management is unavailable, the employee shall contact the local police. A proposed policy follows that presents practical, detailed steps for staff and management:

Protocol for Protecting Library Information and Responding to Judicial Process

I. Oral Requests

1. Library information shall not be released in response to oral requests by law enforcement officers. The term "library information" includes library business information as well as any patron-specific information. The term also includes information in whatever form—whether remembered by employees, maintained in paper or electronic files, or remaining on public computer workstations. Officers making such requests should be informed of this policy and referred to the library director. In all such instances, employees should document the request and contact the site supervisor or library duty officer.

2. To the extent that an officer makes an oral request for non-confidential and non-library information (e.g., requests whether a person in a photograph has been in your library), an employee may, but is not required to, respond. This policy recognizes that, as citizens and library employees, we have an interest in the effective functioning of our law enforcement and intelligence agencies and may wish to cooperate. The subtle distinctions between confidential and non-confidential information and the

ease in which questions may progress to confidential matters, however, suggest caution. If there is any doubt as to what is or is not confidential, the site supervisor, library duty officer, or director should be consulted.

II. Emergency Situations Involving Crime or Physical Danger

3. Information may come to the attention of an employee—orally, visually, or electronically—that reasonably presents evidence of a past, present, or future crime. Such information shall be secured immediately and the site supervisor or library duty officer informed immediately. If such information reasonably suggests an immediate danger of death or serious physical injury, and library management is unavailable, the employee shall contact the local police.

4. Exigent circumstances may permit law enforcement to enter and seize information and equipment from a library without any judicial process. Such rare, warrantless seizures are only appropriate where necessary to prevent the immediate destruction of criminal evidence or in the words of the Department of Justice, "some other consequence improperly frustrating legitimate law enforcement efforts."[224] If such demands are made, allow the officers to proceed but follow the steps below for search warrant procedure. In the alternative, make an agreement to preserve the evidence until a court can evaluate the case and ask for a follow-up letter formalizing the request.

III. Written Demands by Mail or Delivery Service

5. Written requests in the nature of judicial process (or otherwise requesting information) received by mail or delivery service should be forwarded immediately to the library director by fax and receipt confirmed by telephone.

IV. Written Demands Presented in Person by Law Enforcement Personnel; In General

6. Any law enforcement officer (or other individual) presenting judicial process should be invited to a private office by the senior library staff member present. That staff member should request identification—a badge, a current law enforcement agency-issued photo identification credential, and a business card—and should record the name, title, agency, and telephone number of the officer, and request a copy of the process and any associated documents. Verify the credentials with a phone call made to the agency. Use the phone book rather than the number listed on the card.

7. If the document is a subpoena or other form of judicial process

227. SEARCHING AND SEIZING COMPUTERS, *supra* note 111, at 18.

that requires production at a future time, the officer may simply leave a copy. If a signature is requested, inform the officer that you are not authorized to accept service of process and that you will notify the library director and counsel. In all events, the person authorized to and accepting the subpoena should note orally and in writing that "service is accepted in official capacity only."

8. If the document is a search warrant, it will authorize immediate search and seizure and the library must comply with the warrant and instructions of the officer; inform the officer that the library director and counsel will be contacted immediately and request the patience of the officer.

9. Be polite and friendly. It is important that the matter not be treated as adversarial since it is the policy of the library to cooperate, and negotiation of scope of the judicial process can often minimize the intrusion. Remember that many stories of "over-reaching" by law enforcement can be attributed at least in part to a breakdown in communications. Do not consent to release a greater scope of records than the warrant authorizes.

10. The officer may inform you that the terms of the warrant are "secret" or "sealed" and that you may not disclose any information relating to the warrant or execution. This may in fact be correct (if, for instance, the process is issued by the U.S. Foreign Intelligence Surveillance Court or by other courts in particularly sensitive matters) *but it does not preclude notification of the library director and counsel.*

11. If a search warrant has been presented and the law enforcement officer will not wait for the library director and counsel (and IT person if needed), politely remind the officer that the library is an innocent third party and that Constitutional considerations and good faith suggest that a brief delay is appropriate.

12. If the officer still declines to delay, you should carefully inspect the warrant and monitor the search. Remember that the objective is to minimize disruption to the operations of the library but do not impede or obstruct. Take the following steps outlined below in the "Monitoring Search Warrant Execution" section.

V. Monitoring Search Warrant Execution

13. Keep in mind that computer searches may be executed in four basic ways:

- Search the computer and print out a hard copy of particular files at that time (not frequently used because of potential loss of metadata and other information);

- Search the computer and make an electronic copy of particular files at that time;
- Create a duplicate electronic copy of the entire storage device on-site, and then later re-create a working copy of the storage device off-site for review; and
- Seize the equipment, remove it from the premises, and review its contents off-site.

14. Keep in mind that the option selected depends significantly on the role of the computer hardware in the offense:

- If the hardware is itself evidence, an instrumentality, contraband, or a fruit of crime, law enforcement officers will usually plan to seize the hardware and search its contents off-site—this would not be typical of a library environment; and
- If the hardware is merely a storage device for evidence, officers generally will only seize the hardware if less disruptive alternatives are not feasible.

15. Keep in mind two additional facts:

- Although the warrant may speak in terms of information and it is generally the policy of law enforcement to proceed in the least intrusive manner possible, the commingling of target information with other information can justify the seizure of a larger body of records whether in physical or electronic form;
- Moreover, the execution of a search may result in the "plain sight" identification of additional information and seizure if it meets a "probable cause" standard.

16. In any circumstance, however, while the library official on site may object to actions believed in excess of the terms of the warrant, he or she can do nothing to prevent the officers from seizing information deemed appropriate.

17. Undertake the following specific steps:

- Enlist the assistance of one other senior member of the staff to work with and accompany you in order to record and remember relevant facts and events;
- Ensure that the warrant is signed by a magistrate or judge;
- Note exactly what records or items are authorized to be seized; and
- Volunteer to assist the officer by locating the information, enlisting the assistance of those on the staff who are knowledgeable, and offering to provide copies of electronic information in lieu of seizure of hardware. If

recordable media is seized, request the opportunity to make copies before it is removed;

18. Whether or not the officer accepts your offer of assistance, you should monitor the search and seizure process:

- Note areas and rooms entered, files and computers inspected, and/or specific actions taken;
- Attempt to make copies of all records seized;
- Note and advise the officer if information is being seized that appears to be in excess of that authorized by the warrant;
- Note and advise the officer if information is being seized that is privileged (e.g., patron specific information, employee records, or attorney/client) and ask that it be so marked;

19. At the conclusion of the search, the officer should typically provide an inventory; if not, request a copy but do not sign any statement that the inventory is accurate or complete.

20. Whether or not the judicial process is secret or sealed, ask all involved staff not to discuss the matter with the media, patrons, family or other employees since decisions in this regard must be made by the library director and counsel.

L. REFLECTIONS

What is the realistic extent of the impact of judicial process from law enforcement and intelligence authorities on information professionals, educators, and librarians? While the exact impact is difficult to ascertain given that there are no centralized records of law enforcement orders and FISA orders are secret, since September 11, 2001, there has been extensive use of the government powers against schools and libraries. According to the ACLU, citing the American Association of Collegiate Registrars and Admissions Officers, over 200 colleges have received and disclosed information post-USA PATRIOT Act (e.g., Harvard, Texas and Cornell), although the specific statutory authority for the disclosure was not specified.[225] Others, including a few libraries (i.e., Queens Borough), have acknowledged receiving FISA orders.[226] Many more orders, perhaps numbering in the thousands, have been served on ISPs and portals including AOL and Yahoo!.[227] By way of another measure of demands under any form of authority,

225. ACLU, *USA Patriot Act Boosts Government Powers While Cutting Back on Traditional Checks and Balances: An ACLU Legislative Analysis* (Nov. 1, 2001), *available at* http://www.tratical.com/tratville/CAH/110101a.html.

226. Christopher Dreher, *He Knows What You've Been Checking Out* (Mar. 6 2002), *available at* http://archive.salon.com/news/feature/2002/03/06/libraries/index_np.html.

227. *See* Eunice Moscoso, *Feds Demanding More Information About Companies' Customers*, ATLANTA J.-CONST., Aug. 17, 2003, *available at* http://www.ajc.com/business/0803/

the University of Illinois surveyed 1,020 public libraries in January and February of 2004 and found that slightly more than 10% had been asked by law enforcement officers for information about patrons.[228] What is certain and necessary is the need to build a relationship between librarians and legal counsel—whether private or local government—since the receipt of judicial process is not the time to begin that effort.

There is also a second question relating to impact. What does this complex world of judicial process mean for us in management terms? We considered three of the most critical—an adequate records management plan, an institutional policy regulating response to judicial process, and a policy defining electronic asset management (i.e., whether an institution will reserve the right to monitor computer use in order to detect activity that is illegal and may impose institutional liability).

Out of all of this comes a third question. How do we make this all work? One answer is the availability of negotiation as to the scope and execution of any orders with government law enforcement officers. Generally, law enforcement and intelligence officials are willing to discuss the ability of a library to respond in a manner that is reasonable and does not unduly disrupt its operations. If we understand our rights and obligations, as well as the technical options, the ability to reach a mutually agreeable solution is often assured. A second answer involves the importance of good public relations when dealing with such matters. The imbroglios resulting from statements by information professionals in the aftermath of September 11 demonstrate a continual emphasis that the legal rules we have considered exist to balance individual Constitutional rights and effective law enforcement. When librarians and counsel work together, both objectives may be met.

17patriot.html; Miles Benson, Newhouse News Service, *In the Name of Homeland Security, Telecom Firms are Deluged with Subpoenas*, *available at* http://www.newhouse.com/archive/story1a041002.html (last visited Mar. 31, 2004).

228. *See* Leigh S. Estabrook, *PUBLIC LIBRARIES AND CIVIL LIBERTIES: A Profession Divided*, *available at* http://www.lis.uiuc.edu/gslis/research/civil_liberties.html (last modified Jan. 22, 2003).