

# **The USA Patriot Act in the Library**

## **Background**

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA Patriot Act”) became law on October 26, 2001. The legislation originated with Attorney General John Ashcroft, who asked Congress for additional powers that he claimed were needed to fight terrorism in the wake of the events of September 11, 2001. Few amendments were made to Ashcroft’s initial proposal to Congress, and the bill became law without any hearings or markup by a Congressional committee.

The Patriot Act amended over 15 federal statutes, including the laws governing criminal procedure, computer fraud and abuse, foreign intelligence, wiretapping, immigration, and the laws governing the privacy of student records. These amendments expanded the authority of the Federal Bureau of Investigation and law enforcement to gain access to business records, medical records, educational records and library records, including stored electronic data and communications. It also expanded the laws governing wiretaps and “trap and trace” phone devices to Internet and electronic communications. These enhanced surveillance procedures pose the greatest challenge to privacy and confidentiality in the library.

## **Enhanced Surveillance Provisions Affecting Library Confidentiality**

### **Section 215 Access to Records Under Foreign Intelligence Security Act (FISA)**

- Allows an FBI agent to obtain a search warrant for “any tangible thing,” which can include books, records, papers, floppy disks, data tapes, and computers with hard drives.
- Permits the FBI to compel production of library circulation records, Internet use records, and registration information stored in any medium.
- Does not require the agent to demonstrate “probable cause,” the existence of specific facts to support the belief that a crime has been committed or that the items sought are evidence of a crime. Instead, the agent only needs to claim that he believes that the records he wants may be related to an ongoing investigation related to terrorism or intelligence activities, a very low legal standard.
- Libraries or librarians served with a search warrant issued under FISA rules may not disclose, under of penalty of law, the existence of the warrant or the fact that records were produced as a result of the warrant. A patron cannot be told that his or her records were given to the FBI or that he or she is the subject of an FBI investigation.
- Overrides state library confidentiality laws protecting library records.

Codified in law at 50 U.S.C. §1862.

### Section 216: Relating to the Use of Pen Register and Trap and Trace Devices

- Extends the telephone monitoring laws (“pen register,” “trap and trace”) to include routing and addressing information for all Internet traffic, including email addresses, IP addresses, and URLs of web pages.
- State law enforcement agencies may apply for and obtain an order under this provision, which is not limited to the investigation of terrorism or foreign intelligence matters.
- Federal agents can obtain a nationwide court order for a wiretap from any federal court having jurisdiction over the offense under investigation.
- The officers and agents seeking warrants under the pen register statute only need to affirm that the information sought is relevant to a criminal investigation.
- Compels a recipient of a monitoring order to provide all necessary cooperation to law enforcement authorities to facilitate installation of the monitoring device, or provide the information to the investigating officer from their own records. The recipient cannot disclose that communications are being monitored.
- Libraries that provide access to the Internet and email service to patrons may become the target of a court order requiring the library to cooperate in the monitoring of a user’s electronic communications sent through the library’s computers or network.

Codified in law at 18 U.S.C. §§3121-3127

### Section 214 Pen Register and trap and trace authority under FISA

- Extends the FBI’s telephone monitoring authority in FISA investigations (“pen register,” “trap and trace”) to include routing and addressing information for all Internet traffic, including email addresses, IP addresses, and URLs of web pages.
- As with Section 215, the agent only needs to claim that he believes that the records he wants may be related to an ongoing investigation related to terrorism or intelligence activities, a very low legal standard.
- As with Section 216, libraries that provide access to the Internet and email service to patrons may become the target of a court order.

Codified in law at 50 U.S.C. §1852

## **Other Provisions of Interest That Do Not Directly Affect Libraries**

### Section 218: Foreign intelligence information requirement for FISA authority.

- Amends FISA so that foreign intelligence or terrorism need only be "a significant purpose" of the investigation, rather than "the purpose" of the investigation. Relaxes the legal standard for FISA surveillance.

### Section 219: Single-Jurisdiction Warrants for Terrorism

### Section 220: National Search Warrants for Electronic Evidence

- Both provisions permit federal courts located in a district where a crime or act of terrorism has occurred to issue a court order that may be served and executed nationwide. Section 220 affects stored email and other electronic data.

### Section 206: Roving Surveillance Authority under FISA

- Permits the use of "roving wiretaps" in a FISA investigation, which allows the investigating agency to obtain a single court order to monitor the electronic communications of a person at any location or on any device, including email and Internet communications.
- The order need not identify the person or entity whose assistance is required for the monitoring. It is a generic order that may be presented at any time to a newly discovered service provider.
- Updates FISA to match federal wiretap laws that allow roving wiretaps.

---

<http://www.ala.org/alaorg/oif/usapatriotlibrary.html>

American Library Association  
Office for Intellectual Freedom  
April 2002