

Updates to Chapter on Privacy in Cyberspace (3): FISA, FISC, USAPATRIOT, Libraries

M. E. Kabay, PhD, CISSP-ISSMP

Here's yet more new material I just added in another marathon editing task, working on updating a chapter about privacy that had not been updated since 2008.

Foreign Intelligence Surveillance Act and Court

The Foreign Intelligence Surveillance Court (FISC) was established in 1978 as part of the Foreign Intelligence Surveillance Act (FISA). The Federal Judicial Center of the US government describes the origin and functioning of FISC and FISA as follows:

Congress in 1978 established the Foreign Intelligence Surveillance Court as a special court and authorized the Chief Justice of the United States to designate seven federal district court judges to review applications for warrants related to national security investigations. Judges serve for staggered, non-renewable terms of no more than seven years, and until 2001 were drawn from different judicial circuits. The provisions for the court were part of the Foreign Intelligence Surveillance Act (92 Stat. 1783), which required the government, before it commenced certain kinds of intelligence gathering operations within the United States, to obtain a judicial warrant similar to that required in criminal investigations. The legislation was a response to a report of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the "Church Committee"), which detailed allegations of executive branch abuses of its authority to conduct domestic electronic surveillance in the interest of national security. Congress also was responding to the Supreme Court's suggestion in a 1972 case that under the Fourth Amendment some kind of judicial warrant might be required to conduct national security related investigations.

Warrant applications under the Foreign Intelligence Surveillance Act are drafted by attorneys in the General Counsel's Office at the National Security Agency at the request of an officer of one of the federal intelligence agencies. Each application must contain the Attorney General's certification that the target of the proposed surveillance is either a "foreign power" or "the agent of a foreign power" and, in the case of a U.S. citizen or resident alien, that the target may be involved in the commission of a crime.

The judges of the Foreign Intelligence Surveillance Court travel to Washington, D.C., to hear warrant applications on a rotating basis. To ensure that the court can convene on short notice, at least one of the judges is required to be a member of the U.S. District Court for the District of Columbia. The act of 1978 also established a Foreign Intelligence Surveillance Court of Review, presided over by three district or appeals court judges designated by the Chief Justice, to review, at the government's request, the decisions of the Foreign Intelligence Surveillance Court. Because of the almost perfect record of the Department of Justice in obtaining the surveillance warrants and other powers it requested from the Foreign Intelligence Surveillance Court, the review court had no occasion to meet until 2002. The USA Patriot Act of 2001 (115 Stat. 272) expanded the time periods for which the Foreign Intelligence Surveillance Court can authorize surveillance and increased the number of judges serving the court from seven to eleven. The eleven judges must be drawn from at least seven judicial circuits, and no fewer than three are to reside within twenty miles of the District of Columbia.[12]

Privacy Updates

In response to severe criticism by civil-liberties proponents, additional legislation was passed in 2007 and 2008 to strengthen the Executive Branch's powers to order wide-reaching surveillance without prior approval of the FISC.[13]

USAPATRIOT Act

The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (USAPATRIOT) Act, whose name was crafted to result in the positive-sounding acronym, was passed with minimal legislative review in October 2001 as a reaction to the terrorist attacks of September 11, 2001.[14]

The Electronic Frontier Foundation, a civil-liberties organization, summarizes its perception of the threats in the USAPATRIOT Act to online civil liberties as follows:

- The law dramatically expands the ability of states and the Federal Government to conduct surveillance of American citizens. The Government can monitor an individual's web surfing records, use roving wiretaps to monitor phone calls made by individuals "proximate" to the primary person being tapped, access Internet Service Provider records, and monitor the private records of people involved in legitimate protests.
- PATRIOT is not limited to terrorism. The Government can add samples to DNA databases for individuals convicted of "any crime of violence." Government spying on suspected computer trespassers (not just terrorist suspects) requires no court order. Wiretaps are now allowed for any suspected violation of the Computer Fraud and Abuse Act, offering possibilities for Government spying on any computer user.
- Foreign and domestic intelligence agencies can more easily spy on Americans. Powers under the existing Foreign Intelligence Surveillance Act (FISA) have been broadened to allow for increased surveillance opportunities. FISA standards are lower than the constitutional standard applied by the courts in regular investigations. PATRIOT partially repeals legislation enacted in the 1970s that prohibited pervasive surveillance of Americans.
- PATRIOT eliminates Government accountability. While PATRIOT freely eliminates privacy rights for individual Americans, it creates more secrecy for Government activities, making it extremely difficult to know about actions the Government is taking.
- PATRIOT authorizes the use of "sneak and peek" search warrants in connection with any federal crime, including misdemeanors. A "sneak and peek" warrant authorizes law enforcement officers to enter private premises without the occupant's permission or knowledge and without informing the occupant that such a search was conducted.
- The Department of Justice, with little input from Congress and the American people, is developing follow-on legislation - the Domestic Security Enhancement Act (nicknamed Patriot II) -- which would greatly expand PATRIOT's already sweeping powers.[15]

The law firm of Kelly/Warner has published an excellent summary of the COPPA provisions.[16]

Privacy of Activity in Libraries and Bookshops

In sharp contrast with the privacy provisions of privacy protections for cable television and video rentals and sales discussed in previous sections of this chapter, the USAPATRIOT Act specifically allows intelligence and law enforcement agencies to monitor the use of libraries and booksellers by patrons. Specifically, librarians are required to submit detailed borrowing records on demand and may not reveal that these records were surrendered.

The Patriot Act permits federal agents to secretly obtain information from booksellers and librarians about customers' and patrons' reading, internet and book-buying habits, merely by alleging that the records are relevant to an anti-terrorism investigation. The act prohibits librarians and booksellers from revealing these requests, so they cannot be challenged in court. . . . A University of Illinois study . . . concludes that federal agents have sought records from about 220 libraries nationwide since September 2001 . . . [as of January 2002]. The Justice Department refuses to say how many times it has invoked this Patriot Act provision . . . But Assistant Attorney General Daniel Bryant says that people who borrow or buy books surrender their right of privacy. . . . Some libraries and bookstores unhappy with the law begin to fight back in a number of ways. Some libraries have posted signs warning that the government may be monitoring their users' reading habits. . . . Thousands of libraries are destroying records so agents have nothing to seize. . . . Many librarians polled say they would break the law and deny orders to disclose reading records.[17]

The American Library Association explains their perspective on why the provisions matter to the public:

Libraries are key sources of information on all kinds of subjects and from all perspectives for their communities. Reading has always been one of our greatest freedoms. The written word is the natural medium for the new idea and the untried voice from which come the original contributions to social growth.

Libraries provide a place to exercise intellectual freedom: a free and open exchange of knowledge and information where individuals may exercise freedom of inquiry as well as a right to privacy in regards to information they seek. Privacy is essential to the exercise of free speech, free thought, and free association. In a library, the subject of users' interests should not be examined or scrutinized by others.

The ALA believes certain sections of the USA PATRIOT Act endanger constitutional rights and privacy rights of library users. Libraries cooperate with law enforcement when presented with a lawful court order to obtain specific information about specific patrons; however, the library profession is concerned some provisions in the USA PATRIOT Act go beyond the traditional methods of seeking information from libraries.[18]

ENDNOTES

- [12] http://www.fjc.gov/history/home.nsf/page/courts_special_fisc.html
- [13] “Beyond FISA.” Electronic Frontier Foundation (2013).
<https://ssd.eff.org/foreign/beyond-fisa>
- [14] “The USA PATRIOT Act.” Electronic Frontier Foundation (2005-08-03).
<http://w2.eff.org/patriot/>
- [15] “How PATRIOT Threatens Online Civil Liberties.” Electronic Frontier Foundation (2013). <http://w2.eff.org/patriot/why.php>
- [16] Kelly/Warner Internet Law & Defamation Practice. “COPPA: Children’s Online Privacy Protection Act Summary.” (2012). <http://www.aaronkellylaw.com/coppa-childrens-online-privacy-protection-act-summary/>
- [17] “January 2002: Study Finds Agents Have Sought Records From 220 Libraries.” Profile: USA Patriot Act, History Commons (2002).
http://www.historycommons.org/entity.jsp?entity=patriot_act
- [18] “The USA PATRIOT Act.” American Library Association (2013).
<http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact>

* * *

M. E. Kabay, < <mailto:mekabay@gmail.com> > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials. < <http://www.mekabay.com/> >