Order No. EBTER130
Updated July 26, 2004

Congressional Research Service

Terrorism:

Wiretapping Authority
Charles Doyle

Issue Definition

The terrorist attacks of September 11 stimulated calls to give federal authorities greater wiretapping authority for both criminal and intelligence investigation purposes that culminated in the passage of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act. Congress made further adjustments in the Intelligence Authorization Act for Fiscal Year 2002, the 21st Century Department of Justice Appropriations Authorization Act, and the law creating the Department of Homeland Security. A fourth piece of legislation, S. 113, has passed the Senate. On the administrative front, the Department of Justice has announced amendments to Bureau of Prison regulations under which attorney-client communications of imprisoned and otherwise detained inmates may be monitored in a limited number of cases involving the threat of violence or terrorism, 66 *Fed.Reg.* 55061 (October 31, 2001).

Current Legal Authority

The Fourth Amendment to the United States Constitution regulates government searches and seizures. The Amendment applies only where there is a justifiable expectation of privacy, *Kyllo v. United States*, 533 U.S. 27, 32-3 (2001). Thus, it generally does not apply to information compiled by, or entrusted to, others, *Smith v. Maryland*, 442 U.S. 735, 741-43 (1979) (telephone company information on the source of calls placed to and from a particular telephone); *United States v. Miller*, 425 U.S. 435, 443 (1976) (bank records of customer transactions). Nevertheless, Congress has authority to provide broader protection by statute.

Congress has passed laws that implement and augment Fourth Amendment protection in the area of communications privacy, while authorizing law enforcement and foreign intelligence gathering activities under judicial supervision. In the case of criminal investigations, it has established a three tier system. The most protective guards private conversations, 18 U.S.C. 2510-2522 ("Title III"); the next, telephone records and computer communications (e.g., e-mail), 18 U.S.C. 2701-2709; and the third, the identification of parties to a private conversation, 18 U.S.C. 3121-3127 ("pen registers" and "trap and trace devices"). Congress has created an even more protective scheme for similar activity conducted in the United States for foreign intelligence gathering purposes, 50 U.S.C. 1801-1863 (Foreign Intelligence Surveillance Act or "FISA").

Neither the Fourth Amendment nor Title III bar pre-announced monitoring of inmate telephone calls other than those to their attorneys, *United States v. Van Poyck*, 77 F.3d 285, 290-92 (9th Cir. 1996); *Smith v. U.S. Department of Justice*, 251 F.3d 1047, 1050 (D.C.Cir. 2001). The authority

to monitor attorney-client conversations is more uncertain. Pre-trial detainees have a Sixth Amendment right to the assistance of counsel in their defense. They and convicted inmates enjoy a Fifth Amendment due process right to meaningful access to the courts, *Bounds v. Smith*, 430 U.S. 817, 828 (1977). Although neither right protects conspiratorial communications, *United States v. Zolin*, 491 U.S. 554, 462-63 (1989); *cf., Cody v. Weber*, 256 F.3d 764, 769 (8th Cir. 2001), it is a close question whether they permit the government to bar attorney-client communications in the absence of even a confidential government participant, *see Weatherford v. Bursey*, 429 U.S. 545 (1977).

Legislation: Proposals and Analysis

P.L. 107-56, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act makes a number of adjustments in Title III, the telephone records/ computer communications sections, the pen register/trap and trace sections, and FISA. The adjustments (several of which apply only to foreign intelligence investigations initiated before January 1, 2006, or to the criminal investigation of misconduct occurring before that date):

- Permit use of the pen register/trap and trace procedure to determine the sender and addressees of computer communications, with a reporting requirement to ensure that no computer communications content is captured in the process;

- Permit use of the computer communications/telephone records procedure to secretly gain access to voice-mail. This eases standards for accessing voice-mail, which is now controlled by the more restrictive procedures of Title III;

- Allow disclosure of the results a Title III interception that produces foreign intelligence or counterintelligence information to federal law enforcement, intelligence, protective, immigration, national defense or national security officers for use in the performance of their duties. Disclosure had been limited to law enforcement officers;

- Add several terrorism crimes to the list of federal offenses that will support a Title III order (e.g., providing material support to terrorists or a terrorist organization, use of weapons of mass destruction, terrorist acts of violence against Americans overseas);

- Permit interception of a hacker's communications within the invaded computer system;

- Expand the information available under the computer communications/telephone records procedure to include credit card numbers and network addresses;

- Allow federal judges in the districts in which the crime under investigation has occurred to issue orders under the computer

communications/telephone records procedure regardless of the district in which the information is located. Existing law ordinarily requires issuance where the information is located;

- Confirm that the Title III and computer communications/telephone records assistance procedures are equally applicable to cable providers to the extent they provide communication services; and

- Create a claim against the U.S. for federal violations of Title III, FISA, the computer communications/telephone records sections, or the pen register/trap and trace sections, with the possibility of administrative discipline for offending officers.

In the intelligence gathering context, the law contains several FISA amendments and that:

- Allow orders authorizing interception or physical searches to describe in general terms those whose assistance may be required, if the target acts to thwart identification of specific locations. Prior law required that communications carriers, landlords and the like be specifically identified;

- Increase the number of judges assigned to the FISA court from 7 to 11;

- Permit interceptions and searches in which a significant purpose is to gather foreign intelligence. Prior law insisted that intelligence gathering be the exclusive purpose;

- Expand the FISA pen register/trap and trace authority to include orders to determine the identify of the senders and addressees of computer communications;

- Eliminate the requirement that FISA pen register/trap and trace applications, or seeking communication record information, demonstrate that the targeted communications involve a foreign power, an agent of a foreign power, an international terrorist, or one engaged in secret intelligence activities; and

- Authorize court orders to seize any tangible item relevant to a foreign intelligence or international terrorism investigation. Existing law authorizes court orders for business records held by common carriers, public accommodation facilities, storage facilities and car/truck rental agencies.

P.L. 107-108, the Intelligence Authorization Act for FY2002, further amends FISA (1) extending from 24 to 72 hours the permissible duration of an emergency or presidentially ordered, warrantless foreign intelligence surveillance or physical search, and (2) limiting the authority for court ordered access to business records and other tangible items to investigations to obtain foreign intelligence information that does not concern an American (a "U.S. person") (prior law permitted orders regardless of whether the information concerned Americans).

P.L. 107-273, the 21st Century Department of Justice Appropriations Authorization Act, makes it clear that a federal official need not be present when a service provider executes a search warrant for the content customer e-mail or other communications or for customer records in its possession (see also *United States v. Bach*, 310 F.3d 1063 (8th Cir. 2002): search and seizure of defendant's e-mail files from ISP server by its technicians, pursuant to a warrant but in the absence of a federal official, was reasonable for Fourth Amendment purposes).

P.L. 107-296, creating the Department of Homeland Security, also:

- Permits service providers to make good faith disclosures of the content of e-mail and other stored communications in its possession to federal, state, or local governmental entities, when it believes they relate to an emergency involving a danger of death or serious bodily injury; and requires that such disclosures be reported to the Attorney General who in turn is responsible for reporting them to Congress within a year of passage of the act;

- Makes clear that service providers, landlords, and others, who assist authorities in the exercise of their powers under Title III or FISA or the provisions for stored communications and communications records, enjoy immunity from civil liability for their assistance;

- Amends the federal proscription on marketing illegal wiretapping equipment to cover knowingly using the Internet for such advertising purposes;

- Allows senior Justice Department officials to authorize emergency installation of pen registers as well as trap and trace devices (without a prior court order) in cases of immediate threats to national security or of felonious attacks on protected computers systems (in addition to the life threatening and organized crime emergencies that already justified installation without a prior court order);

- Subjects illegal wiretapping of cordless telephone and cellphone conversations to the same criminal penalties that apply to other types of wiretapping;

- Increases the penalties for unlawful access to stored communications so that a simple violation is punishable by imprisonment for not more than 1 year (up from 6 months); a second simple violation by imprisonment for not more than 5 years; and a violation involving commercial gain or advantage, malicious damage, or furtherance of another criminal or tortious act by imprisonment for not more than 5 years for the first offense and not more than 10 years for subsequent convictions (formerly not more than 1 year and not more than 2 years respectively and only in cases of commercial benefit or malice); and

- Authorizes federal law enforcement officers to share the results of a Title III wiretap with federal, foreign, state, or local government law

> enforcement officers (and with foreign, federal, state, or local intelligence officials in the case of foreign treats of terrorism, sabotage, spying or similar hostile acts) for the performance of their duties.

S. 113, which passed the Senate on May 5, 2003, adds lone wolf, foreign terrorists to the list of permissible targets for the exercise of FISA authority. Like several of the USA PATRIOT Act provisions, the amendment would expire on December 30, 2005. Proponents claim the new authority would have permitted a more effective investigation of the activities of Zacarias Moussaoui, the alleged 20th 9/11 hijacker; opponents claim the expansion of authority is unnecessary, *see*, S.Rept. 108-40 (2003).

CRS Products

CRS Report RL30465. *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and Recent Judicial Decisions*.

CRS Report RS21077(pdf). *Monitoring Inmate-Attorney Communications: Sixth Amendment Implications*.

CRS Report 98-326(pdf). *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*. (Also, abridged as CRS Report 98-327(pdf))

CRS Report RS21472. *Proposed Change to the Foreign Intelligence Surveillance Act (FISA) under S. 113*.

CRS Report RL31200(pdf). *Terrorism: Section by Section Analysis of the USA PATRIOT Act*.

CRS Report RL31377. *The USA PATRIOT Act: A Legal Analysis*.

CRS Report RL32186. *USA PATRIOT Act Sunset: Provisions That Expire on December 31, 2005*. (Also, abridged as CRS Report RS21704)

CRS Contacts:
Wiretapping: Gina Stevens (7-2581);
Foreign Intelligence Surveillance Act: Elizabeth Bazan (7-7202); and
Attorney-client communications: T. J. Halstead (7-7981).