USA PATRIOT ACT:
SUNSETS REPORT

APRIL 2005

Introduction:

On October 26, 2001, President Bush signed into law the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act" or "Act"). This legislation, which was passed by both houses of Congress with overwhelming, bipartisan majorities, updated and strengthened laws governing the investigation and prosecution of terrorism within the parameters of our Constitution and our national commitment to the protection of civil rights and civil liberties.

At the end of 2005, sixteen provisions of the USA PATRIOT Act are scheduled to expire: sections 201, 202, 203(b), 203(d), 204, 206, 207, 209, 212, 214, 215, 217, 218, 220, 223, and 225. This report, which was prepared by the Department of Justice at the request of Senator Dianne Feinstein of California, analyzes each of the sixteen provisions. In particular, this report, on a provision-by-provision basis, seeks to: (1) explain how, and the extent to which, these sixteen sections changed the legal landscape, (2) summarize how these sections of the Act have been used by the Department to protect the American people, and (3) survey and analyze any criticisms of the provisions.

In addition to this report, the Department has transmitted many other reports to Congress that provide information explaining in what manner and how frequently the Department has utilized particular USA PATRIOT Act provisions. Most importantly, such information is contained in the semi-annual reports submitted by the Attorney General to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate regarding the Department's use of the Foreign Intelligence Surveillance Act. Six such reports have been submitted to Congress covering the periods in which USA PATRIOT Act authorities were utilized. These reports were transmitted by the Department in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004.

Moreover, section 1001 of the USA PATRIOT Act requires the Department's Office of Inspector General to submit to the House and Senate Judiciary Committees on a semi-annual basis a report detailing any abuses of civil rights and civil liberties by Department employees or officials. To date, six such reports have been submitted by the Office of the Inspector General pursuant to section 1001; these reports were transmitted in July 2002, January 2003, July 2003, January 2004, September 2004, and March 2005. Significantly, the Office of the Inspector General to date has not documented in these reports any abuse of civil rights or civil liberties by the Department related to the use of any substantive provision of the USA PATRIOT Act.

As this report demonstrates, some of the sixteen USA PATRIOT Act provisions that are scheduled to sunset are controversial while others have been subject to little criticism. The Department believes that the criticisms of these particular provisions are misguided and that it is vital that all of these provisions be made permanent so that investigators and prosecutors have the tools they need to protect the American people.

The Department hopes that this report will assist Congress and the American people in evaluating each of these provisions as the important debate over renewing these sixteen sections begins.

Section 201: Authority to Intercept Wire, Oral, and Electronic Communications Relating to Terrorism

Text of Section 201:

> Section 2516(1) of title 18, United States Code, is amended --
>
> > (1) by redesignating paragraph (p), as so redesignated by section 434(2) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132; 110 Stat. 1274), as paragraph (r); and
> >
> > (2) by inserting after paragraph (p), as so redesignated by section 201(3) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (division C of Public Law 104-208; 110 Stat. 3009-565), the following new paragraph:
> >
> > "(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism); or".

How Current Law Now Reads:

> **"§ 2516. Authorization for interception of wire, oral, or electronic communications**
>
> > **(1)** The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—
> >
> > …
> >
> > **(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2332f, 2339A, 2339B, or 2339C of this title (relating to terrorism); or…"**

Analysis:

In the criminal law enforcement context, federal investigators have long been able to obtain court orders to intercept wire communications (voice communications over a phone) and oral communications (voice communications in person) to investigate the predicate offenses listed in federal wiretap statute, 18 U.S.C. § 2516(1). The listed offenses included numerous traditional crimes, including drug crimes, mail fraud, and passport fraud. Prior to the passage of the USA PATRIOT Act, however, certain extremely serious crimes that terrorists are likely to commit – including chemical weapons offenses, killing United States nationals abroad, using weapons of mass destruction, and providing material support to foreign terrorist organizations – were not

listed in 18 U.S.C. § 2516(1). This prevented law enforcement authorities from using many forms of electronic surveillance to investigate these serious criminal offenses. As a result, law enforcement therefore could obtain under appropriate circumstances, a court order to intercept phone communications in a passport fraud investigation but not a chemical weapons investigation or an investigation into the murder of a United States national abroad.

Section 201 of the USA PATRIOT Act ended this anomaly in the law by amending 18 U.S.C. § 2516(1) to add the following to the list of predicate offenses under the criminal wiretap statute: chemical weapons offenses, 18 U.S.C. § 229; certain homicides and other acts of violence against United States nationals occurring outside of the United States, 18 U.S.C. § 2332; use of weapons of mass destruction; 18 U.S.C. § 2332a; violent acts of terrorism transcending national borders, 18 U.S.C. § 2332b; financial transactions with countries which support terrorism, 18 U.S.C. § 2332d; material support of terrorists, 18 U.S.C. § 2339A; and material support of terrorist organizations, 18 U.S.C. § 2339B. Two other predicate offenses were subsequently added to this list by Public Law 107-197 (Implementation of the International Convention for the Suppression of Terrorist Bombings): bombings of places of public use, government facilities, public transportation systems, and infrastructure facilities, 18 U.S.C. § 2332f; and financing of terrorism, 18 U.S.C. § 2339C. As a result, in addition to those offenses added by section 201, if section 201 were allowed to expire at the end of 2005, these two additional offenses may cease to be predicates under the wiretap statute as well.

It is important to point out that section 201 of the USA PATRIOT Act preserved all of the pre-existing standards in the wiretap statute. For example, law enforcement still must: (1) apply for and receive a court order; (2) establish probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (3) establish probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (4) establish that "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous.

Section 201 is extremely valuable to the Justice Department's counterterrorism efforts because it enables investigators to gather information when looking into the full range of terrorism-related crimes. If wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, gambling, and obscenity, then surely investigators should be able to use them when investigating the use of weapons of mass destruction, acts of terrorism transcending national boundaries, and chemical weapons offenses.

Since the passage of the USA PATRIOT Act, Justice Department investigators have utilized section 201 to investigate, among other things, potential weapons of mass destruction offenses as well as the provision of material support to terrorists and foreign terrorist organizations. In total, as of March 10, 2005, the Department had utilized section 201 on four occasions. These four uses occurred in two separate investigations. One of these cases involved an Imperial Wizard of the White Knights of the Ku Klux

Klan, who attempted to purchase hand grenades for the purpose of bombing abortion clinics and was subsequently convicted of numerous explosives and firearms charges.

In part because section 201 preserves all of the preexisting standards for obtaining a wiretap, it has not engendered significant opposition among critics of the USA PATRIOT Act. For example, the Electronic Frontier Foundation (EFF), which has been quite critical of many provisions of the USA PATRIOT Act, has taken the position that it "does not necessarily oppose" the renewal of section 201.[1] In addition, the Center for Democracy & Technology (CDT), which describes itself as "working for civil liberties on the Internet" and has strongly opposed many USA PATRIOT Act provisions, has taken the position that section 201 in its view is not controversial.[2] To be sure, the Electronic Privacy Information Center (EPIC) has noted that "[b]ecause the government already had substantial authority under FISA to obtain a wiretap of a suspected terrorist, the real effect of [section 201] is to permit wiretapping of a United States person suspected of domestic terrorism."[3] It is entirely appropriate, however, to utilize the same surveillance technique in such an investigation as can be used in other criminal investigations. To the extent that there is probable cause to believe that Americans who are not connected to international terrorist groups are planning to use chemical weapons or weapons of mass destruction, it is absolutely vital that the Justice Department have all appropriate tools at its disposal to investigate such conduct.

Section 202: Authority to Intercept Wire, Oral, and Electronic Communications Relating to Computer Fraud and Abuse Offenses

Text of Section 202:

> Section 2516(1)(c) of title 18, United States Code, is amended by striking "and section 1341 (relating to mail fraud)," and inserting "section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse),".

How Current Law Now Reads:

> **"§ 2516. Authorization for interception of wire, oral, or electronic communications**
>
> **(1)** The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of

[1] Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 201, 'Authority to Intercept Wire, Oral, and Electronic Communications Relating to Terrorism,' and Section 805, 'Material Support of Terrorism'", (March 31, 2004) (available at http://www.eff.org/Privacy/Surveillance/Terrorism /PATRIOT/sunset/201.php).

[2] Center for Democracy & Technology. "PATRIOT Act Sunsets", (May 7, 2004) (available at http://www.cdt.org/security/20040507sunsets.pdf).

[3] "EFF and EPIC Analysis Of The USA PATRIOT Act" (available at http://post911timeline.org/USAPA. htm).

Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

…

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 1014 (relating to loans and credit applications generally; renewals and discounts), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3)(relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115(relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), **a felony violation of section 1030 (relating to computer fraud and abuse)**, section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 1992 (relating to wrecking trains), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);”

Analysis:

Just as many traditional terrorism-related offenses were not listed as wiretap predicates in 18 U.S.C. § 2516(1) before passage of the USA PATRIOT Act, neither were many important cybercrime or cyberterrorism offenses. Therefore, while criminal investigators could obtain wiretap orders to monitor wire communications (voice communications over a phone) and oral communications (voice communications in person) to investigate gambling offenses, they could not use such techniques in appropriate cases involving certain serious computer crimes. Section 202 of the USA PATRIOT Act eliminated this anomaly and brought the criminal code up to date with modern technology by adding felony offenses under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, such as computer espionage, extortion, and intentionally damaging a federal government computer, to the list of wiretap predicates in 18 U.S.C. § 2516(1).

As with section 201, section 202 of the USA PATRIOT Act preserved all of the pre-existing standards in the wiretap statute. For example, law enforcement still must: (1) apply for and receive a court order; (2) establish probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (3) establish probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (4) establish that "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous.

As of March 10, 2005, the Justice Department had used section 202 of the USA PATRIOT Act on two occasions. These two uses occurred in a computer fraud investigation that eventually broadened to include drug trafficking.

It is important that section 202 of the USA PATRIOT Act remain available to prosecutors should it be needed in appropriate investigations, such as these. If wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, obscenity, and passport fraud, then surely investigators should be able to use such tools when investigating attempts to damage the computer systems of the federal government. In addition, commentators have noted section 202 benefits Internet service providers (ISPs) by making it "easier for the government to assist them by conducting surveillance related to hacking, denial of service attacks, and related Computer Fraud and Abuse Act (CFAA) violations."[4]

Section 202, like section 201, has not engendered significant opposition. Indeed, the CDT, which has opposed many USA PATRIOT Act provisions, has taken the position that section 202 is not controversial.[5] As one commentator has explained, section 202 "simply modernize[d] the federal police powers in light of the increased

[4] *See* Ronald L. Plesser, James J. Halpert & Emilio W. Cividanes, "USA PATRIOT Act for Internet and Communications Companies", Computer and Internet Lawyer, March 2002.
[5] *See supra* note 2.

importance of telecommunications and digital communications in the economy and society."[6]

Section 203(b): Authority to Share Criminal Investigative Information (Electronic, Wire, and Oral Interception Information)

Text of Section 203(b):

> **(b) AUTHORITY TO SHARE ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION-**
>
> (1) LAW ENFORCEMENT- Section 2517 of title 18, United States Code, is amended by inserting at the end the following:
>
> "(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.".
>
> (2) DEFINITION- Section 2510 of title 18, United States Code, is amended by--
>
> (A) in paragraph (17), by striking "and" after the semicolon;
>
> (B) in paragraph (18), by striking the period and inserting "; and"; and
>
> (C) by inserting at the end the following:
>
> "(19) 'foreign intelligence information' means--
>
> '(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--
>
> '(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> '(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

[6] *See* Jon Garon, "The Electronic Jungle: The Application of Intellectual Property Law to Distance Education," 4 Vand. J. Ent. L. & Prac. 146, 166 (2002).

‘(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

‘(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

‘(i) the national defense or the security of the United States; or

‘(ii) the conduct of the foreign affairs of the United States.”.

How Current Law Now Reads:

“18 U.S.C. § 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

…

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. § 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.”

“18 U.S.C. § 2510. Definitions

…

(17) ‘electronic storage’ means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) ‘aural transfer’ means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) ‘foreign intelligence information’, for purposes of section 2517(6) of this title, means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States."

Analysis:

Before the enactment of the USA PATRIOT Act, federal law was interpreted to limit the ability of federal law enforcement officials to share terrorism-related information derived from certain investigative techniques with national defense officials and members of the intelligence community in order to protect the American people from terrorism. For example, before the Act, federal law was interpreted generally to prohibit federal prosecutors from disclosing information from criminal investigative wiretaps to intelligence and national defense officials even if that information indicated that terrorists were planning a future attack, unless such officials were assisting with the criminal investigation. Consequently, as the 9/11 Congressional Joint Inquiry Report and the report of the 9/11 Commission confirm, our ability to connect the dots and thus prevent terrorist attacks was inhibited by a lack of coordination and information sharing within the federal government.

Section 203(b) of the USA PATRIOT Act was one of the many provisions in the Act designed to alleviate this problem by facilitating information sharing among those federal officials working to prevent terrorist attacks. Because of Section 203(b), when authorities executing a criminal investigative wiretap discover foreign intelligence information, that information may now be passed on to other federal law enforcement, intelligence, protective, immigration, national defense, or national security officials for use in their official duties.

Section 203(b) specifically pertains to information: (1) related to the protection of the United States against a foreign attack or other foreign hostile action, against sabotage or international terrorism by a foreign power or its agents, or against foreign clandestine intelligence activities; (2) concerning a foreign power or territory related to the national defense, security, or foreign affairs activities of the United States; or (3) constituting foreign intelligence or counterintelligence as defined in Section 3 of the National Security Act of 1947 (that is, (a) "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" or (b) "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign

organizations, or foreign persons, or international terrorist activities."). 50 U.S.C. §§ 401a(2), (3)).

Significantly, intelligence information discovered through a criminal investigative wiretap that identifies an American citizen or a permanent resident alien may be shared with other federal officials only pursuant to guidelines mandated by the USA PATRIOT Act and promulgated by the Attorney General.[7]

The Department has made disclosures of vital information to the intelligence community and other federal officials under section 203(b) on many occasions. For example, such disclosures have been used to track terrorists' funding sources and to identify terrorist operatives overseas.

Section 203(b) of the USA PATRIOT Act closed a dangerous gap between criminal investigations and counterterrorism and other national-security investigations. Each restriction on information sharing makes it more difficult for investigators to "connect the dots" to prevent terrorist attacks. Allowing section 203(b) to expire would impede the ability of law enforcement officers to pass along information obtained from wiretaps to other federal officials, including intelligence officers, and thus would help rebuild the "wall" between our law enforcement and intelligence and defense officials that existed before September 11.

Indeed, were section 203(b) allowed to expire, United States law enforcement officers would be allowed to share certain foreign intelligence information collected through criminal investigative wiretaps with foreign intelligence services, such as MI-5, see 18 U.S.C. § 2517(7), but would arguably not be allowed to share that same information with the CIA. Such an outcome would be directly contrary to the spirit of the recently enacted Intelligence Reform and Terrorism Prevention Act of 2004, which included many provisions designed to enhance information sharing within the federal government. While the Homeland Security Act authorized the disclosure of information obtained from such wiretaps to appropriate federal, state, local, and foreign government officials in specified foreign intelligence situations, see 18 U.S.C. § 2517(8), this authority is not as broad as the authority contained in section 203(b).[8] Moreover, allowing section 203(b) and other USA PATRIOT Act provisions that have facilitated information sharing to expire would hinder the ability of Director of National Intelligence

---

[7] *See* Memorandum of the Attorney General, Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons (Sept. 23, 2002) (available at http://www.usdoj.gov/olp/section203.pdf).

[8] Section 203(b) amended 18 U.S.C. § 2517 to allow sharing of information including foreign intelligence, counterintelligence, or foreign intelligence information, as these terms are defined in title 18 and the National Security Act of 1947. 18 U.S.C. § 2517(6). Should section 203(b) sunset, information-sharing would be permissible with respect to only a subset of such information, as specifically defined in section 2517(8), which limits information-sharing to information of "a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat." 18 U.S.C. § 2517(8).

to unify the intelligence community and to assemble a complete picture of terrorism-related information for the President and officials with key national-security and/or homeland-security responsibilities.

Section 203(b) has been subject to criticism from opponents of the USA PATRIOT Act. The ACLU made the most typical objection to the provision on October 23, 2001 (before passage of the USA PATRIOT Act), when it stated that "While some sharing of information may be appropriate in some limited circumstances, it should only be done with strict safeguards. . . . The bill lacks all of these safeguards."[9]

Yet, section 203(b), and the guidelines promulgated for its use, contain precisely the type of safeguards that the provision's critics have advocated. First, Title III itself imposes substantial burdens on law enforcement prior to the collection of the information at issue, greater than that necessary to obtain a search warrant. This provision does not reduce those requirements, but just provides the ability to appropriately share the information after it is collected under court order. Second, on September 23, 2002, the Attorney General issued privacy guidelines governing the sharing of wiretap information that identifies a United States person with the intelligence community. These guidelines provide important safeguards to United States persons identified in information disclosed to the intelligence community under the USA PATRIOT Act. They require that precautions be taken to ensure information is used appropriately, including labeling of all such information before disclosure, and handling the information according to specific protocols designed to ensure its appropriate use. Third, section 203(b) only allows for the sharing of a certain limited class of information gathered under Title III, such information related to national security matters. It does not provide authority to share all information gathered under Title III authority. And fourth, an individual who receives any information under the provision can use it only "in the conduct of that person's official duties."

Section 203(d): Authority to Share Criminal Investigative Information (Foreign Intelligence Information)

Text of Section 203(d):

> (d) FOREIGN INTELLIGENCE INFORMATION.—
>
> > (1) IN GENERAL.—Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

[9] *See* "How the USA PATRIOT Act Puts the CIA Back in the Business of Spying on Americans" (available at http://www.aclu.org/congress/l102301j.html).

(2) DEFINITION.—In this subsection, the term ‘‘foreign intelligence information’’ means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

How Current Law Now Reads:

“50 U.S.C. § 403-5d. Foreign intelligence information

(1) In general

Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 401a of this title) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(2) Definition

In this section, the term ‘foreign intelligence information’ means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States."

Analysis:

Section 203(d) also facilitates information sharing and does so more broadly than section 203(b) by allowing law enforcement officials to share foreign intelligence information obtained as part of a criminal investigation with any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist them in the performance of their official duties. Section 203(d) creates a generic exception to any other law purporting to bar federal law enforcement officials or intelligence, immigration, national defense, or national security officials from receiving, for official use, information regarding foreign intelligence or counterintelligence obtained as part of a criminal investigation.

Section 203(d) has been used by the Department on a regular basis and has been instrumental to the increased coordination and information sharing between intelligence and law enforcement personnel that has taken place in the last three-and-a-half years. This provision, for example, has been utilized to help investigators "connect the dots" and break up terror cells within the United States, such as those in Portland, Oregon, and Lackawanna, New York. It has also been used to revoke suspected terrorists' visas and prevent their reentry into the country.

The provision also contains important safeguards to ensure that it is not misused. A federal official who receives any information under the provision can use it only "in the conduct of that person's official duties." Additionally, that official is bound by "any limitations on the unauthorized disclosure of such information."

The information sharing provisions are overwhelmingly heralded by investigators as the most important provisions of the USA PATRIOT Act. The new ability to share critical information has significantly altered the entire manner in which terrorism investigations are conducted, allowing for a much more coordinated and effective approach than was possible before the passage of the USA PATRIOT Act.

Perhaps the best example of information sharing now permitted by section 203 of the USA PATRIOT Act takes place in the National Counterterrorism Center (NCTC) (formerly the Terrorist Threat Integration Center). The NCTC receives information lawfully collected by its member entities, which include representatives from the law enforcement community. The FBI, one of the NCTC's key members, relies upon section 203(d) of the USA PATRIOT Act to provide information to NCTC analysts on intelligence, protective, immigration, national defense, national security, and terrorism information (a subset of foreign intelligence and counterintelligence information) obtained as part of FBI criminal investigations. In particular, section 203(d) authorizes law enforcement officers to disclose foreign intelligence or counterintelligence information to various federal officials, notwithstanding any other legal restriction.

Information provided to NCTC pursuant to section 203 of the PATRIOT Act is used in three crucial NCTC missions: the production of all-source terrorism analysis, updating the database used by other federal entities to prevent known or suspected terrorists from entering the United States, and the sharing of terrorism-related information across the federal government.

Furthermore, section 203 of the PATRIOT Act facilitates the NCTC's ability to provide strategic analysis to policy makers and actionable leads to officers within the Department of Homeland Security (DHS), the FBI, and the Intelligence Community, transcending traditional government boundaries. The NCTC uses section 203 to assemble terrorism information, both foreign and domestic, and provide the various counterterrorism mission partners with the all-source intelligence necessary to combat and prevent terrorism activities.

The NCTC estimates that the number of known or appropriately suspected terrorists intercepted at borders of the United States, based on FBI reporting alone, has increased due to the information sharing provisions of the USA PATRIOT Act. The NCTC maintains TIPOFF, an up-to-date database of known and appropriately suspected terrorists. The NCTC relies upon various agencies, which provide terrorist identity information on an on-going basis. Much of the terrorist identities information the NCTC receives from the FBI is collected by in the course of criminal investigations and is shared pursuant to section 203.

The NCTC facilitates information sharing through its NCTC Online homepage, where classified information from the intelligence and law enforcement communities on terrorism intelligence is integrated. On a daily basis, NCTC receives and shares intelligence from various law enforcement reports, including those provided by the Transportation Security Administration and Customs and Border Protection. NCTC's efforts to "connect the dots" and share terrorism intelligence across the federal government will be severely restricted if such information sharing is prohibited in the future. In the absence of mandatory or permissive statutory provisions like section 203(d), each Executive Branch entity would be required to identify proper legal authority prior to sharing or disseminating information outside of the collecting agency or community.

FBI Field Offices have also specifically noted that provisions such as section 203(d) enable case agents to involve other agencies in investigations, resulting in a style of teamwork that: enables more effective and responsive investigations; improves the utilization of resources; allows for follow-up investigations by other agencies when the criminal subject leaves the United States; and helps prevent the compromise of foreign intelligence investigations.

Even though the law prior to the USA PATRIOT Act provided for some exchange of information, the law was complex and, as a result, agents often erred on the side of caution and refrained from sharing information. The USA PATRIOT Act's new information sharing authorities, including section 203, eliminated that hesitation and now allow agents to work more openly with other government entities resulting in a much

stronger team approach. Such an approach is necessary in order to effectively prevent and detect the complex web of terrorist activity. As a result, FBI Field Offices report enhanced liaison with state, local and other Federal agencies, resulting in better relationships. If even a portion of the information sharing capabilities are allowed to "sunset" or terminate, then an element of uncertainty will be re-introduced and agents will again hesitate and take the time necessary to seek clarification of the relevant legal restrictions prior to sharing information. This hesitation will lead to less teamwork and much less efficiency. For all of these reasons, section 203(d) should be renewed.

Section 204: Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral, and Electronic Communications

Text of Section 204:

> Section 2511(2)(f) of title 18, United States Code, is amended—
>
> > (1) by striking "this chapter or chapter 121" and inserting "this chapter or chapter 121 or 206 of this title"; and
> >
> > (2) by striking "wire and oral" and inserting "wire, oral, and electronic".

How Current Law Now Reads:

> **"18 U.S.C. § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited**
> ...
>
> (2)
> …
>
> > (f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted."

Analysis:

The purpose of this provision is two-fold. First, it clarifies that chapter 206 of title 18, which governs the installation and use of pen registers and trap-and-trace devices, will not interfere with certain foreign intelligence activities that fall outside of the definition of "electronic surveillance" in the Foreign Intelligence Surveillance Act ("FISA"). *See* 147 Cong. Rec. S11,006 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) (explaining that the purpose of section 204 of the USA PATRIOT Act, entitled "Clarification of intelligence exceptions from limitations on interception and disclosure

of wire, oral, and electronic communications," was "to make clear that these procedures [including those set forth in chapter 206] do not apply to the collection of foreign intelligence information under the statutory foreign intelligence authorities").

Second, section 204 clarifies that the exclusivity provision in section 2511(2)(f) of title 18 applies not only to the interception of wire and oral communications, but also to the interception of electronic communications. Section 2511(2)(f) reflects Congress's intent, when it enacted FISA and the Electronic Communications Privacy Act of 1986, to make the procedures in chapter 119 of title 18 ("Title III") (regulating the interception and disclosure of wire, electronic, and oral communications), chapter 121 of title 18 (regulating access to stored wire and electronic communications and transactional records), and FISA (regulating electronic surveillance undertaken to acquire foreign intelligence information) the exclusive procedures for conducting electronic surveillance, as defined by FISA, and intercepting certain types of domestic communications.

Section 204 remedies an apparent omission in the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, which, among other things, amended chapter 119 of title 18 ("Title III") to provide procedures for intercepting electronic communications and added chapter 121 to title 18 to provide procedures for accessing stored electronic communications, but neglected to make a corresponding change to clarify that the exclusivity provision in section 2511(2)(f) applies to the interception of not only wire and oral, but also electronic, communications.

Section 204 has been criticized by some opponents of the USA PATRIOT Act. For instance, EPIC has implied that section 204 improperly circumvented proper methods of investigation: it argued that the section "amended Title III and the Stored Communications Access Act so that stored voice-mail communications, like e-mail, may be obtained by the government through a search warrant rather than through more stringent wiretap orders."[10]

However, criticism of section 204, which appears to represent the view of a small minority,[11] obscures the fact that section 204 is, as the nonpartisan Congressional Research Service has observed, "essentially a technical amendment." Moreover, EPIC appears to confuse section 204 with section 209 of the Act.[12] In an age when terrorists use electronic communications just like everyone else, it is important to preserve section 204, a technical amendment that merely clarifies what Congress had always intended the statute to mean.

---

[10] *See supra* note 3.

[11] For instance, CDT, which has criticized many provisions of the USA PATRIOT Act, has stated that section 204 is among the provisions "that are not controversial." *See supra* note 2.

[12] Charles Doyle, Congressional Research Service, "USA PATRIOT Act: A Sunset Sketch" at CRS-3 (June 20, 2004).

Section 206: Roving Surveillance Authority under FISA

Text of Section 206:

> Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)(2)(B)) is amended by inserting `, or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,' after `specified person'."

How Current Law Now Reads:

> **"50 U.S.C. § 1805. Issuance of order**
> ...
> (c) Specifications and directions of orders
>
> An order approving an electronic surveillance under this section shall--
> ...
>
> (2) direct--
>
> (A) that the minimization procedures be followed;
>
> (B) **that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance**;
>
> (C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and
>
> (D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid."

Analysis:

A multipoint or "roving" wiretap order attaches to a particular suspect rather than to a particular phone or other communications facility. Prior to enactment of the USA PATRIOT Act, such wiretaps, which have long been available in the criminal investigative context, were not available under FISA. They were and are needed, however; international terrorists and foreign intelligence officers are trained to thwart surveillance by changing the communications facilities they use, thus making roving wiretaps particularly necessary in this context. Without roving wiretaps, investigators were often left two steps behind sophisticated terrorists.

Before the USA PATRIOT Act, 50 U.S.C. § 1805(c)(2)(B) permitted the Foreign Intelligence Surveillance Court ("FISA Court") to order "specified persons" (third parties such as telephone companies) to provide assistance and information to federal authorities in installing a wiretap or collecting information related to a foreign intelligence investigation. However, each time a suspect switched modes of communication, for example by obtaining a new cell phone, investigators had to return to the FISA Court for a new order just to change the name of the "specified person" needed to assist in monitoring the wiretap. This requirement significantly reduced the effectiveness of FISA surveillance.

Section 206 eliminated this problem. It amended 50 U.S.C. § 1805(c)(2)(B) to allow the FISA Court to issue roving wiretap orders under FISA in cases where the target's actions may thwart surveillance. Specifically, it inserted language into section 1805(c)(2)(B) permitting the FISA Court to direct the wiretap order to specified persons and "other persons" if the court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person" who would be required to assist in installing the court-authorized wiretap. Thus, the FISA Court does not have to name in the wiretap order each telecommunications company or other "specified person" whose assistance might be required. Section 206 also allowed the FISA Court to compel any necessary additional parties to assist in the installation of the wiretap and to furnish all information, facilities, or technical assistance necessary without specifically naming such persons in the wiretap order. Significantly, however, section 206 did not change the requirement that the target of the electronic surveillance must be identified or described in the order.

The ACLU has argued that wiretaps issued pursuant to section 206 "pose a greater challenge to privacy because they are authorized secretly without a showing of probable cause of crime. This Section represents a broad expansion of power without building in a necessary privacy protection."[13]

This argument, however, ignores the fact that section 206 did not alter the requirement that before approving electronic surveillance, the FISA Court must find that there is probable cause to believe that the target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. Moreover, for years, law enforcement has been able to use roving wiretaps to investigate traditional crimes, including drug offenses and racketeering. The authority to use roving wiretaps in traditional criminal investigations has existed since 1986. Section 206 simply authorized the same techniques in foreign intelligence investigations.

In addition, wiretaps under section 206 can be ordered only after the FISA court makes a finding that the actions of the target of the application may have the effect of thwarting the surveillance. A number of federal courts – including the Second, Fifth, and Ninth Circuits – have squarely ruled that similar roving wiretaps are perfectly consistent

[13] American Civil Liberties Union, *How the Anti-Terrorism Bill Limits Judicial Oversight of Telephone and Internet Surveillance* (Oct. 23, 2001) (available at http://www.aclu.org/congress/l102301g.html).

with the Fourth Amendment, *see, e.g.*, *United States v. Gaytan*, 74 F.3d 545 (5th Cir. 1996); *United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993); *United States v. Petti*, 973 F.2d 1441 (9th Cir. 1992), and no court of appeals has found otherwise.

Some have claimed that section 206 "authorizes intelligence investigators to conduct 'John Doe' roving surveillance – meaning that the FBI can wiretap every single phone line, mobile communications device or Internet connection that a suspect might be using, without ever having to identify the suspect by name. This, it is argued, gives the FBI a 'blank check' to violate the communications privacy of countless innocent Americans."[14]

Labeling wiretaps authorized under section 206 as "John Doe" wiretaps, however, is misleading. Even if the government is not sure of the actual identity of the target of such a wiretap, FISA nonetheless requires the government to provide "a description of the target of the electronic surveillance" to the FISA Court prior to obtaining a surveillance order. 50 U.S.C. § 1805(c)(1)(A). In certain cases involving terrorists and spies, the government simply may not know the name of the terrorist or spy in question, but still must be able to conduct surveillance of that individual, whom it already has probable cause to believe is involved in terrorism or espionage. A surveillance order under section 206 therefore is always connected to a particular target of surveillance. Moreover, as then-Attorney General Ashcroft explained in a January 28, 2004, letter to Senator Hatch, the government "cannot change the target of its surveillance under such a wiretap order; it must instead apply to the FISA court for a new order for the new target."

A related objection is that section 206 lacks an "ascertainment" requirement supposedly needed to preclude the surveillance of law-abiding Americans. As asserted by John Podesta, former Chief of Staff to President Clinton:

> The main difference between roaming wiretaps under current criminal law and the new FISA authority is that current criminal law requires that law enforcement "ascertain" that the target of a wiretap is actually using a device to be tapped. Section 206 contains no such provision. Ensuring that FISA wiretaps only roam when intelligence officials "ascertain" that the subject of an investigation is using a device, before it is tapped, would prevent abuse of this provision. For example, without the ascertainment requirement, it is conceivable that all the pay phones in an entire neighborhood could be tapped if suspected terrorists happened to be in that neighborhood. Bringing FISA roaming wiretaps in line with criminal roaming wiretaps would prevent such abuse and provide greater protection to the privacy of ordinary Americans.[15]

---

[14] *See* Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 206: 'Roving Surveillance Authority Under the Foreign Intelligence Surveillance Act of 1978'", (Feb. 24, 2004) (available at http://shop.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/sunset/206.php).

[15] *See* American Bar Association, Section on Individual Rights and Responsibilities, "USA PATRIOT Act: The Good, the Bad, and the Sunset," *Human Rights Magazine* (Winter 2002).

This criticism misses the mark. The specific "ascertainment" requirement contained in the criminal wiretap statute, *see* 18 U.S.C. § 2518(12), applies to the interception of oral communications, such as through hidden microphones, and not to the interception of wire or electronic communications, such as telephone calls. This provision of the criminal wiretap statute states that the interception of an oral communication "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." Applying that ascertainment requirement to FISA roving wiretaps, as would be done by the SAFE Act, which was introduced in the 108th Congress, would therefore make it harder to conduct effective surveillance of international terrorists than of drug dealers.[16] Moreover, section 206 in no way altered the robust FISA minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons.

Indeed, Podesta himself has endorsed the rationale underlying section 206, writing that before the USA PATRIOT Act: "FISA required a separate court order be obtained for each communication carrier used by the target of an investigation. In the era of cell phones, pay phones, e-mail . . . , and BlackBerry wireless e-mail devices, such a requirement is a significant barrier in monitoring an individual's communications. Section 206 allows a single wiretap to legally 'roam' from device to device, to tap the person rather than the phone. In 1986, Congress authorized the use of roaming wiretaps in criminal investigations that are generally subject to stricter standards than FISA intelligence gathering, so extending this authority to FISA was a natural step."[17] Section 206 should be preserved. Without this crucial authority, investigators would once again often be struggling to catch up to sophisticated terrorists trained to constantly change phones in order to avoid surveillance.

Section 207: Duration of FISA Surveillance of Non-United States Persons Who Are Agents of a Foreign Power

Text of Section 207:

> (a) DURATION -
>
> > (1) SURVEILLANCE- Section 105(e)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(e)(1)) is amended by--
> >
> > > (A) inserting "(A)" after "except that"; and
> > >
> > > (B) inserting before the period the following: ", and (B) an order under this Act for a surveillance targeted against an agent of a foreign power, as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less".
> >
> > (2) PHYSICAL SEARCH- Section 304(d)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)(1)) is amended by--

[16] *See* S. 1709 (The Security and Freedom Ensured Act of 2003), 108th Congress, § 2.
[17] *Id.*

(A) striking “forty-five” and inserting “90”;

(B) inserting “(A)” after “except that”; and

(C) inserting before the period the following: “, and (B) an order under this section for a physical search targeted against an agent of a foreign power as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less”.

(b) EXTENSION-

(1) IN GENERAL- Section 105(e)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(e)(2)) is amended by--

(A) inserting “(A)” after “except that”; and

(B) inserting before the period the following: “, and (B) an extension of an order under this Act for a surveillance targeted against an agent of a foreign power as defined in section 101(b)(1)(A) may be for a period not to exceed 1 year”.

(2) DEFINED TERM- Section 304(d)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)(2) is amended by inserting after “not a United States person,” the following: “or against an agent of a foreign power as defined in section 101(b)(1)(A),”.

How Current Law Now Reads:

§ 1805. Issuance of order

...

(e) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated

(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, for the period specified in the application or for one year, whichever is less, and (B) an order under this chapter for a surveillance targeted against an agent of a foreign power, as defined in section 1801(b)(1)(A) of this title may be for the period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this subchapter may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that (A) an extension of an order under this chapter for a surveillance targeted against a foreign power, as defined in section 1801(a)(5) or (6) of this title, or against a foreign power as defined in section 1801(a)(4) of this title that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and (B) an extension of an order under this chapter for a surveillance targeted against an agent of a foreign power as defined in section 1801(b)(1)(A) of this title may be for a period not to exceed 1 year.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

§ 1824. Issuance of order

...

(d) Duration of order; extensions; assessment of compliance

(1) An order issued under this section may approve a physical search for the period necessary to achieve its purpose, or for 90 days, whichever is less, except that (A) an order under this section shall approve a physical search targeted against a foreign power, as defined in paragraph (1), (2), or (3) of section 1801(a) of this title, for the period specified in the application or for one year, whichever is less, and (B) an order under this section for a physical search targeted against an agent of a foreign power as defined in section 1801(b)(1)(A) of this title may be for the period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this subchapter may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that an extension of an order under this chapter for a physical search targeted against a foreign power, as defined in section 1801(a)(5) or (6) of this title, or against a foreign power, as defined in section 1801(a)(4) of this title, that is not a United States person, or against an agent of a foreign power as defined in section 1801(b)(1)(A) of this title, may be for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period.

(3) At or before the end of the period of time for which a physical search is approved by an order or an extension, or at any time after a physical search is carried out, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

Analysis:

Prior to the passage of the USA PATRIOT Act, surveillance orders issued by the FISA Court and directed against agents of a foreign power, such as international terrorists or spies, had a maximum duration of 90 days, and could be extended with court approval for additional periods of 90 days. Physical search orders issued by the FISA Court and directed against agents of a foreign power were effective for no more than 45 days. These short timeframes forced Justice Department investigators to needlessly divert manpower from the primary mission of detecting and disrupting potential terrorist attacks in order to return frequently to the FISA Court to extend FISA search and surveillance orders even in routine matters where there was no question about the legal sufficiency of a particular case.

Section 207 of the USA PATRIOT Act helped to ameliorate this problem by increasing the maximum time duration for FISA surveillance and physical search orders. Now, initial surveillance orders directed against non-United States person members of international terrorist groups or officers and employees of foreign powers may be in

effect for up to 120 days (instead of 90 days),[18] and such orders may be extended for a maximum of one year (instead of 90 days) at a time with court approval. Similarly, physical search orders may now remain effective for up to 90 days (instead of 45 days) in the case of agents of a foreign power who are United States persons and 120 days (instead of 45 days) with respect to non-United States person members of international terrorist groups or officers and employees of foreign powers. In the case of non-United States person members of international terrorist groups or officers and employees of foreign powers, such search orders may be extended for up to one year with court approval in certain circumstances.

While many critics of the USA PATRIOT Act, such as the CDT, have expressed the view that section 207 is not controversial,[19] others disagree. EFF, for example, opposes the renewal of section 207.[20] EFF complains the time limits for FISA wiretaps and searches before the passage of the USA PATRIOT Act "were already generous compared to taps and warrants available to the FBI in criminal investigations."[21] Wiretap orders in the criminal context, for example, may only initially authorize surveillance for up to 30 days, and such orders may only be extended by a court for 30 days at a time. EFF further asserts that the only benefit derived from section 207 is "reduced paperwork" and that this benefit comes at the cost of the interception of "many more innocent communications" between "many more innocent persons."[22]

These criticisms of section 207, however, fall wide of the mark. To begin with, section 207 does not make it easier to conduct surveillance of innocent Americans. The provision does not change the requirement that surveillance and physical search orders may only be directed against those the FISA Court finds probable cause to believe are foreign powers or agents of foreign powers. Moreover, the extended time periods for FISA wiretap and surveillance orders only apply to certain agents of a foreign power who are not United States persons. Such time periods thus do not apply to wiretaps and surveillance orders directed against United States citizens or lawful permanent resident aliens. Finally, section 207 in no way altered the robust FISA minimization procedures that limit the acquisition, retention, and dissemination of information or communications involving United States persons.

Perhaps more importantly, however, EFF's criticism significantly underemphasizes the important benefits brought about by section 207. The Department

---

[18] Pursuant to 50 U.S.C. § 1805(e)(1), surveillance orders may now be directed against agents of a foreign power, as defined in 50 U.S.C. § 1801(b)(1)(A), for a maximum of 120 days. Agents of a foreign power, as defined in 50 U.S.C. § 1801(b)(1)(A), are non-United States persons who "act[] in the United States as an officer of employee of a foreign power, or as a member of a foreign power defined in [50 U.S.C. § 1801(a)(4)]." Title 50 U.S.C. § 1801(a)(4), in turn, refers to "a group engaged in international terrorism or activities in preparation therefor."

[19] *See supra* note 2.

[20] Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 207: 'Duration of Surveillance of Non-United States Persons Who Are Agents of a Foreign Power " (Mar. 2, 2004) (available at http://www.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/sunset/207.php).

[21] *Id*.

[22] *Id*.

believes that section 207 has made a critical contribution to protecting the national security of the United States by making changes to the time periods for which electronic surveillance and physical searches are authorized under FISA. This is critical, because by doing so, it has conserved the limited resources that are available at the FBI and the Department's Office of Intelligence Policy and Review to process FISA applications. Instead of devoting time to the mechanics of processing FISA applications, which are considerable, government resources can be devoted to other investigative activity as well as reviewing compliance with laws, executive orders, and policy guidelines intended to ensure appropriate oversight of the use of intelligence collection authorities.

For example, prior to enactment of section 207, in order to conduct electronic surveillance and physical search of foreign diplomats and non-resident alien terrorists during one calendar year, the government had to file four applications for electronic surveillance covering successive 90-day periods, and eight applications for physical search covering successive 45-day periods, for a total of 12 separate applications. Thanks to section 207, however, this number can be reduced to two applications -- one combined electronic surveillance and physical search application for an initial period of 120 days, and, at the end of that 120-day period, a second combined application for one year (provided that the court finds that there is probable cause to believe that no property of any individual United States person will be acquired during the one year physical search authorization period). This represents an 83 percent reduction in the amount of paperwork involved to target clearly legitimate agents of foreign powers, and allows the government to devote those resources to other important tasks.

Section 207 also enables the government to more efficiently conduct electronic surveillance and physical search of United States persons who are agents of a foreign power. While section 207 did not change the time periods applicable for electronic surveillance of United States persons, which remained at 90 days, by making the time periods of electronic surveillance orders and physical search orders equivalent with respect to United States persons, it has enabled the Department to file streamlined combined electronic surveillance and physical search applications that, in the past, were tried but abandoned as too cumbersome to do effectively. Thus, prior to enactment of section 207, in order to conduct electronic surveillance and physical search of such targets, the government had to file four applications for electronic surveillance covering successive 90-day periods, and eight applications for physical search covering successive 45-day periods, for a total of 12 separate applications. Thanks to section 207, this number can be reduced to four combined electronic surveillance and physical search applications. This represents a two-thirds reduction in the number of applications the government is required to file with the FISA court in these circumstances.

This provision has not merely led to reduced paperwork; section 207 has resulted in a more effective utilization of available personnel resources and the collection mechanisms authorized under FISA. It has allowed investigators to focus their efforts on more significant and complicated terrorism-related cases and to spend more time ensuring that appropriate oversight is given to investigations involving the surveillance of United States persons. Given the finite resources at the Justice Department's disposal, the use of personnel to prepare and process routine extensions of FISA surveillance and

search orders reduces the manpower available to focus on preventing terrorist attacks as well as processing new applications for FISA surveillance. While the Department has been subjected to criticism by some for processing FISA applications too slowly, great strides have been made in the recent years in improving the efficiency of the FISA process because of both the addition of new personnel and the use of section 207. However, were section 207 allowed to expire, much of this progress would be reversed, and Justice Department personnel would be forced to spend significantly more time on the routine extensions of current FISA orders and significantly less time on new applications.

While specific information regarding the Department's use of section 207 is classified, relevant data has been provided to Congress in the Attorney General's semi-annual report on the Department's use of the Foreign Intelligence Surveillance Act. Such reports were transmitted to Congress in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004.

Section 209: Seizure of Voice-Mail Messages Pursuant to Warrants

Text of Section 209:

> Title 18, United States Code, is amended--
>
> > (1) in section 2510--
> >
> > > (A) in paragraph (1), by striking beginning with "and such" and all that follows through "communication"; and
> > >
> > > (B) in paragraph (14), by inserting "wire or" after "transmission of"; and
> >
> > (2) in subsections (a) and (b) of section 2703--
> >
> > > (A) by striking "CONTENTS OF ELECTRONIC" and inserting "CONTENTS OF WIRE OR ELECTRONIC" each place it appears;
> > >
> > > (B) by striking "contents of an electronic" and inserting "contents of a wire or electronic" each place it appears; and
> > >
> > > (C) by striking "any electronic" and inserting "any wire or electronic" each place it appears.

How Current Law Now Reads:

> **"§ 2510. Definitions**
>
> As used in this chapter--
>
> > (1) 'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in

providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;
...
(14) 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;"

"§ 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."

Analysis:

Prior to the passage of the USA PATRIOT Act, law enforcement officers were able to obtain access to voice messages stored on home answering machines with a search warrant. Likewise, under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703 et seq., law enforcement officers needed only a search warrant to access stored electronic communications, such as e-mail. If, however, a voice-mail message was stored on a voice-mail system with a telecommunications provider, instead of on an answering machine, law enforcement officers were required to meet the higher standard necessary for obtaining a wiretap order. This was because access to stored wire communications (such as voice-mail) was governed by the wiretap statute, 18 U.S.C. § 2510(1), instead of ECPA.

Regulating stored wire communications through the wiretap statute created large and unnecessary burdens for criminal investigators. Stored voice communications, however, possess few of the sensitivities associated with the real-time interception of telephones, making the extremely burdensome process of obtaining a wiretap order unreasonable. Moreover, in large part, the pre-USA PATRIOT Act statutory framework envisioned a world in which technology-mediated voice communications (such as telephone calls) were conceptually distinct from non-voice communications (such as faxes, pager messages, and e-mail). To the limited extent that Congress had acknowledged that data and voice might co-exist in a single transaction, it had not anticipated the convergence of these two kinds of communications typical of today's telecommunications networks. With the advent of MIME — Multipurpose Internet Mail Extensions — and similar features, an e-mail may now include one or more "attachments" consisting of any type of data, including voice recordings. As a result, a law enforcement officer seeking to obtain a suspect's unopened e-mail from an Internet service provider by means of a search warrant (as required under 18 U.S.C. § 2703(a)) has no way of knowing whether the inbox messages include voice attachments (i.e., wire communications), which could not be compelled using a search warrant.

Section 209 of the USA PATRIOT Act solved these problems by harmonizing the rules for obtaining stored "wire" communications (e.g., voice-mail) with those for obtaining stored "electronic" communications (e.g., e-mail), making 18 U.S.C. § 2703 equally applicable to both and eliminating the disparity in treatment of what was essentially the same type of information. As a result, just as law enforcement may obtain access to voice messages stored on a home answering machine or stored e-mail messages through the use of a search warrant, law enforcement may now also obtain voice-mail stored electronically with a telecommunications provider through the use of a warrant rather than through the use of a wiretap order.

Section 209 preserved all of the pre-existing standards for the availability of search warrants. For example, law enforcement still must: (1) apply for and receive a court order; and (2) establish probable cause that the property to be searched or seized is evidence of a crime or property that is designed for use, intended for use, or was used in committing a crime.

Section 209 of the USA PATRIOT Act thus modernized federal law by enabling investigators to more quickly access suspects' voice-mail by using a search warrant. This is important because the speed with which voice-mail is seized and searched can be critical to an investigation where time is of the essence. Section 209 has been very useful to the Department, and warrants issued pursuant to this provision have been used to obtain evidence in a variety of criminal cases, including a number of drug trafficking investigations, such as an investigation of a large-scale ecstasy smuggling ring based in the Netherlands, an investigation into a series of violent robberies, and a kidnapping investigation.

Section 209 has not generated significant opposition. However, some, such as EFF, have complained that section 209 unnecessarily reduces the privacy of Americans' voice-mail.[23] Such critics have failed to explain, however, why it should be harder for law enforcement to gain access to voice-mail messages stored on the system of a telecommunications provider than to messages stored on a home answering machine or to e-mail messages stored by an Internet service provider. To date, no persuasive explanation has been provided.

Section 212: Emergency Disclosure of Electronic Communications to Protect Life and Limb

Text of Section 212:

(a) DISCLOSURE OF CONTENTS-

(1) IN GENERAL- Section 2702 of title 18, United States Code, is amended--

(A) by striking the section heading and inserting the following:

"Sec. 2702. Voluntary disclosure of customer communications or records";

(B) in subsection (a)--

(i) in paragraph (2)(A), by striking "and" at the end;

(ii) in paragraph (2)(B), by striking the period and inserting "; and"; and

(iii) by inserting after paragraph (2) the following:

"(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the

[23] *See* Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 209: 'Seizure of Voice Mail Messages Pursuant to Warrants'", (Mar. 10, 2004) (available at http://www.eff.org/ Privacy/Surveillance/Terrorism /PATRIOT/sunset/209.php).

contents of communications covered by paragraph (1) or (2)) to any governmental entity.";

(C) in subsection (b), by striking "EXCEPTIONS- A person or entity" and inserting "EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS- A provider described in subsection (a)";

(D) in subsection (b)(6)--

(i) in subparagraph (A)(ii), by striking "or";

(ii) in subparagraph (B), by striking the period and inserting "; or"; and

(iii) by adding after subparagraph (B) the following:

"(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay."; and

(E) by inserting after subsection (b) the following:

"(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS- A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

"(1) as otherwise authorized in section 2703;

"(2) with the lawful consent of the customer or subscriber;

"(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

"(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

"(5) to any person other than a governmental entity.".

(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2702 and inserting the following:

"2702. Voluntary disclosure of customer communications or records.".

(b) REQUIREMENTS FOR GOVERNMENT ACCESS-

(1) IN GENERAL- Section 2703 of title 18, United States Code, is amended--

(A) by striking the section heading and inserting the following:

"Sec. 2703. Required disclosure of customer communications or records";

(B) in subsection (c) by redesignating paragraph (2) as paragraph (3);

(C) in subsection (c)(1)--

(i) by striking "(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may" and inserting "A governmental entity may require a provider of electronic communication service or remote computing service to";

(ii) by striking "covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

"(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity' and inserting `)";

(iii) by redesignating subparagraph (C) as paragraph (2);

(iv) by redesignating clauses (i), (ii), (iii), and (iv) as subparagraphs (A), (B), (C), and (D), respectively;

(v) in subparagraph (D) (as redesignated) by striking the period and inserting "; or"; and

(vi) by inserting after subparagraph (D) (as redesignated) the following:

"(E) seeks information under paragraph (2)."; and

(D) in paragraph (2) (as redesignated) by striking "subparagraph (B)" and insert "paragraph (1)".

(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2703 and inserting the following:

"2703. Required disclosure of customer communications or records.".

How Current Law Now Reads:

"§ 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.--Except as provided in subsection (b)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.-- A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

(7) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

> (8) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.
>
> (c) Exceptions for disclosure of customer records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--
>
> (1) as otherwise authorized in section 2703;
>
> (2) with the lawful consent of the customer or subscriber;
>
> (3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
>
> (4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;
>
> (5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or
>
> (6) to any person other than a governmental entity.

Analysis:

Prior to the passage of the USA PATRIOT Act, federal law contained no special provision authorizing electronic communication service providers to disclose voluntarily customer records or communications to federal authorities in emergency situations. If, for example, an Internet service provider ("ISP") possessed information that, if disclosed to the government, could prevent an imminent terrorist attack, an ISP making such a disclosure on a voluntary basis might have been sued civilly since providing such information did not fall within one of the statutory exceptions to the limitations on disclosure contained in the Electronic Communications Privacy Act ("ECPA"), even if that disclosure was necessary to save lives.

In addition, prior to the enactment of the USA PATRIOT Act, federal law did not expressly permit an ISP to voluntarily disclose customer records (such as a subscriber's login records) to the government to protect itself against hacking. The law did, however, allow providers to disclose the content of communications for this reason. *See* 18 U.S.C. §§ 2702(b)(5), former § 2703(c)(1)(B). This created a nonsensical anomaly in the law as the right to disclose the content of communications logically implies the less-intrusive ability to disclose non-content records. Moreover, as a practical matter, providers need to have the right to disclose to law enforcement the facts surrounding attacks on their systems. For example, when an ISP's customer hacks into the ISP's network, gains complete control over an e-mail server, and reads or modifies the e-mail of other customers, the provider must have the legal ability to report the complete details of the crime.

Section 212 corrected both of these inadequacies in the statute. First, it amended 18 U.S.C. § 2702(b)(6) to permit, but not require, a service provider to disclose to federal authorities either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. It is important to recognize, however, that this voluntary disclosure authority does not create an affirmative obligation on service providers to review customer communications in search of such imminent dangers. Section 212 also amended ECPA to allow service providers to disclose information to protect their rights and property. Specifically, it amended 18 U.S.C. § 2702(c)(3) to clarify that service providers do have the statutory authority to disclose non-content records to protect their rights and property.

In 2002, the Homeland Security Act repealed that portion of section 212 governing the disclosure of the content of communications in emergency situations and placed similar authority in a separate statutory provision, 18 U.S.C. § 2702(b)(7). The Homeland Security Act, however, did not alter that portion of section 212 pertaining to the voluntary disclosure of non-content customer records in emergency situations. Thus, were Section 212 of the USA PATRIOT Act allowed to expire at the end of 2005, an ISP would find itself in the anomalous position of being able to voluntarily disclose the content of customers' communications in emergency situations but not being able to voluntarily disclose non-content customer records pertaining to those communications in emergency situations.

Section 212 has been used often and has already saved lives. To give just a few examples, voluntary disclosures from computer service providers pursuant to section 212 have assisted law enforcement in safely recovering an 88-year-old Wisconsin woman who was kidnapped and held for ransom while bound in an unheated shed during a cold Wisconsin winter and in safely recovering four kidnapped or missing children. For instance, a few months ago, Bobbie Jo Stinnett of Skidmore, Missouri, who was eight months pregnant, was found strangled in her home lying in a pool of her own blood. Her unborn daughter had been cut out of her womb with a kitchen knife. Police officers examined a computer found in Bobbie Jo's home. They discovered that she had been active on the Internet in connection with her dog-breeding business. As the investigation intensified, the officers found an exchange from a message board between Bobbie Jo and someone who called herself Darlene Fischer. Fischer claimed to be interested in a dog. She had asked Bobbie Jo for directions to her house for a meeting on December 16—the same day as the murder. Using section 212, FBI agents and examiners at the Regional Computer Forensic Laboratory in Kansas City were able to trace Darlene Fischer's messages to a server in Topeka, find Darlene Fischer's email address, and then trace it to a house in Melvern, Kansas. Darlene Fischer's real name was in fact Lisa Montgomery. Montgomery was arrested and subsequently confessed, and baby Victoria Jo Stinnett was found alive—less than 24 hours after she was cut from her mother's womb.

Section 212 was also used to foil an alleged kidnapping plot that turned out to be an extortion racket. Additionally, the provision has been used to successfully respond to a cyberterrorist threat to the South Pole Research Station, a bomb threat to a high school, a threat to kill the employees of a European company as well as their families, and a

threat to burn down an Islamic mosque in Texas. In all of these cases, voluntary disclosures from Internet service providers were critical to apprehending the perpetrators before their threats could be carried out. These are just a few examples of the utility of section 212.

Although section 212 has not been the subject of significant criticism, EFF has complained that computer service providers should not be able to disclose customer records or communications unless a court or grand jury demands them.[24] Requiring that procedure, however, would eliminate the vital benefits provided by section 212. First, section 212 allows a service provider to disclose information voluntarily not only when the government seeks it, but also when the service provider itself becomes aware of an emergency that poses a threat to life and limb. To require a court order or subpoena in such a case would require the service provider first to contact authorities and provide a sufficient basis for authorities to seek such an order, then would require authorities to obtain the order and serve it on the provider, and only then would the critical information be made available. That cumbersome process would waste precious time in an emergency. Second, even in the more usual case where the government seeks information from a service provider in response to an emergency, obtaining a court order or subpoena could still take a significant amount of time. In some emergency situations, even a matter of minutes might mean the difference between life and death. EFF complains that section 212 may result in unnecessary invasions of privacy because an ISP's belief that a life-threatening emergency justifies the disclosure of customer records or communications may turn out to be mistaken. Such mistakes are no doubt bound to happen. However, section 212 requires the ISPs' belief to be a reasonable one,[25] and, in order to save lives, their evaluation of the situation must be made at the time of the emergency and should not be subject to Monday-morning quarterbacking.

Section 214: Pen Register and Trap and Trace Authority under FISA

Text of Section 214:

> (a) APPLICATIONS AND ORDERS- Section 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842) is amended--
>
> > (1) in subsection (a)(1), by striking "for any investigation to gather foreign intelligence information or information concerning international terrorism" and inserting "for any 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";

[24] *See* Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 212 and Homeland Security Act Section 225: 'Emergency Disclosures of Electronic Communications to Protect Life and Limb'", (Mar. 24, 2004) (available at http://www.eff.org/Privacy/Surveillance/Terrorism /PATRIOT/sunset/212.php).

[25] The relevant standard with respect to the disclosure of communications was changed by the Homeland Security Act from reasonable belief to good-faith belief.

(2) by amending subsection (c)(2) to read as follows:

"(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation 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.";

(3) by striking subsection (c)(3); and

(4) by amending subsection (d)(2)(A) to read as follows:

"(A) shall specify--

`(i) the identity, if known, of the person who is the subject of the investigation;

"(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

"(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.".

(b) AUTHORIZATION DURING EMERGENCIES- Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended--

(1) in subsection (a), by striking "foreign intelligence information or information concerning international terrorism" and inserting "foreign intelligence information not concerning a United States person or information 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"; and

(2) in subsection (b)(1), by striking "foreign intelligence information or information concerning international terrorism" and inserting "foreign intelligence information not concerning a United States person or information 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".

How Current Law Now Reads:

"50 U.S.C. § 1842. Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations

(a) Application for authorization or approval

(1) Notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any 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 which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

…

(c) Executive approval; contents of application

…

(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation 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.

…

(d) Ex parte judicial order of approval

…

(2) An order issued under this section--

(A) shall specify--

(i) the identity, if known, of the person who is the subject of the investigation;

(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order."

"50 U.S.C. § 1843. Authorization during emergencies

(a) Requirements for authorization

Notwithstanding any other provision of this subchapter, when the Attorney General makes a determination described in subsection (b) of this section, the Attorney General may authorize the installation and use of a pen register or trap and trace device on an emergency basis to gather foreign intelligence information not concerning a United States person or information 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 if--

> (1) a judge referred to in section 1842(b) of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to install and use the pen register or trap and trace device, as the case may be, on an emergency basis; and
>
> (2) an application in accordance with section 1842 of this title is made to such judge as soon as practicable, but not more than 48 hours, after the Attorney General authorizes the installation and use of the pen register or trap and trace device, as the case may be, under this section.
>
> (b) Determination of emergency and factual basis
>
> A determination under this subsection is a reasonable determination by the Attorney General that--
>
> (1) an emergency requires the installation and use of a pen register or trap and trace device to obtain foreign intelligence information not concerning a United States person or information 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 before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 1842 of this title[.]"

Analysis:

A pen register is a device that can track routing and addressing information about a communication – for example, which numbers are dialed from a particular telephone. Pen registers, however, are not used to collect the substance of communications. Similarly, a trap-and-trace device tracks numbers used to call a particular telephone, without monitoring the substance of the telephone conversation. Both devices are routinely used in criminal investigations where, in order to obtain the necessary order authorizing use of the device, the government must show simply that the information sought is relevant to an ongoing investigation.

Under FISA, government officials may seek a court order for a pen register or trap-and-trace device to gather foreign intelligence information or information about international terrorism or espionage. Prior to enactment of the USA PATRIOT Act, however, FISA required government personnel to certify not just that the information they sought was relevant to an intelligence investigation, but also that the facilities to be monitored had been used or were about to be used to contact a foreign agent or an agent of a foreign power, such as a terrorist or spy. Thus, it was much more difficult to obtain an effective pen register or trap-and-trace order in an international terrorism investigation than in a criminal investigation.

Section 214 of the USA PATRIOT Act eliminated the provision cabining FISA pen register and trap-and-trace orders to facilities used by foreign agents or those engaged in international terrorist or clandestine intelligence activities, thus bringing authorities for terrorism and other foreign intelligence investigations into line with similar criminal authorities. *See* 50 U.S.C. § 1842(c)(3). Significantly, however, applicants must still certify that the devices are likely to reveal information relevant to a foreign intelligence investigation, such as an international terrorism or espionage investigation. This provision made the standard contained in FISA for obtaining a pen

register or trap-and-trace order parallel with the standard for obtaining a pen register or trap-and-trace order in the criminal context. This section preserved the requirement predicating the government's installation of a pen register on permission from the independent FISA court, which must find that the government's application satisfies the requirements of the Act before it authorizes use of the device.

The Department has applied section 214 to international terrorism and counterintelligence investigations, including a case where the subject was believed to be attempting to procure nuclear arms. In one terrorism case, the only phone that the FBI could prove was used by the subject was his associate's phone. Additionally, the FBI had insufficient information that this associate was an agent of a foreign power. Thus, under the previous standard for a FISA pen register or trap-and-trace order, the FBI may not have succeeded in obtaining a pen register or trap-and-trace order. The standard established by section 214, however, allowed the agents to obtain the order by demonstrating that the information to be collected was relevant to an ongoing terrorism investigation. The information obtained by the order was valuable because it demonstrated the extent that the subject and his associate were communicating with subjects of other terrorism investigations. In another example, section 214 allowed FISA pen-register authority to be obtained based on the fact that information was likely to result in foreign intelligence information. This provision allowed the FBI to collect data on target lines even when the subject was out of the country and provided valuable intelligence information regarding the subject and terrorism-related matters.

Current law requires the Department to "fully inform" the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on a semi-annual basis concerning all uses of pen register and trap and trace devices pursuant to FISA. It also requires the Department to provide those committees as well as the House and Senate Judiciary Committees a semi-annual report setting forth the total number of applications made for orders approving the use of pen registers or trap-and-trace devices under FISA along with the total number of such orders either granted, modified, or denied. *See* 50 U.S.C. § 1846. The Department transmitted the aforementioned reports to Congress regarding the use of section 214 in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004.

The Electronic Privacy Information Center has voiced the most common criticism of section 214: that it "significantly eviscerates the constitutional rationale for the relatively lax requirements that apply to foreign intelligence surveillance."[26] This criticism misses the mark; section 214 in fact goes *further* to protect privacy than the U.S. Constitution requires. The Supreme Court has long held that law enforcement is not constitutionally required to obtain court approval before installing a pen register. Under long-settled Supreme Court precedent, the use of pen registers does not constitute a "search" within the meaning of the Fourth Amendment. This is so because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," and "when he used his phone, petitioner voluntarily conveyed numerical information to the telephone company." *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

[26] *See* "The USA PATRIOT Act" (available at http://www.epic.org/privacy/terrorism/usapatriot/).

Consequently, the Constitution does not require that law enforcement obtain court approval before installing a pen register. Moreover, section 214 explicitly safeguards First Amendment rights by providing that any "investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

Section 215: Access to Records and Other Items Under the Foreign Intelligence Surveillance Act

Text of Section 215:

> Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:
>
> **"SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.**
>
> (a) (1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may 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, 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.
>
> (2) An investigation conducted under this section shall--
>
> (A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and
>
> (B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.
>
> (b) Each application under this section--
>
> (1) shall be made to--
>
> (A) a judge of the court established by section 103(a); or
>
> (B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and
>
> (2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to protect against international terrorism or clandestine intelligence activities.
>
> (c) (1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

SEC. 502. CONGRESSIONAL OVERSIGHT.

(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.
(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period--

(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and

(2) the total number of such orders either granted, modified, or denied."

How Current Law Now Reads:

"§ 1861. Access to certain business records for foreign intelligence and international terrorism investigations

(a) (1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may 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 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.

(2) An investigation conducted under this section shall

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(b) Each application under this section

(1) shall be made to--

(A) a judge of the court established by section 1803(a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of Title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

(c) (1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

§ 1862. Congressional oversight

(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 1861 of this title.

(b) On a semiannual basis, the attorney general shall provide to the committees on the judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period--

(1) the total number of applications made for orders approving requests for the production of tangible things under section 1861 of this title; and

(2) the total number of such orders either granted, modified, or denied."

Analysis:

Prior to the passage of the USA PATRIOT Act, it was difficult for the government to obtain court orders for access to business records and other tangible items in connection with national security investigations. Such records, for example, could be sought from only common carriers, public accommodation providers, physical storage facility operators, and vehicle rental agencies. *See* 50 U.S.C. §§ 1861-1863 (2000 ed.). In addition, intelligence investigators had to meet a much higher evidentiary standard to obtain an order requiring the production of such records than prosecutors had to meet to obtain a grand jury subpoena to require the production of those same records in a criminal investigation. *See id*.

As a result, section 215 of the USA PATRIOT Act made several important changes to the FISA business records authority so that intelligence agents are better able to obtain crucial information in important national security investigations. For example, just as there is no artificial limit to the range of items or types of entities that criminal prosecutors may subpoena, section 215 now allows the FISA Court to issue orders requiring the production of any business record or tangible item, and there is no limitation on the types of entities from which items may be sought. Similarly, just as prosecutors in a criminal case may subpoena any item so long as it is relevant to their investigation, so too may the FISA Court issue an order requiring the production of records or items that are relevant to investigations to protect against international terrorism or clandestine intelligence activities.

Section 215 may be the most widely-criticized provision of the Act. Much of this criticism, however, has resulted from inaccurate characterizations of what is contained in the provision. Critics, for example, have complained that section 215 does not require the government to make any evidentiary showing in order to obtain a court order requiring the production of records. So long as the government certifies that the records are being sought for an international terrorism or espionage investigation, critics contend that the FISA Court has no choice but to issue the requested order.[27]

This portrayal of section 215, however, is categorically false. Pursuant to section 215, a judge "shall" issue an order "approving the release of records if the judge finds that the application meets the requirements of this section." 50 U.S.C. § 1861(c)(1) (emphasis added). As a result, before issuing an order requiring the production of any records under section 215, a federal judge must find that the requested records are sought for (and thus relevant to) "an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2).

Section 215's opponents also claim that the provision is open to abuse and fishing expeditions because court orders under section 215 are subject to less oversight and a lower burden of proof than are grand jury subpoenas in criminal investigations.[28]

Once again, however, this criticism is completely inaccurate. Section 215 orders, in fact, are subject to greater judicial oversight than are grand jury subpoenas, which prosecutors regularly use to obtain business records in criminal investigations. A court must explicitly authorize the use of section 215 to obtain business records. A grand jury subpoena for such records, by contrast, is typically issued without any prior involvement by a judge. Section 215 orders are similarly subject to greater congressional oversight than are grand jury subpoenas. Every six months, the Attorney General must "fully inform" the House and Senate Intelligence Committees "concerning all requests for the production of tangible things" under section 215. 50 U.S.C. § 1862(a). There is no similar mechanism, however, for congressional oversight of grand jury subpoenas.

---

[27] *See, e.g.*, Letter from Ralph G. Neas, President of People for the American Way, and Marge Baker, Director of Public Policy for People for the American Way, to Members of Congress, July 6, 2004.
[28] *See id*.

Section 215 orders are also subject to the same burden of proof as are grand jury subpoenas -- a relevance standard**.** Just as grand jury subpoenas may be issued to obtain records that are relevant to a criminal investigation, a court may issue orders requiring the production of records under section 215 that are relevant to an authorized international terrorism or espionage investigation. Some critics have complained that section 215 does not contain a "relevance" standard because the word "relevance" is not specifically mentioned in the provision itself. Section 215, however, states that the FISA Court may only enter an order requiring the production of records if such records are "sought for an authorized investigation conducted in accordance with [50 U.S.C. § 1861(a)(2)] to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1862(a). This is the equivalent of a relevance standard because if records are irrelevant to an investigation, then they are not being "sought for" that investigation.

Finally, many organizations, including the American Library Association, have attacked section 215 because of its potential application to library records, raising the ominous spectre of Big Brother monitoring Americans' reading habits or Internet usage.[29] The arguments made by these critics, however, do not take into account the safeguards built into the provision, well-established grand jury practice, and the reality of the terrorist threat.

Although a section 215 order could be issued to a library so long as a judge determined that the library possessed records relevant to an international terrorism or espionage investigation, the provision does not single libraries out or even mention them at all; it simply does not exempt libraries from the range of entities that may be required to produce records. This lack of a special exemption for libraries, however, is completely consistent with criminal investigative practice. Prosecutors have always been able to obtain records from bookstores and libraries through grand jury subpoenas. For instance in the 1997 Gianni Versace murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach. Similarly, in the famed Zodiac gunman investigation, a grand jury in New York subpoenaed library records after investigators came to believe that the gunman was inspired by a Scottish occult poet and wanted to learn who had checked out the poet's books.

The fact that section 215 does not exempt libraries is also wise policy. Libraries should not be carved out as safe havens for terrorists and spies. The Department, for example, has confirmed that as recently as the winter and spring of 2004, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates. Furthermore, we know that spies have used public library computers to do research to further their espionage and to communicate with their co-conspirators. For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office, who recently was convicted of

[29] *See, e.g.,* Campaign for Reader Privacy, "What is Section 215?" (available at http://www.readerprivacy.com/?mod[type]=learn_more).

espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments.

The concern that section 215 somehow allows the government to target Americans because of the books that they read or websites that they visit also misses the mark because the provision explicitly protects First Amendment rights. It provides that an investigation under this section shall "not be conducted of a United States person solely upon the basis of activities protected by the First Amendment to the Constitution of the United States." 50 U.S.C. § 1861(a)(2)(B).

Many critics have also complained that those who receive a section 215 order requiring the production of records are not allowed to tell others that they received the order.[30] Such a nondisclosure requirement, however, is standard operating procedure for the conduct of surveillance in sensitive international terrorism or espionage investigations. As the U.S. Senate concluded when adopting the Foreign Intelligence Surveillance Act: "By its very nature, foreign intelligence surveillance must be conducted in secret."[31] Were information identifying the targets of international terrorism and espionage investigations revealed, according to the U.S. Court of Appeals for the D.C. Circuit, such disclosures would "inform terrorists of both the substantive and geographic focus of the investigation[,] . . . would inform terrorists which of their members were compromised by the investigation, and which were not[,] . . . could allow terrorists to better evade the ongoing investigation and more easily formulate or revise counter-efforts * * * [and] be of great use to al Qaeda in plotting future terrorist attacks or intimidating witnesses in the present investigation."[32] Maintaining the secrecy of such investigations is therefore centrally important to the Department's ability to gather information regarding the activities of international terrorists and hostile foreign adversaries without causing the disclosure of information that would undermine its efforts to prevent further acts of terrorism.

On September 18, 2003, the Attorney General declassified the fact that as of that date, section 215 of the USA PATRIOT Act had not been used. Subsequent information regarding the utilization of section 215 (or lack thereof) remains classified but has been provided to Congress on a semiannual basis as required by 50 U.S.C. § 1862. In particular, the Department has reported to Congress six times on its use of section 215. These reports were transmitted by the Department in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004.

Some opponents of section 215 have seized on the fact that the provision was not used in the two years following the passage of the USA PATRIOT Act and used it as evidence that the provision is not necessary and should be repealed.[33] The fact that an

---

[30] *See id*.
[31] S. Rep. No. 95-604, 95th Cong. 2d Sess., at 60 (1978).
[32] *Center of National Security Studies v. U.S. Department of Justice*, 331 F.3d 918, 928-29 (D.C. Cir. 2003).
[33] *See* Kim Zetter, "ACLU Chief Assails Patriot Spin" *Wired News (*Sept. 23, 2003) (available at http://www.wired.com/news/conflict/0,2100,60541,00.html?tw=wn_story_related).

authority may be used infrequently, however, does not denigrate its importance; to the contrary, it is important that the authority exists for situations in which a section 215 order could be critical to the success of an investigation. Just as a police officer knows that his firearm may be invaluable in preventing crime, even if he cannot predict when he might need to draw it from his holster, section 215 provides investigators an authority they may find crucial to stop a terrorist plot. The fact that the Department has used this authority in a judicious manner should not be used as an argument for repealing the provision altogether.

Section 217: Interception of Computer Trespasser Communications

Text of Section 217:

> Chapter 119 of title 18, United States Code, is amended--
>
> (1) in section 2510--
>
> (A) in paragraph (18), by striking "and" at the end;
>
> (B) in paragraph (19), by striking the period and inserting a semicolon; and
>
> (C) by inserting after paragraph (19) the following:
>
> "(20) 'protected computer' has the meaning set forth in section 1030; and
>
> "(21) 'computer trespasser'--
>
> (A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and
>
> (B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer."; and
>
> (2) in section 2511(2), by inserting at the end the following:
>
> "(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--
>
> (I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;
>
> (II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.".

How Current Law Now Reads:

"18 U.S.C. § 2510. Definitions

…

(20) 'protected computer' has the meaning set forth in section 1030; and

(21) 'computer trespasser'--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer."

"18 U.S.C. § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

…

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser."

Analysis:

Although the criminal wiretap statute ("Title III") allows computer service providers to monitor activity on their machines to protect their rights and property, prior to the passage of the USA PATRIOT Act, it was unclear whether computer owners could obtain law enforcement assistance in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims in taking reasonable steps in their own

defense that would be entirely legal in the physical world. In the physical world, for example, burglary victims may invite the police into their homes to help them catch burglars in the act of committing the crime. Before the USA PATRIOT Act, however, Title III arguably blocked investigators from responding to similar requests from computer service providers in the electronic context. Because service providers often lacked the expertise, equipment, or financial resources required to monitor hacker attacks, they commonly had no effective way to protect themselves from such attacks. This anomaly in the law created the bizarre result that a computer hacker's supposed "privacy" right trumped the privacy rights of his victims.

To correct this problem, section 217 of the USA PATRIOT Act clarified that victims of computer attacks may authorize persons "acting under color of law" to monitor trespassers on their computer systems. Under section 217, law enforcement can intercept the communications of a computer trespasser transmitted to, through, or from a "protected computer"[34] – basically, a federal government computer or a computer that is used in or affects interstate or foreign commerce or communication – so long as four requirements are met. First, the owner or operator of the protected computer must authorize the interception of the trespasser's communications. 18 U.S.C. § 2511(2)(i)(I). Second, the person who intercepts the communication must be lawfully engaged in an ongoing investigation, but the authority to intercept ceases at the conclusion of the investigation. 18 U.S.C. § 2511(2)(i)(II). Third, the person acting under color of law must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. 18 U.S.C. § 2511(2)(i)(III). Fourth, investigators may intercept only the communications sent or received by trespassers. Thus, this section applies only where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of communications to or from non-consenting authorized users. 18 U.S.C. § 2511(2)(i)(IV).

In addition, section 217 amended the wiretap statute to create a definition of "computer trespasser." Pursuant to the provision, a computer trespasser is any person who accesses a protected computer without authorization. The definition, however, explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21). This exemption provides important privacy protections for the customers of Internet service provider ("ISPs"). For example, certain ISPs do not allow their customers to send bulk unsolicited e-mails ("spam"). Customers who send spam would be in violation of the provider's terms of

---

[34] Section 217 adopted the same definition of the term "protected computer" as is specified in 18 U.S.C. § 1030. 18 U.S.C. § 1030(e)(2), in turn, defines "protected computer" to mean a computer—

"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."

service, but do not qualify as trespassers – both because they are authorized users and because they have an existing contractual relationship with the provider.

As explained above, these changes simply brought the law relating to cyber-trespassing in line with the law relating to physical trespassing. Just as in the physical world victims of burglary may call the police to enter their home to catch an intruder, so too under section 217 may victims of hacking and cyber-terrorism now obtain law enforcement assistance in catching intruders on their systems.

Section 217 has played a key role to date in sensitive national security matters, including investigations into hackers' attempts to compromise military computer systems. The provision has also been used to uncover serious criminal conduct. For example, in an investigation into an international conspiracy to use stolen credit cards to fraudulently purchase stolen goods and ship them overseas, FBI agents discovered that members of the conspiracy had illegally accessed a computer in Texas and used it to communicate with each other. Pursuant to section 217, the computer owner requested that the agents monitor the trespassers to identify them and determine how they broke in. Monitoring of the criminals' communications revealed useful evidence about the criminal scheme and has led to an indictment for conspiracy to commit fraud.

Section 217 has provoked some opposition from privacy advocates. The Electronic Privacy Information Center, for example, has criticized section 217, claiming that it:

> places the determination [of whether to permit government access to and interception of communications] solely in the hands of law enforcement and the system owner or operator. In those likely instances in which the interception does not result in prosecution, the target of the interception will never have an opportunity to challenge the activity (through a suppression proceeding). Indeed, such targets would never even have notice of the fact that their communications were subject to warrantless interception. However, the USA PATRIOT Act does include an exception prohibiting surveillance of someone who is known by the owner of the protected computer "to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer." The [never-introduced Anti-Terrorism Act bill], which did not contain such an exception, was so vague that the provision could have been applied to users downloading copyrighted materials off the Web. However, even with this fix, the amendment has little, if anything, to do with legitimate investigations of terrorism.[35]

Similarly, EFF claims that the section, which it asserts has "no apparent connection to preventing terrorism," permits "[g]overnment spying on suspected computer trespassers with no need for court order."[36] Finally, CDT has criticized the Department's

---

[35] *See supra* note 3.

[36] *See* "EFF Analysis of USA PATRIOT Act" (Oct. 31, 2001) (available at http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php).

comparison of physical trespassing and computer trespassing, asserting that section 217 "is a far cry from burglary victims being able to invite [police] officers into their homes to catch burglars, as DOJ argues. Under those circumstances, the burglar is well aware that the victim thinks the burglar is trespassing and that the police are investigating - and has the full panoply of protections available in the criminal system. Anyone designated a computer trespasser has no such rights or knowledge."[37]

All of these objections are seriously misplaced. To begin with, when homeowners seek the police's assistance in detecting and apprehending physical trespassers, there is no obligation whatsoever to notify or warn those trespassers that the police have begun an investigation or are physically present on the trespassed property, and the CDT's suggestion to the contrary is simply incorrect. Moreover, a trespasser, whether a computer trespasser or a physical trespasser, has no reasonable expectation of privacy precisely because he or she is a trespasser, and thus has no legitimate privacy rights that merit or receive legal recognition

As stated above, section 217 appropriately places computer owners' privacy rights above the non-existent "privacy" rights of trespassers. Computer operators are not required to involve law enforcement if they detect trespassers on their systems. Section 217 simply gives them the option of doing so. Moreover, it is worth noting that section 217 also preserves the privacy of law-abiding computer users. Officers cannot agree to help a computer owner unless (1) they are intercepting the communications of a computer trespasser; (2) they obtain the permission of the owner or operator of the computer through which the communications have traveled; (3) they are engaged in a lawful investigation; (4) there is reason to believe that the communications will be relevant to that investigation; and (5) their activities will not acquire the communications of non-trespassers.

Section 218: Foreign Intelligence Information

Text of Section 218:

> Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking "the purpose" and inserting "a significant purpose".

How Current Law Now Reads:

> **"§ 1804. Applications for court orders**
>
> (a) Submission by Federal officer; approval of Attorney General; contents
>
> Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based

[37] Center for Democracy & Technology, "Setting the Record Straight" (Oct. 27, 2003) (available at http://www.cdt.org/security/usapatriot/031027cdt.shtml).

upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include—

. . .

(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate--

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

(E) including a statement of the basis for the certification that--

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques."

"§ 1823. Application for order

(a) Submission by Federal officer; approval of Attorney General; contents

Each application for an order approving a physical search under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge of the Foreign Intelligence Surveillance Court. Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements for such application as set forth in this subchapter. Each application shall include--

. . .

(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the advice and consent of the Senate-

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the search is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

> (E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D);

Analysis:

Before the passage of the USA PATRIOT Act, a metaphorical "wall" largely separated intelligence personnel from law enforcement personnel within the federal government. This "wall" dramatically limited vital information sharing and greatly hindered the Department's counterterrorism efforts.

The origins of this "wall" can be traced back to the pre-USA PATRIOT Act requirement that applications for orders authorizing electronic surveillance or physical searches under FISA had to include a certification from a high-ranking Executive Branch official that "*the* purpose*"* of the surveillance or search was to gather foreign intelligence information. As interpreted by the courts and later the Justice Department, this requirement meant that the "primary purpose" of the collection had to be to obtain foreign intelligence information rather than evidence of a crime. Over the years, the prevailing interpretation and implementation of the "primary purpose" standard had the effect of sharply limiting coordination and information sharing between intelligence and law enforcement personnel. Because the courts evaluated the government's purpose for using FISA at least in part by examining the nature and extent of coordination between intelligence and law enforcement officials, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence, had become the primary purpose of the surveillance or search.

During the 1980s, the Department operated under a set of largely unwritten rules that limited to some degree information sharing between intelligence and law enforcement officials. In 1995, however, the Department established formal procedures that more clearly separated law enforcement and intelligence investigations and limited the sharing of information between intelligence and law enforcement personnel more than the law required. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation's primary purpose. To be sure, the procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers, while at the same time ensuring that the FBI would be able to obtain or continue FISA coverage and later use the fruits of that coverage in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement investigators became even more limited in practice than was allowed in theory under the Department's procedures. Due both to confusion about when sharing was permitted and to a perception that improper information sharing could end a career, a culture developed within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

Section 218 of the USA PATRIOT Act, however, helped to bring down the perceived "wall" separating intelligence agents from law enforcement agents. It not only

erased the impediment to more robust information sharing between intelligence and law enforcement personnel; it also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing.

Section 218 did this by eliminating the "primary purpose" requirement. Under section 218 of the USA PATRIOT Act, the government may now conduct FISA surveillance or searches if foreign-intelligence gathering is a "significant" purpose of the surveillance or search, thus eliminating the need for courts to compare the relative weight of the "foreign intelligence" and "law enforcement" purposes of the surveillance or search. This has allowed for significantly more coordination and sharing of information between intelligence and law enforcement personnel.

FISA contains ample safeguards to ensure that innocent Americans are not subject to government surveillance. First, under section 218, the government may conduct a physical search or electronic surveillance under FISA only if a significant purpose of the search is to obtain foreign intelligence information. And second, the government must have probable cause to believe that the target of a FISA physical search or electronic surveillance is a foreign power or agent of a foreign power, such as a terrorist or spy.

The Department has moved aggressively to implement section 218 and bring down "the wall." Following passage of the Act, the Department adopted new procedures designed to increase information sharing between intelligence and law enforcement agents, which were affirmed by the Foreign Intelligence Surveillance Court of Review on November 18, 2002. The Attorney General also instructed every U.S. Attorney to review intelligence files to discover whether there was a basis for bringing criminal charges against the subjects of intelligence investigations. Thousands of files have been reviewed as part of this process. The Attorney General likewise directed every U.S. Attorney to develop a plan to monitor terrorism and intelligence investigations, and to ensure that information about terrorist threats is shared with other agencies and that criminal charges are considered in those investigations.

The increased coordination and information sharing between intelligence and law enforcement personnel facilitated by section 218 has allowed the FBI to approach terrorism investigations not as separate criminal and intelligence investigations, each with separate agents developing separate information and evidence on parallel tracks, but as a single integrated investigation that enables us to "connect the dots." In the course of a terrorism investigation, agents can now use all the tools in the toolbox, utilizing both criminal investigative tools and intelligence tools, as long as the requirements for each are properly met. This approach has yielded extraordinary dividends, enabling the Department to open numerous criminal investigations, disrupt terrorist plots, bring numerous criminal charges, and convict numerous individuals in terrorism cases.

For example, the removal of the "wall" separating intelligence and law enforcement personnel played a crucial role in the Department's successful dismantling of a Portland, Oregon terror cell, popularly known as the "Portland Seven." Members of

this terror cell had attempted to travel to Afghanistan in 2001 and 2002 to take up arms with the Taliban and al Qaeda against United States and coalition forces fighting there. Law enforcement agents investigating that case learned from one member of the terror cell, Jeffrey Battle, through an undercover informant, that before the plan to go to Afghanistan was formulated, at least one member of the cell had contemplated attacking Jewish schools or synagogues and had even been casing such buildings to select a target for such an attack. By the time investigators received this information from the undercover informant, they had information that a number of other persons besides Battle had been involved in the Afghanistan conspiracy. But while several of these other individuals had returned to the United States from their unsuccessful attempts to reach Afghanistan, investigators did not yet have sufficient evidence to arrest them.

Before the USA PATRIOT Act, prosecutors would have faced a dilemma in deciding whether to arrest Battle immediately. If prosecutors had failed to act, lives could have been lost through a terrorist attack. But if prosecutors had arrested Battle in order to prevent a potential attack, the other suspects in the investigation would have undoubtedly scattered or attempted to cover up their crimes. Because of section 218, however, it was clear that the FBI agents could conduct FISA surveillance of Battle to detect whether he had received orders from an international terrorist group to reinstate the domestic attack plan on Jewish targets and keep prosecutors informed as to what they were learning. This gave prosecutors the confidence not to arrest Battle prematurely while they continued to gather evidence on the other members of the cell. Ultimately, prosecutors were able to collect sufficient evidence to charge seven defendants and then to secure convictions and prison sentences ranging from three to eighteen years for the six defendants taken into custody. Without section 218, this case likely would have been referred to as the "Portland One" rather than the Portland Seven.

Likewise, the Department shared information pursuant to section 218 before indicting Sami Al-Arian and several co-conspirators on charges related to their involvement with the Palestinian Islamic Jihad (PIJ). PIJ is alleged to be one of the world's most violent terrorist outfits. It is responsible for murdering over 100 innocent people, including Alisa Flatow, a young American killed in a bus bombing near the Israeli settlement of Kfar Darom. The indictment details that Al-Arian served as the secretary of the Palestinian Islamic Jihad's governing council ("Shura Council"). He was also identified as the senior North American representative of the PIJ.

In this case, section 218 of the USA PATRIOT Act enabled prosecutors to consider all evidence against Al-Arian and his co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach was essential to enabling prosecutors to build their case and pursue the proper charges. The trial in this case is currently scheduled to start later this year.

Prosecutors and investigators also used information shared pursuant to section 218 in investigating the defendants in the so-called "Virginia Jihad" case. This

prosecution involved members of the Dar al-Arqam Islamic Center, who trained for jihad in Northern Virginia by participating in paintball and paramilitary training, including eight individuals who traveled to terrorist training camps in Pakistan or Afghanistan between 1999 and 2001. These individuals are associates of a violent Islamic extremist group known as Lashkar-e-Taiba (LET), which operates in Pakistan and Kashmir, and that has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring charges against these individuals. Six of the defendants have pleaded guilty, and three were convicted in March 2004 of charges including conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban. These nine defendants received sentences ranging from a prison term of four years to life imprisonment.

Moreover, the information sharing between intelligence and law enforcement personnel made possible by section 218 was useful in the investigation of two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged in 2003 with conspiring to provide material support to al Qaeda and HAMAS. The complaint against these two individuals alleges that an FBI undercover operation developed information that Al-Moayad boasted that he had personally handed Usama Bin Laden $20 million from his terrorist fund-raising network and that Al-Moayad and Zayed flew from Yemen to Frankfurt, Germany in 2003 with the intent to obtain $2 million from a terrorist sympathizer (portrayed by a confidential informant) who wanted to fund al Qaeda and HAMAS. During their meetings, Al-Moayad and Zayed specifically promised the donor that his money would support HAMAS, al Qaeda, and any other mujahideen, and "swore to Allah" that they would keep their dealings secret. Following their indictment, Al-Moayad and Zayed were extradited to the United States from Germany, and both were convicted in March 2005 of conspiring to provide material support to a foreign terrorist organization.

In addition, the Department used section 218 to gain access to intelligence, which facilitated the indictment of Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation (BIF). Arnaout conspired to fraudulently obtain charitable donations in order to provide financial assistance to Chechen rebels and organizations engaged in violence and terrorism. Arnaout had a long-standing relationship with Usama Bin Laden and used his charity organization both to obtain funds illicitly from unsuspecting Americans for terrorist organizations, such as al Qaeda, and to serve as a channel for people to contribute money knowingly to such groups. Arnaout ultimately pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

The broader information sharing made possible by section 218 also assisted the prosecution in San Diego of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in two guilty pleas. Two defendants, Muhamed Abid Afridi and Ilyas Ali, admitted that they conspired to distribute approximately five metric tons of hashish and 600 kilograms of heroin originating in Pakistan to undercover United States law enforcement officers. Additionally, they admitted that they conspired to receive, as

partial payment for the drugs, four "Stinger" anti-aircraft missiles that they then intended to sell to the Taliban, an organization they knew at the time to be affiliated with al Qaeda. Afridi and Ali pleaded guilty to the felony charges of conspiracy to provide material support to terrorists and conspiracy to distribute heroin and hashish The lead defendant in the case is currently awaiting trial.

Finally, section 218 was critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq as well as two counts of perjury. Before the Gulf War, Dumeisi passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence agents conducting surveillance of Dumeisi pursuant to FISA coordinated and shared information with law enforcement agents and prosecutors investigating Dumeisi for possible criminal violations. Because of this coordination, law enforcement agents and prosecutors learned from intelligence agents of an incriminating telephone conversation that took place in April 2003 between Dumeisi and a co-conspirator. This phone conversation corroborated other evidence that Dumeisi was acting as an agent of the Iraqi government and provided a compelling piece of evidence at his trial.

As evidenced by these examples and many others, section 218 has been crucial to the success of the Department's efforts in the war against terrorism by allowing for the full coordination between intelligence and law enforcement that is necessary to conduct an integrated counterterrorism effort.

Notwithstanding section 218's importance to the fight against terrorism, this provision has been the subject of criticism. The ACLU, for example, has complained that section 218 allows the FBI to circumvent constitutional safeguards by conducting a search or wiretap for the purpose of investigating a crime without demonstrating probable cause that a crime has been committed.[38] That is incorrect. In 2002, the FISA Court of Review found that section 218 was constitutional; that Court squarely held "that FISA as amended [by the USA PATRIOT Act] is constitutional because the surveillances it authorizes are reasonable." *In re Sealed Case*, 310 F.3d 717, 746 (FISCR 2002).

The ACLU also predicted at the time of the USA PATRIOT Act's passage: "courts will exclude the evidence gathered from surveillance conducted under [s]ection 218 because the probable cause of crime requirement was not met for a search conducted primarily to gather evidence of crime."[39] Experience, however, has revealed that this criticism of section 218 is without merit. In the first place, the Department is unaware of a single case where evidence gathered from FISA surveillance authorized pursuant to section 218 has been excluded from any criminal case on the grounds identified by the

[38] "How the Anti-Terrorism Bill Enables Law Enforcement to Use Intelligence Authorities to Circumvent the Privacy Protections Afforded in Criminal Cases", (Oct. 23, 2001) (available at http://www.asata.org/resources/articles/civil_rights/ACLU_loss_of_privacy.pdf).
[39] *Id*.

ACLU. Indeed, such evidence has been extremely important at trial in many of the criminal cases discussed above.

Many of the criticisms of section 218 are based on a false dichotomy, which strictly separates obtaining foreign intelligence information from gathering evidence for use in a criminal trial. Such a dichotomy, however, represents the same pre-9/11 mindset that led to the creation of the "wall" separating intelligence and law enforcement personnel, which prevented the sharing of valuable information. As the FISA Court of Review noted, for instance, "the definition of foreign intelligence information includes evidence of crimes such as espionage, sabotage or terrorism." *In re Sealed Case*, 310 F.3d 717, 723 (FISCR 2002). The Court therefore concluded that it is "virtually impossible" to read FISA "to exclude from its purpose the prosecution of foreign intelligence crimes." *Id* at 724. Indeed, the Court explained that "arresting and prosecuting terrorist agents of, or spies for, a foreign power may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity." *Id*. The government after all does not obtain intelligence for the sake of gathering intelligence. Rather, it gathers intelligence, among other reasons, to disrupt terrorist plots, and one of the best ways to prevent terrorist acts is to arrest and prosecute terrorists before they are able to strike.

Section 220: Out-of-District Service of Search Warrants for Electronic Evidence

Text of Section 220:

> (a) IN GENERAL- Chapter 121 of title 18, United States Code, is amended--
>
> > (1) in section 2703, by striking "under the Federal Rules of Criminal Procedure" every place it appears and inserting "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation"; and
> >
> > (2) in section 2711--
> >
> > > (A) in paragraph (1), by striking "and";
> > >
> > > (B) in paragraph (2), by striking the period and inserting "; and"; and
> > >
> > > (C) by inserting at the end the following:
> > >
> > > "(3) the term `court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.".

How Current Law Now Reads:

"§ 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, **only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains **a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.—

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a

subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a **warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure; or

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer."

"§ 2711. Definitions for chapter

As used in this chapter--

. . .

(3) the term 'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation."

Analysis:

Federal law requires investigators to use a search warrant to compel an Internet service provider to disclose unopened e-mail messages that are less than six months old.

See 18 U.S.C. § 2703(a). But because Rule 41 of the Federal Rules of Criminal Procedure requires that the "property" to be obtained through a search warrant be located "within the district" of the issuing court, some courts, prior to the passage of the USA PATRIOT Act, declined to issue warrants for e-mail stored on computer servers located in other judicial districts. For example, in a murder investigation centered in Massachusetts, law enforcement officials, in order to obtain e-mail stored on an ISP's server in the Silicon Valley, were not allowed to obtain a search warrant from a judge in Massachusetts but rather were forced to seek a search warrant in California.

Not only did this requirement deprive the judges most knowledgeable about a particular case of the ability to evaluate search warrant requests, forcing judges and prosecutors with little or no knowledge of an investigation to process search warrants, but it also placed an enormous administrative burden on those districts in which major ISPs are located, such as the Northern District of California and the Eastern District of Virginia. Before the USA PATRIOT Act, these districts were inundated with search warrant requests for electronic evidence. For example, before the enactment of the USA PATRIOT Act, the U.S. Attorney's Office in Alexandria, Virginia was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for records from a particular ISP. For each of these applications, an Assistant United States Attorney in Virginia and a law enforcement agent in the district had to learn all of the details of another district's investigation to present an affidavit to the court in support of the application for the search warrant. The result was that agents and attorneys spent many hours each month processing applications for investigations conducted in other districts rather than working on cases involving crimes occurring within their district. In addition, requiring investigators to go through the aforementioned process of seeking warrants to obtain electronic evidence in distant jurisdictions often slowed time-sensitive investigations.

Section 220 of the USA PATRIOT Act solved these problems by allowing courts with jurisdiction over a particular investigation to order the release of stored communications relevant to that investigation through a search warrant valid in another specified judicial district. Therefore, for example, in the investigation of a murder occurring in Pennsylvania, a federal judge in Pennsylvania now may issue a search warrant for e-mail messages pertaining to the investigation that are stored on a server in California.

This enhanced ability to obtain electronic evidence efficiently has been used by the Department on a frequent basis and proved helpful in several terrorism investigations as well as time-sensitive criminal investigations. For example, as Assistant Attorney General Chris Wray testified before the Senate Judiciary Committee on October 21, 2003, section 220 was useful in the Portland terror cell case because "the judge who was most familiar with the case was able to issue the search warrants for the defendants' e-mail accounts from providers in other districts, which dramatically sped up the investigation and reduced all sorts of unnecessary burdens on other prosecutors, agents and courts." Section 220 was also helpful in the investigations of a Northern Virginia terror cell and the infamous "shoebomber" Richard Reid.

The provision was also used in a time-sensitive investigation involving a fugitive, who after abducting his estranged wife and sexually assaulting her, fled West Virginia in a stolen car to avoid capture armed with a sawed-off shotgun. While in flight, he continued to contact cooperating individuals by e-mail using an ISP located in California. Using the authority provided by section 220, investigators in West Virginia were able to quickly obtain an order from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account, rather than wasting additional time obtaining such an order from a California court. Within a day of the order being issued, the ISP had released information to the government revealing that the fugitive had contacted individuals from a public library in a small town in South Carolina. The very next day, Deputy U.S. Marshals went to the town and arrested the fugitive. In this case, the fast turn-around on the order for information related to the fugitive's e-mail account made possible by section 220 was crucial to capturing the fugitive.

In addition to allowing law enforcement to gain access to information quickly in time-sensitive investigations, section 220 has significantly improved the Justice Department's ability to mount large-scale child-pornography investigations. The ability to obtain search warrants in the jurisdiction of a child-pornography investigation rather than in the jurisdiction of the Internet service provider is critical to the success of a complex, multi-jurisdictional child-pornography case. In the absence of section 220, law enforcement agents would either have to spend hours briefing other agents across the country to obtain warrants or travel hundreds or thousands of miles to present a warrant application to a local magistrate judge. In practice, one of two things would often occur in light of limited law enforcement resources: either the scope of the investigation would be narrowed or the case would be deemed impractical at the outset and dropped.

Finally, section 220 has eased the administrative burden on U.S. Attorney's Offices and courts that are located in districts that are home to ISPs. Now, investigators and prosecutors in those districts, such as the Northern District of California and Eastern District of Virginia, can spend their time handling cases involving crimes committed in their home districts rather than spending their time getting up to speed and handling requests for search warrants necessary to obtain electronic evidence pertaining to investigations being conducted by other U.S. Attorney's Offices.

While section 220 has not generated a significant amount of criticism, some privacy advocates have opposed its renewal for two reasons. First, they claim that the provision allows law enforcement officers to pick and choose the courts in which they will seek warrants, thus allowing them to "shop" for judges with a pro-law enforcement bias.[40] This criticism, however, reflects a fundamental misunderstanding of section 220. Section 220 does not allow investigators to seek search warrants for electronic evidence from any court in the country. Rather, it allows investigators to seek a search warrant only in a court with jurisdiction over the offense under investigation. Thus, for example,

[40] *See* Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 220: 'Nationwide Service of Search Warrants for Electronic Evidence" (Mar. 16, 2004) (available at http://www.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/sunset/220.php).

while a court in Ohio may issue a search warrant for electronic evidence stored in California in the investigation of a murder committed in Ohio, a judge located in a district with no connection to the investigation, such as North Dakota, is not allowed to issue such a warrant. In practice, judges and prosecutors with the most knowledge of a particular investigation are now permitted to process requests for search warrants to obtain electronic evidence in that investigation.

Second, critics such as the EPIC allege that section 220 reduces the chances that Internet service providers will seek to challenge search warrants for electronic evidence.[41] According to them, a Virginia ISP is less likely to go through the additional time and expense of challenging a search warrant issued by a judge in Oregon than one issued by a judge in Virginia. This argument is flawed for several reasons. To begin with, the nationwide reach of search warrants issued pursuant to section 220 is no different than the nationwide reach of grand jury subpoenas that are issued in federal criminal investigations. Therefore, just as a Virginia company receiving a subpoena from an Oregon grand jury must challenge that subpoena in Oregon, so too must a Virginia ISP receiving a search warrant issued by a federal judge in Oregon challenge that warrant in Oregon. The latter case, in fact, should be far less troubling to privacy advocates as grand jury subpoenas do not require prior judicial approval while search warrants do require such approval. Moreover, since the passage of section 220, the Justice Department has not observed any noticeable decrease in the frequency of instances in which search warrants for electronic evidence have been challenged by ISPs, which rarely challenged such warrants prior to the passage of the Act. This is not surprising as the most popular ISPs are sufficiently large that any additional expense from challenging a search warrant issued by a judge in another district does not constitute a significant deterrent. Indeed, the Justice Department is not aware of any complaints from Internet service providers regarding section 220.

Section 223: **Civil Liability for Certain Unauthorized Disclosures**

Text of Section 223:

> (a) Section 2520 of title 18, United States Code, is amended--
>
> (1) in subsection (a), after "entity", by inserting ", other than the United States,";
>
> (2) by adding at the end the following:
>
> "(f) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector

[41] *See id*.

General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination."; and

(3) by adding a new subsection (g), as follows:

"(g) IMPROPER DISCLOSURE IS VIOLATION- Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a)."

(b) Section 2707 of title 18, United States Code, is amended--

(1) in subsection (a), after "entity", by inserting ", other than the United States,";

(2) by striking subsection (d) and inserting the following:

"(d) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination."; and

(3) by adding a new subsection (g), as follows:

"g) IMPROPER DISCLOSURE- Any willful disclosure of a `record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.".

(c)(1) Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

"Sec. 2712. Civil actions against the United States

(a) IN GENERAL- Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

(1) actual damages, but not less than $10,000, whichever amount is greater; and

(2) litigation costs, reasonably incurred.

(b) PROCEDURES-

(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.'.

(3) Any action under this section shall be tried to the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) EXCLUSIVE REMEDY- Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) STAY OF PROCEEDINGS-

(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms `related criminal case' and `related investigation' mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall

consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.'"

(2) The table of sections at the beginning of chapter 121 is amended to read as follows:

"2712. Civil action against the United States.".

How Current Law Now Reads:

"18 U.S.C. § 2520. Recovery of civil damages authorized

…

(a) In general.--Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

…

(f) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper disclosure is violation.--Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a)."

"18 U.S.C. § 2707. Civil action

(a) Cause of action.--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

…

(d) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved

determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

…

(g) Improper disclosure.--Any willful disclosure of a 'record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter."

"**18 U.S.C. § 2712. Civil actions against the United States**

(a) In general.--Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

(1) actual damages, but not less than $10,000, whichever amount is greater; and

(2) litigation costs, reasonably incurred.

(b) Procedures.—

(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

(3) Any action under this section shall be tried to the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(b) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the

violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) Exclusive remedy.--Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) Stay of proceedings.--(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms "related criminal case" and "related investigation" mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party."

Analysis:

Prior to the passage of the USA PATRIOT Act, individuals were permitted only in limited circumstances to file a cause of action and collect money damages against the United States if government officials unlawfully disclosed sensitive information collected through wiretaps and electronic surveillance. Thus, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. Section 223 of the USA PATRIOT Act remedied this inequitable situation; it created an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

Section 223 permits persons harmed by willful violations of the criminal wiretap statute or the prohibitions on the improper use and disclosure of information contained in FISA to file a claim against the United States for at least $10,000 in damages, plus costs. Section 223 also broadened the circumstances under which administrative discipline could be imposed upon a federal official who improperly handled sensitive information; now, if the relevant court or agency finds a (possible) legal violation, section 223

requires the agency to initiate a proceeding in order to determine the appropriate disciplinary action.

To date, no complaints have been filed against Department employees pursuant to section 223. This is a reflection of the professionalism of the Department's employees as well as their commitment to the rule of law. The Department believes, however, that it is important that section 223 remain on the books in order to provide an important disincentive to those who would unlawfully disclose intercepted communications as well as give compensation to those whose privacy is compromised by any such unlawful disclosure.

The Justice Department does not believe that section 223 has generated any significant criticism. For instance, CDT lists the section as one of the USA PATRIOT Act provisions scheduled to sunset that is not controversial.[42] Indeed, EPIC has even praised section 223 as "serv[ing] to limit misuse of communications captured through lawful surveillance,"[43] and EFF has stated that the provision contains "valuable tools and should certainly be renewed."[44]

Section 225: Immunity for Compliance with FISA Wiretap

Text of Section 225:

> Section 105 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805) is amended by inserting after subsection (g) the following:
>
> "(h) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act.".

How Current Law Now Reads:

> **"§ 1805. Issuance of Order**
>
> (a) Necessary findings
>
> Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that--
>
> > (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
> >
> > (2) the application has been made by a Federal officer and approved by the Attorney General;

---

[42] See *supra* note 2.

[43] Electronic Privacy Information Center, "The USA PATRIOT Act," (available at http://www.epic.org/privacy/terrorism/usapatriot).

[44] Electronic Frontier Foundation, "Let the Sun Set on PATRIOT – Section 223 "Civil Liability for Certain Unauthorized Disclosures", *EFFector* (Nov. 19, 2004) (available at http://eff.org/effector/17/43.php#IV).

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that--

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or 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) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and

(5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

. . .

(i) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act."

Analysis:

Pursuant to FISA, the United States may obtain electronic surveillance and physical search orders from the FISA Court concerning an entity or individual whom the court finds probable cause to believe is an agent of a foreign power. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers to carry out such court orders.

In the criminal and civil contexts, those who disclose information pursuant to a subpoena or court order are generally exempted from liability. For example, those assisting the government in carrying out criminal investigative wiretaps are provided with immunity from civil liability. *See* 18 U.S.C. § 2511(2)(a)(ii) ("No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter."). This immunity is important because it helps to secure the prompt cooperation of private parties with law enforcement officers to ensure the effective implementation of court orders.

Prior to the passage of the USA PATRIOT Act, however, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying

out surveillance orders issued by the FISA Court under FISA. Section 225 ended this anomaly in the law by immunizing from civil liability communications service providers and others who assist the United States in the execution of such FISA orders, thus helping to ensure that such entities and individuals will comply with orders issued by the FISA Court without delay. For example, in the investigation of an espionage subject, the FBI was able to convince a company to assist in the installation of technical equipment pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order.

Because section 225 simply extends to the FISA context the exemption long applied in the civil and criminal contexts, where individuals who disclose information pursuant to a subpoena or court order generally are immune from liability for disclosure, it has not provoked any significant opposition. For example, CDT has taken the position that section 225 is not controversial.[45] Moreover, the provision has been praised for protecting those companies and individuals who are simply fulfilling their legal obligations.[46]

[45] *See supra* note 2.

[46] *See* Ronald L. Plesser, James J. Halpert & Emilio W. Cividanes, "USA PATRIOT Act for Internet and Communications Companies," Computer and Internet Lawyer, March 2002 (calling section 225 "a very important expansion of service provider immunity for compliance with FISA").