Order Code RL32186

USA PATRIOT Act Sunset: Provisions That Expire on December 31, 2005

Updated January 27, 2005

Charles Doyle
Senior Specialist
American Law Division

USA PATRIOT Act Sunset: Provisions That Expire on December 31, 2005

Summary

Several sections of Title II of the USA PATRIOT Act (the act) and one section of the Intelligence Reform and Terrorism Prevention Act each relating to enhanced foreign intelligence and law enforcement surveillance authority expire on December 31, 2005. The authority remains in effect only with respect to foreign intelligence investigations begun before sunset or to offenses or potential offense begun or occurring before that date. Aside from the fact there may be some disagreement of whether a "potential offense" is a suspected crime, and/or an incomplete crime, and/or a future crime, after December 31, 2005 the law reverts to its previous form unless it has been amended or extended in the interim. The 9/11 Commission mentioned the approaching sunset and thought as a general matter that "a full and informed debate on the PATRIOT Act would be healthy."

The consequences of sunset are not the same for every expiring section. In some instances the temporary provision has been replaced with a permanent one; in some, other provisions have been made temporary by attachment to an expiring section; in still others, the apparent impact of termination has been mitigated by related provisions either in the act or elsewhere.

The temporary provisions are: sections 201 (wiretapping in terrorism cases), 202 (wiretapping in computer fraud and abuse felony cases), 203(b) (sharing wiretap information), 203(d) (sharing foreign intelligence information), 204 (Foreign Intelligence Surveillance Act (FISA) pen register/trap & trace exceptions), 206 (roving FISA wiretaps), 207 (duration of FISA surveillance of non-United States persons who are agents of a foreign power), 209 (seizure of voice-mail messages pursuant to warrants), 212 (emergency disclosure of electronic surveillance), 214 (FISA pen register/ trap and trace authority), 215 (FISA access to tangible items), 217 (interception of computer trespasser communications), 218 (purpose for FISA orders), 220 (nationwide service of search warrants for electronic evidence), 223 (civil liability and discipline for privacy violations), and 225 (provider immunity for FISA wiretap assistance); and in the Intelligence Reform and Terrorism Prevention Act, section 6001 ("lone wolf" FISA orders).

The unimpaired provisions of Title II are: sections 203(a)(sharing grand jury information), 203(c)(procedures for grand jury and wiretap information sharing that identifies U.S. persons), 205 (employment of translators by the Federal Bureau of Investigation), 208 (adding 3 judges to FISA court), 210 (access to payment source information from communications providers), 211 (communications services by cable companies), 213 (sneak and peek warrants), 216 (law enforcement pen register/ trap and trace changes), 219 (single-jurisdiction search warrants for terrorism), 221 (trade sanctions), and 222 (provider assistance to law enforcement agencies).

This report is available in an abridged version (without its footnotes, chart, and most of its citations to authority) as CRS Report RS21704, *USA PATRIOT Act Sunset: A Sketch.*

Contents

List of Tables

USA PATRIOT Act Sunset: Provisions That Expire on December 31, 2005

> (a) In General. – Except as provided in subsection (b), this title and the amendments made by this title (other than sections 203(a) 203(c), 205, 208, 210, 211, 213, 216, 219, 221, and 222, and the amendments made by those sections) shall cease to have effect on December 31, 2005.
>
> (b) Exceptions. – With respect to any particular foreign intelligence investigation that began before the date on which the provisions referred to in subsection (a) cease to have effect, or with respect to any particular offense or *potential* offense that began or occurred before the date on which such provisions cease to have effect, such provisions shall continue in effect. P.L. 107-56, §224, 18 U.S.C. 2510 note (emphasis added).

> (a) In General.– Section 101(b)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 180(b)(1) is amended by adding at the end the following new subparagraph: "(C) engages in international terrorism or activities in preparation therefore; or".
>
> (b) Sunset. – The amendment made by subsection (a) shall be subject to the sunset provision in section 224 of Public Law 107-56 (115 Stat. 295), including the exception provided in subsection (b) of such section 224. P.L. 108-458, §6001, 118 Stat. 3742 (2004).

Introduction

Subsection 224(a) of the USA PATRIOT Act (the act) indicates that various sections in Title II of the act are to remain in effect only until December 31, 2005. Subsection 224(b) creates two exceptions for matters that straddle the termination date, one for foreign intelligence investigations and the other for criminal cases. Even a quick reading of section 224 raises a number of questions. What is the substance of the temporary sections that disappear on December 31, 2005? What is the breath of the subsection 224(b) exceptions? What is the fate and impact of amendments to the expiring sections or to related provisions of law, enacted after passage of the act but before December 31, 2005? What is the substance of the sections in Title II that continue on unimpaired by virtue of their inclusion in the "other-than" list of the subsection 224(a)?

These questions are among those likely to be asked as twilight approaches. The 9/11 Commission noted the coming sunset, and expressed the belief that as a general matter, "[b]ecause of the concerns regarding the shifting balance of power to the government ...a full and informed debate on the Patriot Act would be healthy," *9/11 Commission Report*, 394 (2004).

The expiring sections deal with the power of federal authorities to conduct searches and seizures, generally searches and seizures relating to communications.

In most instances, they allow authorities to move more quickly; they reduce the required layers of administrative and judicial approval; they permit searches and seizures of a wider range of targets thus making these tools available earlier in an investigation; and they allow authorities to coordinate their activities. In doing so, they make it more likely that terrorism and crime will be prevented and that terrorists and criminals will be caught and punished. They accomplish these things, however, by easing or removing safeguards designed to protect individual privacy and to prevent government abuse. And so, they increase the risk that government authority will be abused and that the privacy of those who are neither terrorists nor criminals will be invaded. The debate over sunset is a debate of where the balance should be struck.

To further complicate the debate, in some instances the expiring sections curtail rather than expand governmental authority; bolster rather than erode the safeguards against governmental overreaching or abuse of authority.

Impact of Sunset

Subject to the exceptions of subsection 224(b), the new sections of law and the amendments to existing law, created by the sections of the act that expire on December 31, 2005, will cease to exist after that date. The same is true for any subsequent amendments to the expiring sections. They expire along with their hosts. Pre-existing provisions of law, repealed or amended by the expiring sections, will be revived automatically, unless they themselves have been repealed or amended by intervening legislation (as several have).

The impact of subsection 224(b) is somewhat more difficult to discern. It provides two standards: one with respect to "any particular foreign intelligence investigations that began" before sunset and a second with respect to "any particular offense or potential offense that began or occurred" before sunset, P.L. 107-56, §224, 18 U.S.C. 2510 note. The first seems fairly straightforward. The authority granted by an expiring provision of the act may be exercised after sunset or may continue to be exercised after sunset, with respect to any foreign intelligence investigation initiated before sunset.

The second comes with questions. What is a "potential offense"? Does the phrase refer to pre-sunset circumstances whose criminality is determined in a post-sunset investigation? Or does the phrase also include post-crimes that evolved out of pre-sunset circumstances which themselves constituted neither crimes nor elements of a crime? As a general rule, when Congress uses ordinary words, it is presumed to have intended them to have their commonly understood meaning.[1] The word "potential" usually contemplates the incomplete, the unfulfilled, the undeveloped, or the unawakened possibility, rather than the suspected or uncertain

---

[1] *National Railroad Passenger Corp. v. Morgan*, 536 U.S. 101, 109-110 (2002), *quoting, Walters v. Metropolitan Ed. Enterprises, Inc.*, 519 U.S. 202, 207 1997)("In the absence of an indication to the contrary, words in a statute are assumed to bear their ordinary, contemporary, common meaning").

possibility.[2] That might suggest the term was intended at least in part to apply to post-sunset crimes that grow out pre-sunset circumstances. Although hardly a term of art, earlier federal courts have used the term to describe possible past offenses in some cases,[3] and to describe possible future offenses in others.[4] Congress in subsection 224(b), however, is not referring to all "potential offenses," but only to those "that began or occurred" before sunset. Offenses occurring entirely after sunset cannot be said to have begun or occurred beforehand. Thus, although it is scarcely beyond debate, Congress appears to have added the term "potential offense" out of an abundance of caution lest the exception be read to extend only to investigations of conduct whose criminality was known prior to sunset but not of pre-sunset conduct whose innocence or criminality was only ultimately determined after sunset.

Temporary Law Enforcement Sections of Title II

The expiring law enforcement sections of Title II of the USA PATRIOT Act involve three communications-related aspects of federal law: wiretapping; stored electronic communications and communication transaction records; and pen registers and trap and trace devices. Federal law prohibits the interception of telephone, face to face, and electronic communications (wiretapping), subject to certain exceptions including a procedure for judicially supervised law enforcement interceptions, 18 U.S.C. 2510-2520 (Title III).[5] With the approval of senior Justice Department

---

[2] "**[P]otential**, *adj*. Capable of coming into being; possible," BLACK'S LAW DICTIONARY, 1188 (7th ed. 1999); "**potential.** adj. [ME *potencial*, LL *potentialis* potential, powerful, fr. LL *potential* dynamis, state of that which is not yet fully realized & L *potentia* potency] 1a. existing in possibility: having the capacity or a strong possibility for development into a state of actuality... b. having the capacity for acting or being acted upon and hence for undergoing change ...." WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY OF THE ENGLISH LANGUAGE UNABRIDGED, 1775 (1986)(phonetic pronunciation guide omitted).

[3] *E.g.*, *United States v. Hart*, 324 F.3d 575, 579 (8th Cir. 2003)(emphasis added)("Hart provided his corporation's tax identification number to Plaza Motors, and Plaza Motors reported all its commission payments to the government on Form 1099s ... Neither Hart nor Midtown Motors filed tax returns for the income reported by Plaza Motors. Thus, the government clearly had notice of a *potential offense*"); *United States v. Rivera*, 906 F.2d 319, 322 (7th Cir. 1990)(emphasis added)("The court below found that there were three *potential offenses* that needed investigation or citation [when officers stopped Rivera's car]: The material obstruction, Rivera's erratic driving, and his passenger's (later discovered) nonwearing of a seat belt").

[4] *E.g.*, *Screws v. United States*, 325 U.S. 91, 157 (1945)(Roberts, J., dissenting)(emphasis added)("By ... establishing as federal crimes violations of the vast, undisclosed range of the Fourteenth Amendment, this Court now creates new delicate and complicated problems for the enforcement of the criminal law. The answers given to these problems, in view of the tremendous scope of *potential offenses* against the Fourteenth Amendment, are bound to produce a confusion detrimental to the administration of criminal justice "); *Wyner v. Struhs*, 254 F.Supp.2d 1297, 1302 (S.D.Fla. 2003)(emphasis added)("Does the regulation [against nudity on a state beach] serve a significant government interest? ... That interest in protecting the public from the *potential offense* of nudity meets this standard ").

[5] 18 U.S.C. 2510-2522 (chapter 119 of title 18 of the United States Code) is often referred to as Title III, because it was originally enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968, P.L. 90-351, 82 Stat. 212 (1968). Even though Title III

officials, federal law enforcement authorities may apply for a court order approving the use of wiretapping in connection with the investigation of certain serious federal crimes, 18 U.S.C. 2516, 2517, 2518. The orders must be narrowly drawn, of short duration, and based upon probable cause to believe that they will generate evidence relating to the predicate offenses under investigation, id. When the orders expire, those whose communications have been intercepted must be notified, 18 U.S.C. 2518.

The procedure for law enforcement access to the content of wire and electronic communications stored with communications providers and to provider transaction records is somewhat less demanding, although it generally requires a court order, warrant, or subpoena, 18 U.S.C. 2701-2702.

Pen registers and trap and trace devices surreptitiously capture the identity of the sender and recipient of communications. The procedure for a court order approving law enforcement installation and use of a pen register or a trap and trace device is less demanding still, 18 U.S.C. 3121-3127.

Sections 201 (authority to intercept wire, oral, and electronic communications relating to terrorism) and 202 (authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses).

Federal courts may authorize wiretapping – the interception of wire, oral or electronic communications – for law enforcement purposes in connection with the investigation of one or more specifically designated, serious federal crimes (predicate offenses), 18 U.S.C. 2516. Sections 201 and 202 temporarily add crimes to this predicate offense list. Section 202 places felonious violations of 18 U.S.C. 1030 (computer fraud and abuse) on the list; section 201 contributes:

- 18 U.S.C. 229 (chemical weapons);
- 2332 (crimes of violence committed against Americans overseas);
- 2332a (weapons of mass destruction);
- 2332b (multinational terrorism);
- 2332d (financial transactions with a country designated a sponsor of terrorism);
- 2339A (providing material support to a terrorist), and
- 2339B (providing material support to a terrorist organization).

Background. The Administration's request for legislation submitted immediately following the attacks of September 11, 2001 did not include any proposal comparable to either section 201 or section 202, *Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the House Comm. on the Judiciary (Hearing)*, 107th Cong., 1st Sess. (2001). Nor can any similar provision be found in the legislation reported out of the House Judiciary Committee, H.Rept. 107-236 (2001). They appear first, and in the language ultimately enacted, in the initial

---

encompasses wire, oral and electronic communications it is often referred to as the "wiretap" statute as a matter of convenience.

version of S. 1510, 147 *Cong. Rec.* S10309 (daily ed. Oct. 4, 2001). They were referred to as among the "number of sensible proposals that should not be controversial," 147 *Cong. Rec.* S10552 (daily ed. Oct. 11, 2001)(remarks of Senator Leahy), and otherwise seem to have attracted little attention.

What Does Not Expire. Sections 201 and 202 expire on December 31, 2005. By operation of subsection 224(b), law enforcement officials may seek a wiretap order in conjunction with an investigation of any of the offenses added to the predicate offense list by sections 201 or 202, as long as the particular offense or potential offense begins or occurs before December 31, 2005.

The passing of section 201 will, in all probability, carry with it a subsequent addition to the predicate list. Section 201 makes its additions to the wiretap predicate offense list using these words (emphasis added), "Section *2516(1)* of title 18, United States Code, is amended ... (2) by inserting ... the following new paragraph: '*(q)* any criminal violation section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism); or'."

Again with emphasis added, Public Law 107-197 (Implementation of the International Convention for the Suppression of Terrorist Bombings) subsequently provides that, "Section *2516(1)(q)* ... is amended by – (1) inserting '2332f' after '2332,' and (2) striking 'or 2339B' and inserting '2339B, or 2339C'." 116 Stat. 728 (2002).

Thus, section 201 enacts 18 U.S.C. 2516(1)(q); section 201 and therefore 18 U.S.C. 2516(1)(q) expire on December 31, 2005; P.L. 107-197 amends subsection 2516(1)(q); and therefore on the face of things the later amendment expires with the rest of 2516(1)(q).

Yet although the language of the statute may indicate that the P.L. 107-197 amendments expire with the rest of subsection 2516(1)(q), the scant legislative history might suggest that Congress intended to add the new crimes, 18 U.S.C. 2332f(bombing public buildings and places) and 2339C (financing terrorism), to the wiretap predicate offense list permanently. The House Judiciary Committee report (there is no Senate report), for instance, notes the addition of the new crimes not only to the wiretap predicate list, but to the list of "Federal crimes of terrorism" in 18 U.S.C. 2332b(g)(5)(B), to the predicate offense list for 18 U.S.C. 2339A (assistance of terrorists), and to the forfeiture predicate list in 18 U.S.C. 981(a)(1) – "This section of the bill, which is not required by the treaty but will assist in Federal enforcement, adds the new 18 U.S.C. §§2332f and 2339C to four existing provisions of law," H.Rept. 107-307, at 14 (2001). Other than its placement, there is nothing to indicate Congress intended to insert the new crimes temporarily on the wiretap predicate list but permanently on the other lists. The reasons for making the section 224 provisions temporary do not seem to apply to the treaty implementing provisions; the additions were made to implement treaty obligations not root out 9/11 terrorists.

On the other hand, the treaty deals with terrorism offenses and the crimes added to subsection 2516(1)(q) are much like those already found there. More importantly, the clearest indication of what Congress means is what it says. It said the treaty-implementing crimes should be added to that portion of the wiretap predicate list that

is clearly scheduled to expire. In other instances when called upon to construe a statute in apparent contradiction to its precise language, the courts have been loath to rewrite a statute in the name of statutory construction.[6]

Considerations. The Justice Department indicates that "several recent wiretap orders have been based on this expanded list of terrorism offenses [authorized by section 201], including one involving a suspected domestic terrorist, who was subsequently charged with unlawfully making an explosive bomb, as well as another involving an individual with suspected ties to Columbian [sic] terrorists," U.S. Department of Justice, *Report from the Field: The USA PATRIOT Act at Work (Report),* 26 (July, 2004).[7]

Critics might argue that the authority conveyed by sections 201 and 202 is unnecessary. Neither the Justice Department's *Report* nor its *Dispelling the Myths (Myths)* report[8] mention any use of the authority under section 202 (computer abuse felonies). Moreover, federal law would seem to provide ample authority elsewhere for wiretaps in the case of the two somewhat specific examples the Department supplied for section 201. Federal explosives offenses and conspiracy to violate them are among the existing permanent federal wiretap predicates, 18 U.S.C. 2516(1)(c), (r); 844(d), (e), (f), (g), (h), (i). And it is not clear why wiretaps under the Foreign Intelligence Surveillance Act (FISA) should not be adequate and perhaps even more appropriate with respect to "an individual with suspected ties to Columbian terrorists," 50 U.S.C. 1804, 1805, 1801. Or so critics might contend.[9]

Such critics might argue that the statistics published annually by the Administrative Office of the United States Courts indicate that the authority under sections 201 and 202 is little used and little needed. Terrorism offenses are not even designated as one of the major offense categories for which court-authorized interceptions are granted, unlike narcotics (502 orders), racketeering (43), bribery (1), gambling (2), homicide and assault (1), kidnaping (0), theft (0), or loansharking (5),

---

[6] *Barnhard v. Sigmon Coal Co.* , 534 U.S. 438, 461-62 (2002), *quoting*, *Connecticut Nat. Bank v. Germain*,503 U.S. 249, 253-54 (1992)("We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there. When the words of a statute are unambiguous, then, this first canon is also the last: judicial inquiry is complete").

[7] Available on Jan. 6, 2005 at [http://www.lifeandliberty.gov/docs/071304_report_from_the_field.pdf].

[8] U.S. Department of Justice, *Dispelling the Myths: Dispelling Some of the Major Myths about the USA PATRIOT Act*, available on Jan. 6, 2005 at [http://www.lifeandliberty.gov/subs/add_myths.htm].

[9] *See also*, Electronic Privacy Information Center, *The USA PATRIOT Act (EPIC Report),* available on January 25, 2004 at [http://www.epic.org/privacy/terrorism/usapatriot] (Section 201 added crimes of terrorism or production/dissemination of chemical weapons as predicate offenses under Title III, suspicion of which enable the government to obtain a wiretap of a party's communications. Because the government already had substantial authority under FISA to obtain a wiretap of a suspected terrorist, the real effect of this amendment is to permit wiretapping of a United State person suspected of domestic terrorism.

2003 Wiretap Report, Table 3 (2004), available on Jan. 6, 2005 at [http://www.uscourts.gov].

Finally, critics – particularly those who view law enforcement use of wiretapping with concern – might argue that the appropriate question is not how many terrorists and criminals have been caught through use of the new authority, but how often and under what circumstances the authority has been used in instances where it proved to be a false trail; where the individuals whose conversations were intercepted proved to have no incriminating ties to terrorists (Colombian or otherwise) or criminal events (past, present or future).[10]

Summary. Section 201 permits the use of court-supervised wiretaps in cases involving various terrorism offenses; section 202 permits such use in cases of felony computer fraud or abuse.

- Here and elsewhere the full extent of the "potential offense" sunset exception (224(b)) is unclear.
- The annual wiretap report suggests this authority has been little used.
- Section 201 authority has been used in a bomb case and case involving suspected links to Colombian terrorists.
- Some may feel that alternative, permanent authority could have been used in the two instances where the Justice Department notes section 201 authority has been used.
- There is no indication section 202 authority has ever been used.

Subsections 203(b) (authority to share electronic, wire, and oral interception information) and 203(d) (general authority to share foreign intelligence information).

Evidence obtained through a court-ordered wiretap for federal law enforcement purposes may be disclosed under limited circumstances (e.g., testimony in judicial proceedings or disclosure to other law enforcement officials for official use), 18 U.S.C. 2517. Prior to the act, there was no explicit authorization for disclosure to intelligence officials.

Subsection 203(b) amends federal wiretap law to permit law enforcement officials to disclose wiretap evidence to various federal officials ("law enforcement, intelligence, protective, immigration, national defense [and] national security

---

[10] *Cf.*, Whitehead & Aden, *Forfeiting "Enduring Freedom" for "Homeland Security": A Constitutional Analysis of the USA PATRIOT Act and the Justice Department's Anti-Terrorism Initiatives*, 51 AMERICAN UNIVERSITY LAW REVIEW 1081, 1108-109 (2002)(Whitehead & Aden)("[W]iretap orders are virtually never denied. . . . Despite the apparent lack of judicial checks on the availability of wiretap orders before the passage of the Patriot Act, the act expands their availability even further. Sections 201 and 202 of the Patriot Act amend the Wiretap Act to allow the FBI to obtain wiretap warrants for 'terrorism' investigations, 'chemical weapons' investigations, or 'computer fraud and abuse' investigations. This expands the federal government's wiretap authority into the broad, as-yet-undefined area of 'terrorism' investigations and investigations relating to computer use").

official[s]") when it involves foreign intelligence, counterintelligence, or foreign intelligence information, 18 U.S.C. 2517(6).

Subsection 203(d) authorizes law enforcement officers to share foreign intelligence, counterintelligence, and foreign intelligence information with the same set of federal officials notwithstanding any other legal restriction.

The subsections use the same definitions for foreign intelligence, counterintelligence and foreign intelligence information:

> The term "foreign intelligence information" means:
> (a) information, whether or not it concerns a United States person, that relates to the ability of the United States to protect against —
>
> - actual or potential attack or other grave hostile acts of a foreign power or its agent;
> - sabotage or international terrorism by a foreign power or its agent; or
> - clandestine intelligence activities by an intelligence service or network of a foreign power or by its agent; or
>
> (b) information, whether or not it concerns a United States person, with respect to a foreign power or foreign territory that relates to —
>
> - the national defense or the security of the United States; or
> - the conduct of the foreign affairs of the United States. 18 U.S.C. 2510(19)
>
> The term "foreign intelligence" means information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. 50 U.S.C. 401a(2).
>
> The term "counterintelligence" means 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(3).

Background. Federal law has long permitted wiretap generated information to be shared with law enforcement officers for the performance of their duties, 18 U.S.C. 2517(1) (2000 ed.). The Administration's initial proposal was to expand the definition of "law enforcement officer" to include all federal officers and employees, §103, H.R.--, *Hearings* at 70. It contended that:

> At present, 18 U.S.C. §2517(1) generally allows information obtained via wiretap to be disclosed only to the extent that it will assist a criminal investigation. One must obtain a court order to disclose Title III information in non-criminal proceedings. Section 109 [sic] would modify the wiretap statutes to permit the disclosure of Title III-generated information to a non-law enforcement officer for such purposes as furthering an intelligence investigation. This will harmonize Title III standards with those of the Foreign Intelligence Surveillance Act (FISA), which allows such information-sharing. Allowing disclosure under Title III is particularly appropriate given that the requirements for obtaining a Title III surveillance order in general are more stringent than for

> a FISA order, and because the attendant privacy concerns in either situation are similar and are adequately protected by existing statutory provisions, *Id.* at 54.

A second Administration proposal sought general catch-all authority for criminal investigators to share foreign intelligence information with federal law enforcement, intelligence, protective immigration, customs, and military personnel, notwithstanding any other provision of law – including the specifically mentioned limitations on sharing grand jury and wiretap information, §154, H.R.--, *Id.* at 74. The Administration's explanation leaned heavily on the value of grand jury disclosure and said nothing of its other Title III sharing request, *Id.* at 57 (The Administration also proposed a complementary grand jury information sharing measure, §354, H.R.--, *Hearings* at 86 (text), 62-3(explanation)).

Both Houses modified the proposals. The House Judiciary Committee trimmed the Administration's "law enforcement officer" language so that the amendment defined law enforcement officer to include only law enforcement, intelligence, national security and defense, protective and immigration personnel and then only for the purposes of sharing foreign intelligence information, §103, H.R. 2975, H.Rept. 107-236, at 5 (2001). It split off the grand jury components from the second proposal, and permitted sharing of grand jury matters only with court approval, §§154, 353, H.R. 2975, *Id.* at 8, 30.

The Senate, in the approach carried through to enactment, merged the three Administration sections into a single four-part section 203, S. 1510, 147 *Cong. Rec.* S10309 (daily ed. Oct. 4, 2001). The first and third subsections (203(a) and 203(c)) dealt with sharing grand jury information and the Attorney General's regulatory authority. The second, subsection 203(b), was limited to the sharing of wiretap produced foreign intelligence information; and the fourth, subsection 203(d), constituted a general residual grant of authority (a "catch-all" or "notwithstanding any other law" provision) for the disclosure to federal law enforcement, intelligence, protective, military and immigration officials of foreign intelligence information unearthed in a criminal investigation.

Apparently, at the time of passage it was unclear what legal obstacles subsection 203(d) cleared away. Subsection (a) addressed grand jury secrecy impediments and subsection (c) spoke to Title III wiretap hurdles; what other legal barriers to disclosure did subsection (d) order down? Some were uncertain,[11] but the answer may be of some consequence since another section of the act (sec. 905) requires the Justice Department to disclose to the Director of Central Intelligence any foreign intelligence information uncovered during the course of a criminal investigation – unless otherwise provided by law.

---

[11] *See e.g.*, 147 *Cong. Rec.* S11002 (daily ed. Oct. 25, 2001)(remarks of Sen. Leahy)("Even the Administration, which wrote this provision, has not been able to provide a fully satisfactory explanation of its scope. If there are specific laws that the Administration believes impede the necessary sharing of information on terrorism and foreign intelligence within the executive branch, we should address those problems through legislation that is narrowly targeted to those statutes. Tacking on a blunderbuss provision whose scope we do not fully understand can only lead to consequences that we cannot foresee").

What Does Not Expire. The authority for disclosure under subsections 203(b)(wiretap) or 203(d)(catch-all) sunsets on December 31, 2005, unless either the foreign intelligence investigation or crime exception can be claimed. Both subsections list "law enforcement, intelligence, protective, immigration, national defense [and] national security official[s]" as permissible recipients. Yet since subsection 224(b) exempts only foreign intelligence and criminal investigations, the post-December 31, 2005 exceptions might be thought to limit the continued authority of subsections 203(b) and 203(d) to disclosure to law enforcement and intelligence officials and not to allow disclosures to protective, immigration, national defense and national security officials. At most, the extended authority can only apply to disclosures related to criminal or foreign intelligence investigations.

The termination of authority under subsection 203(b) may be of little consequence, since (A) the wiretap law's criminal disclosure and use prohibitions, 18 U.S.C. 2511(1)(c), (d), only outlaw the disclosure and use of information gleaned from *illegal* wiretaps; they say nothing of the disclosure and use for official purposes of information gathered from *lawful* interceptions; (B) the civil constrains on unlawful disclosure by officials, established in section 223 of the act, likewise expire on December 31, 2005; (C) the wiretap law elsewhere authorizes disclosure of wiretap information to law enforcement officers, 18 U.S.C. 2517(1); and (D) the subsequently-passed Homeland Security Act authorizes disclosure, in separate, permanent subsections, to a wide range of officials particularly when confronted with the more serious foreign intelligence situations, P.L. 107-296, §896, 116 Stat. 2257 (2002) (18 U.S.C. 2517(7),(8)).[12]

---

[12] "(7) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, 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 or derivative evidence to a foreign investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure, and foreign investigative or law enforcement officers may use or disclose such contents or derivative evidence to the extent such use or disclosure is appropriate to the proper performance of their official duties.

"(8) Any investigative or law enforcement officer, or other Federal official in carrying out official duties as such Federal official, 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 or derivative evidence to any appropriate Federal, State, local, or foreign government official to the extent that such contents or derivative evidence reveals 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. Any 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, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue," 18 U.S.C. 2517(7),(8).

The Homeland Security Act's treatment of the general law enforcement disclosure to intelligence authorities found in subsection 203(d) is a bit different. It adopts language much like that which it provides in the wiretap context of subsection 203(b). But rather than placing the amendment in a separate subsection so that it survives the passing of the subsection on December 31, 2005, it embeds the amendment in subsection 203(d) thereby suggesting the amendment is intended to terminate with the rest of subsection 203(d), P.L.107-296, §897(a), 116 Stat. 2257 (2002)(50 U.S.C. 403-5d).[13]

Considerations. When the Justice Department speaks of how it has used the authority granted by section 203, it ordinarily does so in general terms without indicating whether it is referring to the grand jury secrecy release of subsection (a) that does not expire or to the wiretap exception or catch-all authority of subsections (b) and (d) that do expire. Its comments, however, do indicate that the authority under one or more of the subsections has been used with some regularity: "the Department has made disclosures of vital information to the intelligence community and other federal officials under section 203 on dozens of occasions," *Myths* at §203; *see also*, *Report* at 8 ("The Department has made disclosures of vital information to the intelligence community and other federal officials under section 203 on many occasions. For instance, such disclosures have been used to support the revocation of visas of suspected terrorists and prevent their reentry into the United States, track terrorists' funding sources, and identify terrorist operatives overseas").

At an earlier time, the Justice Department had objected to language comparable to subsection (b) allowing the disclosure of wiretap foreign intelligence information to intelligence officials in part because it asserted in the more serious cases it was unnecessary.[14]

---

[13] "Section 203(d)(1) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) (Public Law 107-56; 50U.S.C. 403-5d) is amended by adding at the end the following: 'Consistent with the responsibility of the Director of Central Intelligence to protect intelligence sources and methods, and the responsibility of the Attorney General to protect sensitive law enforcement information, it shall be lawful for information revealing 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, obtained as part of a criminal investigation to be disclosed to any appropriate Federal, State, local, or foreign government official for the purpose of preventing or responding to such a threat. Any 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, and any State, local, or foreign official who receives information pursuant to this provision may use that information only consistent with such guidelines as the Attorney General and Director of Central Intelligence shall jointly issue,'" P.L.107-296, §897(a), 116 Stat. 2257 (2002).

[14] 146 *Cong. Rec.* S11119 (daily ed. Oct. 26, 2000)(letter from Ass't Att'y Gen. Robert Raben to Sen. Richard Shelby, dated Sept. 28, 2000)("Section 10 would amend 18 U.S.C. §2517 to permit the sharing of foreign intelligence or counterintelligence information, collected by investigative or law enforcement officers under title III, with the intelligence community. We oppose this provision. Although we recognize the arguments for allowing

Most wiretap orders – focused on narcotics trafficking, racketeering, loansharking, and the like – do not seem likely to unearth evidence of international terrorist activities, *cf. 2003 Wiretap Report*, Table 3. On the other hand, there seems a real possibility that grand jury investigations would disgorge evidence of international terrorism and other foreign intelligence information from time to time. As a consequence the examples the Justice Department cites for the use of section 203 may seem most likely to have involved subsection (a)(disclosure of grand jury information) rather than subsection (b)(disclosure of wiretap information).

Summary. Subsection (b) permits the disclosure of wiretap-generated foreign intelligence information to federal law enforcement, intelligence, protective, immigration and military personnel for official use.

- Permanent authority elsewhere allows for law enforcement sharing.
- Permanent authority enacted subsequently allows authorities to share information concerning domestic or international terrorism with federal, state, local and foreign officials.
- A prior Justice Department letter claimed the existence of authority elsewhere to share wiretap generated information in the presence of an overriding national security concern.
- It is not clear that the authority has ever been used.
- Subsection (d) permits the disclosure of foreign intelligence information discovered in the course of a federal criminal investigation notwithstanding any legal impediment.
- It is unclear what, if any, legal impediments exist.
- It is not clear that the authority has ever been used.

Section 204 (clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications).

Section 204 is essentially a technical amendment. Prior wiretap law makes it clear that the general prohibitions against wiretapping, 18 U.S.C. 2511, and against the acquisition of communications records and stored electronic communications, 18 U.S.C. 2701, do not preclude foreign intelligence gathering activities in international or foreign communications systems, 18 U.S.C. 2511(2)(f)(2000 ed.). Section 204 amends the provision to add that the general prohibition against the use of pen

---

title III information to be shared as a permissible matter this would be a major change to existing law and could have significant implications for prosecutions and the discovery process in litigation. Any consideration of the sharing of law enforcement information with the intelligence community must accommodate legal constraints such as Criminal Rule 6(e)[relating to grand jury secrecy] and the need to protect equities relating to ongoing criminal investigations. While we understand the concerns of the Commission on Terrorism, we believe that law enforcement agencies have authority under current law to share title III information regarding terrorism with intelligence agencies when the information is of overriding importance to the national security. Section 10 also raises significant issues regarding the sharing with intelligence agencies of information collected about United States persons. Such a change to title III should not be made lightly, without full discussion of the issues and implications").

registers or trap and trace devices, 18 U.S.C. 3121, is likewise no impediment to such activities, 18 U.S.C. 2511(2)(f).[15]

Background. The Administration explained in its request for this section that, "This provision clarifies that the collection of foreign intelligence information is governed by foreign intelligence authorities rather than by criminal procedural statutes, as the current statutory scheme envisions," *Hearing*, at 54. The proposal passed *in haec verba* from the Administration's draft bill (§104), through the House and Senate bills (§104 and §204 respectively), to the USA PATRIOT Act (§204).

What Does Not Expire. The authority under section 204 ends on December 31, 2005 except for investigations relating to offenses or potential offenses begun or occurring before then. The provisions of section 204 have not been substantively amended.

Considerations. Neither of the Justice Department reports mentions section 204. Neither the continuation nor the demise of section 204 seem likely to alter the fact that the general trap and trace device and pen register proscriptions do not preclude the exercise of authority to use trap and trace devices and pen registers to gather foreign intelligence information.

Summary. - Makes clear that the general trap and trace device and pen register prohibitions do not bar use of FISA authority to use trap and trace devices and pen registers to gather foreign intelligence information.

Section 209 (seizure of voice-mail messages pursuant to warrants).

At one time, at least some courts felt that authorities needed a wiretap order rather than a search warrant to seize unretrieved voice mail, *United States v. Smith*, 155 F.3d 1051 (9th Cir. 1998). Section 209 treats voice mail like e-mail, subject to seizure under a search warrant rather than a more demanding wiretap order law, 18 U.S.C. 2703.

Background. Section 209 likewise passed in large measure unaltered from Administration proposal to enactment. The proposal simply sought to treat voice mail like e-mail:

> This section enables law enforcement personnel to seize suspected terrorists' voice mail messages pursuant to a search warrant. At present, 18 U.S.C. §2510(1) anomalously defines "wire communication" to include "any

---

[15] *See e.g.*, "This section is a technical and conforming amendment that would add chapter 206 (relating to pen registers/trap and trace orders) to section §2511(f) of the Wiretap Statute. Section 2511(f) provides that nothing in chapter 119 (relating to the interception of communications), chapter 121 (relating to stored wire and electronic communications and transaction records access), 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 form international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law. . . .' The bill would include chapter 206 under that §2511(f)," H.Rept. 107-307 at 55 (2001).

> electronic storage of such communication," meaning that the government must apply for a Title III wiretap order before it can obtain unopened voice mail messages held by a service provider. The section amends the definition of "wire communication" so that it no longer includes stored communications. It also amends 18 U.S.C. §2703 to specify that the government may use a search warrant (instead of a wiretap order) to compel the production of unopened voice mail, thus harmonizing the rules applicable to stored voice and non-voice (e.g., e-mail) communications. *Hearing* at 54; *see also*, H.Rept. 107-236, at 54.

What Does Not Expire. The authority under section 209 ends on December 31, 2005 except for investigations relating to offenses or potential offenses begun or occurring before then. The provisions of section 209 have not been substantively amended.

Considerations. The Justice Department cites the ease and speed with which a warrant can be obtain as the principal virtue of section 209:

> Investigations of terrorism and other crimes have also long been frustrated by the failure of federal law to permit agents to gain access to voice-mail messages with a search warrant. Prior to the USA PATRIOT Act, federal law required officers to waste critical time and resources going through the burdensome process of obtaining a wiretap order (rather than a search warrant) to obtain unopened voice-mail. This was so despite the fact that authorities could use a search warrant, for example, to obtain messages stored on the suspect's own answering machine. Section 209 of the USA PATRIOT Act has modernized federal law by enabling investigators to access more quickly suspects' voice-mail by using a search warrant. The speed with which voice-mail is seized and searched can often be critical to an investigation because stored voice-mail is regularly deleted by service providers and thus lost forever. Warrants pursuant to section 209 have been used to obtain key evidence in a variety of criminal cases, including voice-mail messages left for those participating in a large-scale ecstasy smuggling ring based in the Netherlands, *Report* at 22.

The Justice Department also reports that "[s]ince passage of the act, such warrants have been used in a variety of criminal cases to obtain key evidence, including voice mail messages left for foreign and domestic terrorists," *Myths* at §209. And it points out that while the procedure under Title III is more demanding and consequently slower and more burdensome, the warrant procedure necessarily involves a finding of probable cause on evidence presented under oath and found by a neutral magistrate, *Id*.

Critics might suggest that Congress could have supplied consistency of treatment in a different manner. It might have concluded that an ongoing conversation (i.e., one in which communications are being transmitted but have not been received) should be accorded the same level of Title III protection whether it involves a telephone conversation, a face to face conversation, an e-mail conversation, or a voice mail conversation. As it now stands, a telephone conversation is treated differently than an incomplete voice mail conversation. Here and elsewhere, critics might also suggest that information on the utility of the new authority seems somewhat general and fairly skeletal. Here and elsewhere, critics might be concerned with the extent to which the enhancement of government

authority heralds a loss of personal privacy.[16] The fact that Title III is only available in connection with the investigation of certain serious crimes while a search warrant is available in connection with any criminal investigation does not seem to be a consideration of any substantial force to either critics or the Justice Department.

Summary. The section permits use of a search warrant to seize unopened voice mail held by a service provider.

- Previous requirements of a wiretap order were slow, burdensome, and not compatible with the manner in which unopened, provider-stored e-mail was handled.
- Critics might suggest that compatibility might have been achieved by expanding wiretap order requirements to cover unopened e-mail.
- Critics might question the section's continued utility if no more detailed and extensive evidence of successful use is available.
- Search warrants can be used to secure evidence of any crime; Title III orders are limited to investigations involve serious predicate offenses.

Section 212 (emergency disclosure of electronic surveillance).

Prior law confined the circumstances under which service providers might disclose the particulars of their customers' transaction records or communications without a warrant, court order, or their customers' consent, 18 U.S.C. 2702, 2703 (2000 ed.). Section 212 permitted communications service providers to disclose either customer records or the content of their customers' communications to authorities in any emergency situation that involved an immediate danger of physical injury, P.L. 107-56, §212(a)(1)(D), 115 Stat. 284-85 (2001). The content provision has been repealed and replaced; the records provision has not, 18 U.S.C. 2702(b)(7), (8), 2702(c)(4).

Background. Although with a only fleeting reference to cyber terrorism offered as justification, the proposal for emergency provider disclosure came as part of the original package, §110, H.R. --, *Hearing*, at 72.[17] The House and Senate

---

[16] Lee, *The USA PATRIOT Act and Telecommunications: Privacy Under Attack*, 29 RUTGERS COMPUTER & TECHNOLOGY LAW JOURNAL 371, 382 (2003)("By eliminating the burdensome process of obtaining a wiretap order, though, this provision ultimately encourages more government searches. Even case law that required the government to apply for a Title III warrant is now overturned"); Whitehead & Aden, at 1110 ("The Patriot Act incorporates 'wire communication' into the definition of an 'electronic communications system,' effectively permitting access to such messages via a standard search warrant, as if a voice mail message were merely a documentary record. However, an individual's constitutionally recognized expectation of privacy in his or her message is not diminished by the fact that the message is stored temporarily in a voice messaging system before being retrieved by the recipient. Consequently, this provision of the Patriot Act is constitutionally suspect under the Fourth Amendment").

[17] The Justice Department's explanation ran as follows, "Existing law contains no provisions that allow providers of electronic communications service to disclose the communications (or records relating to such communications) of their customers or

proposals contained essentially the same provision, §110, H.R. 2975, H.Rept. 107-236, at 6-7; §212, S. 1510, 147 *Cong. Rec.* S10311 (daily ed. Oct. 4, 2001).

What Does Not Expire. The Homeland Security Act repealed section 212's provision governing *content* disclosure in emergency situations and recasts it as a separate provision, 18 U.S.C. 2702(b)(7), but said nothing of the emergency disclosure of customer *records*, 18 U.S.C. 2703(c)(4). As a consequence, the authority to disclose customer records in an emergency situation disappears on December 31, 2005 (except with respect to crimes or potential crimes beginning or occurring before then), but the freestanding emergency content disclosure provision which replaced its section 212 predecessor remains in effect.

Considerations. The Justice Department cites several instances where the authority of section 212 has been used. Although capsulized, its descriptions seem to speak of providers supplying record, rather than content, information:

> The cooperation of third parties in criminal or terrorist investigations is often crucial to a positive outcome. Third parties, such as telecommunications companies, often can assist law enforcement by providing information in emergency situations. Previous federal law, however, did not expressly allow telecommunications companies to disclose customer records or communications in emergencies. Even if a provider believed that it faced an emergency situation in which lives were at risk, if the provider turned over customer information to the government, it risked, in some circumstances, being sued for money damages. Congress remedied this problem in section 212 of the USA PATRIOT Act by allowing electronic communications service providers to disclose records to the government in situations involving an immediate danger of death or serious physical injury to any person. Section 212 has already amply proved its utility.
>
> **Examples:**
>
> - Section 212 was used in the investigation of a bomb threat against a school. An anonymous person, claiming to be a student at a high school, posted on the Internet a disturbing death threat ... The operator of the Internet site initially resisted disclosuring to law enforcement any information... Once a prosecutor explained that the

---

subscribers in emergencies that threaten death or serious bodily injury. This section amends 18 U.S.C. §2702 to authorize such disclosures 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.

"Current law also contains an odd disconnect: a provider may disclose the **contents** of the customer's communications in order to protect its rights or property but the current statute does not expressly permit a provider to voluntarily disclose **non-content** records (such as a subscriber's login records). 18 U.S.C. 2702(b)(5). This problem substantially hinders the ability of providers to protect themselves from cyber-terrorists and criminals. Yet the right to disclose the contents of communications necessarily implies the less intrusive ability to disclose non-content records. In order to promote the protection of our nation's critical infrastructures, this section's amendments allow communications providers to voluntarily disclose both content and non-content records to protect their computer systems."

> USA PATRIOT Act created a new provision allowing for voluntary release of information in emergencies, the owner turned over evidence that led to the timely identification of the individual responsible for the bomb threat....
>
> - Section 212 was recently used to apprehend quickly an individual threatening to destroy a Texas mosque before he could carry out his threat....
>
> - Section 212 was invaluable in swiftly resolving a cyber-terrorist [extortion] threat to the South Pole Research Station... The hacked computer also controlled the life support systems for the South Pole station that housed 50 scientists "wintering over" during the South Pole's most dangerous season....
>
> - Section 212 has further proven to be extremely useful in cases involving abducted or missing children. The provision, for instance, was instrumental in quickly rescuing a 13-year-old girl from Western Pennsylvania who had been lured from her home and was being held captive by a 38-year-old man she had met online.... *Report* at 26-7; *see also, Myths* at §212.

None of the examples seem to involve a victim alerting unsuspecting authorities of an intrusion, as the section appears to contemplate; each seems to relate to a case where authorities were aware of the intrusion and the information might have been effectively secured through the use of a search warrant, 18 U.S.C. 2703(c). None of the examples appear to relate to the rationale offered for the proposal's passage – "protection of our nation's critical infrastructure."

Summary. Section 212 authorizes service providers in emergency situations to disclose customer communications record information and the content of stored customer communications.

- Subsequent legislation made the content disclosure but not the record disclosure authority permanent, P.L. 107-296, 116 Stat. 2157 (2002)(18 U.S.C. 2702(b)(7)).
- The record disclosure feature has proven useful in several life-threatening situations.
- The same benefits might be available after sunset through the use of a search warrant.
- There are apparently no reported instances of the section's use for its intended purposes, protection of the nation's critical infrastructure.

Section 217 (interception of computer trespasser communications).

Federal wiretap law proscribes the interception of telephone, face to face, or computer conversations, subject to certain narrow exceptions such as the issuance of a wiretap order, the consent of one of the participants in the conversation, or a communications carrier's protection of its property, 18 U.S.C. 2511. Computer service providers occasionally discover that trespassers have established electronic

outposts within their systems. Section 217 allows providers to consent to law enforcement interception of communications to and from these outposts, 18 U.S.C. 2511(2)(i).

Background. Section 217 reflects the Administration's original request with two exceptions, *compare*, §106, H.R. --, *Hearings* at 71, *with*, §217, 115 Stat. 290-91 (2001). Section 217 excludes from the definition of "computer trespasser," those with contractual access to the computer system in question (notwithstanding the fact they may be exceed their authorization), 18 U.S.C. 2510(21)(B); and limits permissible interceptions to the trespasser's communications within the invaded computer system, 18 U.S.C. 2511(2)(i). The first exception originated in §217 of S. 1510, as passed by the Senate, 147 *Cong. Rec.* S10609 (daily ed. Oct. 11, 2001). The second initially appeared in §217 of H.R. 2975, as passed by the House, 147 *Cong. Rec.* H6744-745 (daily ed. Oct. 12, 2001).[18]

Speaking of the basic proposal, the Administration had stated that:

> Current law may not allow victims of computer trespassing to request law enforcement assistance in monitoring unauthorized attacks as they occur. Because service providers often lack the expertise, equipment, or financial resources required to monitor attacks themselves as permitted under current law, they often have no way to exercise their rights to protect themselves from unauthorized attackers. Moreover, such attackers can target critical infrastructures and engage in cyber terrorism. To correct this problem, and help to protect national security, the proposed amendments to the wiretap statute would allow victims of computer attacks to authorize persons "acting under color of law" to monitor trespassers on their computer systems in a narrow class of cases. §106, H.R. --, *Hearings* at 55.

What Does Not Expire. The authority under section 217 expires on December 31, 2005. There have been no amendments relevant to section 217 since its passage and the sunset exceptions for ongoing intelligence investigations or for investigations of earlier crimes seem likely to be of limited application here. The exception, however, applies "with respect to any ... potential offense that began or occurred before" December 31, 2005. In this context, "potential offenses" may refer those crimes for which preparation but not completion predates December 31, 2005; for example, computer trespassing with an eye to launching a denial of service attack at some future date. On the other hand, in such cases the initial crime of intrusion will have occurred prior sunset, a fact that would seem to permit post-sunset exercise of the section's authority.

The House Judiciary Committee had recommended expansion of the good faith defense to civil liability for computer system operators who sought to take advantage of section 217, §105(3), H.R. 2975, H.Rept. 107-236, at 5, 56 (2001). The recommendation was not included in the act, §217, P.L. 107-56, 115 Stat. 291

---

[18] Neither exception appeared in H.R. 2975 as reported by the House Judiciary Committee, §105, H.R. 2975, H.Rept. 107-236, at 5 (2001).

(2001). The Homeland Security Act, however, added it as a permanent amendment to 18 U.S.C. 2520(d)(3), §225(e), P.L. 107-296, 116 Stat. 2157 (2002).[19]

Considerations. The Justice Department's post-enactment comments relating to section 217 tend to describe its reach rather than its use:

> The USA PATRIOT Act also empowered Internet service providers and others to enlist the help of law enforcement to monitor the activities of hackers who unlawfully access their computer networks. Section 217 of the act allows victims of computer attacks by cyber-terrorists and others to ask law enforcement officers to monitor trespassers on their systems. Section 217 thus places cyber-intruders on the same footing as physical intruders: hacking victims can seek law-enforcement assistance to combat hackers just as burglary victims can invite police officers into their homes to catch burglars. *Report* at 28.

The Department's comments in *Myths* are more expansive and do include a general statement of use:

> The law has always recognized the right of landowners to ask law enforcement to help expel people who illegally trespass on their property. Section 217 made the law technology-neutral, placing cyber-intruders on the same footing as physical intruders. Now, hacking victims can seek law-enforcement assistance to combat hackers, just as burglary victims have been able to invite officers into their homes to catch burglars. Prior to the enactment of the USA PATRIOT Act, the law prohibited computer service providers from sharing with law enforcement that hackers had broken into their systems. 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. Section 217 preserves the privacy of law-abiding computer users. Officers cannot agree to help a computer owner unless (1) they are engaged in a lawful investigation; (2) there is reason to believe that the communications will be relevant to that investigation; and (3) their activities will not acquire the communications of non-hackers. *This provision has played a key role in a number of terrorist investigations, national-security cases, and investigations of other serious crimes.* Section 217 is extremely helpful when computer hackers launch massive denial of service attacks - which are designed to shut down individual websites, computer networks, or even the entire Internet. The definition of computer trespasser does not include an individual who has a contractual relationship with the service provider. Thus, for example, America Online could not ask law enforcement to help monitor a hacking attack on its system that was initiated by one of its own subscribers. *Myths*, at §217 (emphasis added).

The section's solution does not seem to match the statement of the problem it was purportedly designed to address. It does not remove intruders or prevent their entry; it merely permits eavesdropping on them while they are trespassing. There is no clear explanation by word or example of why this is preferable or effective. The Department indicated during oversight hearings that authority under the section had

---

[19] 18 U.S.C. 2520(d)(3)("A good faith reliance on ... (3) a good faith determination that section ... 2511(2)(i) of this title permitted the conduct complained of; is a complete defense against any civil or criminal action brought under this chapter or any other law").

been use "comparatively rarely."[20] Some critics have expressed the concern that the provision might be used to circumvent the safeguards and oversight that attends Title III wiretaps.[21]

Summary. Section 217 permits federal authorities to intercept an intruder's communications within an invaded computer system.

- It requires consent of the system operator, a law enforcement investigation, a reasonable belief that the communications are relevant to the investigation, and limits interception to the intruder's communications.
- Statements of support have leaned heavily on descriptions of the authority rather than examples of its use.
- The Justice Department has stated that the authority has been used "comparatively rarely."
- The solution does not seem to match the problem. Section 217 does not authorize removal of computer hackers bent on denial of service attacks nor does it prevent or punish trespassers; instead it eavesdrops on their communications.

---

[20] *Oversight Hearing of the Department of Justice: Hearing Before the Senate Comm. on the Judiciary*, 107th Cong., 2d Sess. at (2002), quoted in Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEORGE WASHINGTON LAW REVIEW 1145, 1203 (2004).

[21] *National Security at What Price?: A Look into Civil Liberty Concerns in the Information Age under the USA PATRIOT Act of 2001 and a Proposed Constitutional Test for Future Legislation*, 12 CORNELL JOURNAL OF LAW AND PUBLIC POLICY 447, 460-61 (2003)("In addition to allowing broad discretion and authorization for both ISPs and computer owners and operators, the USA PATRIOT Act, removes most judicial oversight of this particular task. In situations that do not result in prosecution, the computer users whose activities are targeted are likely never to discover the monitoring, and therefore they would be effectively unable to challenge the provision in court. Furthermore, law enforcement could unduly pressure owners and operators of computers to obtain permission for the interception and to circumvent the safeguards built into the PATRIOT Act"); *EPIC Report* ("The new exception [under section 217] has broad implications, given that a 'protected computer' includes any 'which is used in interstate or foreign commerce or communications' (which, with the internet, includes effectively any computer). The 'authorization' assistance permits wiretapping of the intruder's communications without any judicial oversight, in contrast to most federal communication-interception laws that require objective oversight from someone outside the investigative chain. The new law places the determination 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 target would never even have notice of the fact that their communications were subject to warrantless interception.... [T]he amendment has little, if anything, to do with legitimate investigations of terrorism").

Section 220 (nationwide service of search warrants for electronic evidence).

Before the act, federal authorities could gain access to a communications service provider's customer records and the content of their electronic communications either through the use of a search warrant or in some instances a court order, 18 U.S.C. 2703. Certainly in the case of the search warrant and arguable in the case of the court order, the warrant or order could only be issued in the judicial district in which it was to be executed, F.R.Crim.P. 41; 18 U.S.C. 3127 (2000 ed.). Federal authorities found this inconvenient and sometimes frustrating where the criminal investigation was conducted in one district and the communications provider was located in another, H.Rept. 107-236, at 57.

Section 220 addresses the difficulty by authorizing the court in the district where the crime occurred to issue search warrants or orders to be served anywhere in the country for access to electronic communications content and customer record information (which by virtue of section 209, discussed above, now includes content and records of voice, e-mail, and other electronic communications), 18 U.S.C. 2703, 3127.

Background. But for the addition of a technical conforming amendment, section 220 passed untouched through the legislative process from request to presidential signature.[22] The justification for the proposals was rather straightforward:

> Current law requires the government to use a search warrant to compel a provider to disclose unopened e-mail. 18 U.S.C. §2703(a). Because Federal Rule of Criminal Procedure 41 requires that the "property" to be obtained "be within the district" of the issuing court, however, the rule may not allow the issuance of §2703(a) warrants for e-mail located in other districts. Thus, for example, where an investigator in Boston is seeking electronic e-mail in the Yahoo! account of a suspected terrorist, he may need to coordinate with agents, prosecutors, and judges in the Northern District of California, none of whom have any other involvement in the investigation. This electronic communications information can be critical in establishing relationships, motives, means, and plans of terrorists. Moreover, it is equally relevant to cyber-incidents in which a terrorist motive has not (but may well be) identified. Finally, even cases that require the quickest response (kidnaping, threats, or other dangers to public safety or the economy) may rest on evidence gathered under §2703(a). To further public safety, this section accordingly authorizes courts with jurisdiction over investigations to compel evidence directly, without requiring the intervention of their counterparts in other districts where major Internet service providers are located. §108, H.R. --, *Hearings*, at 55.

What Does Not Expire. The authority under section 220 terminates on December 31, 2005 except with respect to earlier crimes or potential crimes. Section 219, however, appears to mitigate the impact of section 220's expiration in certain

---

[22] *Compare*, §108, H.R. --, *Hearings* at 72, *with*, §220, P.L. 107-56, 115 Stat. 291-92 (2001); *see also*, §108, H.R. 2975, H.Rept. 107-236, at 5-6; §220, S. 1510, 147 *Cong. Rec.* S10610 (daily ed. Oct. 11, 2001).

terrorism cases. Section 219 is not subject to the sunset provision. It provides for at least nation-wide, and perhaps world-wide, service of federal search and arrest warrants in cases of international or domestic terrorism as defined in 18 U.S.C. 2331.[23]

Considerations. The Justice Department asserts that section 220 has proven beneficial in a number of criminal cases, some involving charges of terrorism.

> In section 220 ... Congress adapted federal law to changing technology by allowing courts to order the release of stored communications through a search warrant valid in another specified judicial district. The enhanced ability to obtain this information efficiently has proved invaluable in several terrorism investigations, such as the Virginia Jihad[24] and the "shoebomber"[25] cases ... as well as time-sensitive criminal investigations, such as [one] involving a dangerous fugitive[26].... In addition to allowing law enforcement to gain access to information quickly in time-sensitive investigations, Congress also significantly improved the Justice Department's ability to mount large-scale child

---

[23] "[A] magistrate judge — in an investigation of domestic terrorism or international terrorism (as defined in 18 U.S.C. 2331) — having authority in any district in which activities related to the terrorism may have occurred, may issue a warrant for a person or property within or outside that district," F.R.Crim.P. 41(b)(3).

"[T]he term 'international terrorism' means activities that — (A) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State; (B) appear to be intended — (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnaping; and (C) occur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum....

"[T]he term 'domestic terrorism' means activities that — (A) involve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State; (B) appear to be intended — (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnaping; and (C) occur primarily within the territorial jurisdiction of the United States," 18 U.S.C. 2331(1), (5).

[24] Several Northern Virginia residents were convicted or pleaded guilty to terrorism-related charges including paramilitary "paintball" training, *United States v. Khan*, 309 F.Supp.2d 789 (E.D.Va. 2004); Department of Justice Press Release, dated April 9, 2004).

[25] Richard Reid, a British citizen, pleaded to eight terrorism-related charges arising out of his efforts to ignite explosives concealed in his shoes while on board an American Airlines flight from Paris to Miami, *United States v. Reid*, 369 F.3d 619 (1st Cir. 2004). A second British resident was later indicted as Reid's accomplice, Department of Justice Press Release, dated Oct. 4, 2004. All the misconduct here seems to involve the overseas activities of foreign nationals; it is unclear how access to the customer records of communications service providers in this country could have been helpful.

[26] The *Report* refers to the case of an interstate fugitive charged with abduction and sexual assault of his estranged wife, tracked down through his Internet use, and ultimately convicted on state charges.

> pornography investigations by including section 220 in the USA PATRIOT Act. 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.... Section 220 has also dramatically reduced the administrative burdens in judicial districts that are home to large Internet service providers. *Report* at 20-1.

Critics might suggest that the principal objection to section 220 is that it makes it expensive and inconvenient for service providers to contest or request modification of orders directed to them from district courts throughout the country.[27] For the Justice Department with United States Attorneys Offices throughout the country, by way of contrast, the burden is simply a matter of resource allocation, it might be argued. Some may feel that the section allows the Justice Department to forum shop should the federal courts in the home districts of large providers prove sympathetic to the burdens such orders impose upon the providers. They might also contend that expiration arrives with little loss in terrorism cases since section 219 of the act which does not expire allows for nation-wide service of search warrants in terrorism cases.

Summary. Section 220 authorizes nation-wide execution of search warrants and court orders for customer communications records and the content of stored customer communications.

- A search warrant must ordinarily be executed in the judicial district in which it is issued except in terrorism cases.
- The Justice Department asserts that the authority has proven useful in serious terrorism and other criminal cases.
- The section makes it more difficult for large communications service providers to seek modification of burdensome disclosure orders; instead of being able to contest a warrant or order within their home federal district they must challenge in whatever district throughout the country the warrant or order originated.
- Section 219 which does not expire permits nation-wide service of search warrants in terrorism cases.

Section 223 (civil liability for certain unauthorized disclosures).

Unrelated to section 223, federal law imposes criminal penalties for illegal wiretapping, 18 U.S.C. 2511, unlawful access to store communications (e.g., e-mail or voice mail), or illegally using a pen register or trap and trace device, 18 U.S.C. 3121. Except with respect to pen registers and trap and trace devices, the same misconduct also triggers civil liability, 18 U.S.C. 2520, 2707. There is a comparable set of provisions imposing criminal and civil liability for FISA surveillance and physical search violations, 50 U.S.C. 1809, 1810, 1827, 1828.

---

[27] *See*, 18 U.S.C. 2703(e)("... A court issuing an order pursuant to this section [for the content or records held by communications providers], on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are usually voluminous in nature or compliance with such order otherwise would cause undue burden on such provider").

Although the federal wiretap statute outlaws use or disclosure of *unlawfully* intercepted communications, 18 U.S.C. 2511(1)(c), (d), and describes narrow circumstances under which communications intercepted under a court order may be used or disclosed, 18 U.S.C. 2517, without more, it does not expose to civil or criminal liability those who disclose or use communications *lawfully* intercepted under a court order.[28]

Section 223 confirms the authority of agency heads to discipline federal officers and employees for willful or intentional violations of federal wiretap or stored communications law, 18 U.S.C. 2520(f), 2707(d). It also imposes civil liability for any willful use or disclosure of information beyond that authorized by those two statutory schemes, 18 U.S.C. 2520(g), 2707(g). Finally, the section creates a cause of action against the United States for the benefit of victims of willful violations of federal wiretap law, the stored communications proscriptions, or the FISA requirements relating to surveillance, physical searches or the use or installation of pen registers or trap and trace devices, 18 U.S.C. 2712.

Background. Section 223 was not among those requested by the Administration, H.R. --, *Hearings*, at 67-90. Nor does it appear in S. 1510 as passed by the Senate, 147 *Cong. Rec.* S10604-630 (daily ed. Oct. 11, 2001). It comes instead from the House Committee on the Judiciary where it was added to H.R. 2975 as §161, H.Rept. 107-236, at 10-13, 305-13. As the section's sponsor explained:

> So what the amendment does is as follows: First, it says that wherever we gather information, whether it is pen register, trace and trap or wiretap or whatever, wiretap under one statute, wiretap under FISA, if information gained during the surveillance is inappropriately released, if it winds up on the White House desk and somebody leaks it, if J. Edgar Hoover tells bad stories about you, then you have a right to go in under the Federal Tort Claims Act as the aggrieved party and sue.... It also then says that if someone goes in and wins the lawsuit against the government because surveilled information has been inappropriately leaked, the head of that bureau or agency either must initiate disciplinary proceedings against the leaker or explain in writing ... that wasn't done. H.Rept. 107-236, at 311 (remarks of Representative Frank).

What Does Not Expire. There have been no amendments to section 223. The precise application of the sunset provision and its exceptions to the cause of action created in section 223 appears somewhat uncertain. Reading only the language of termination and before considering the exception, any cause of action created by section 223 seems to expire on December 31, 2005. This could mean either that no suit (pending or merely actionable) survives thereafter, or alternatively that pending suits survive but none may be filed thereafter, or that regardless of when it is filed any cause of action will only survive with respect to matters occurring prior to that date.

---

[28] Disclosure of the existence of the tap (rather than of its results) may be punishable under the anti-tip off provisions of 18 U.S.C. 2332(d), which proscribes disclosure, with the intent to obstruct, of the fact that a wiretap order has been sought or granted, *United States v. Aguilar*, 515 U.S. 593 (1995).

Under some circumstances the demise of a cause of action deprives the courts of subject matter jurisdiction. Longstanding Supreme Court precedent holds that "when a law conferring jurisdiction is repealed without any reservation as to pending cases, all cases fall with the law."[29]

Taking the exception into consideration, the language on its face seems to say that section 223 continues in effect "with respect to any particular foreign intelligence investigation that began before [December 31, 2005], or with respect to any particular offense or potential offense that began or occurred before" December 31, 2005; that is, a cause of action arising out of foreign intelligence investigation initiated before the date of expiration or out of a criminal investigation of conduct occurring before the date survives – regardless of when the conduct giving rise to the cause of action occurred.

On the other hand, subsection 224(b) may speak only to investigations not to causes of action. It may be that the exception is intended to do no more than extend investigative powers conveyed by other expiring sections of the act. The exceptions may be calculated to do no more than to avoid cutting off investigations pending as of December 31, 2005. Although the language seems to point more strongly to a different conclusion, this view is compatible with the general rule that authority to sue the United States should be narrowly construed.[30]

Considerations. The Justice Department reports that "[t]here have been no administrative disciplinary proceedings or civil actions initiated under section 223 of the act for unauthorized disclosure of intercepts," *Myths* at §223. Critics of the section might argue that the prospect of disciplinary action might serve as a disincentive to information sharing.

Summary. Section 223 creates a cause of action against the United States for official willful violations of Title III or FISA, 18 U.S.C. 2712; amends individual civil liability provisions of Title III for official unlawful disclosure or use, 18 U.S.C. 2520(g), 2707(g); confirms disciplinary authority of agencies officials over violations of the Title III or FISA, 18 U.S.C. 2520(f), 2707(d).

- There have been no disciplinary proceedings initiated or civil actions filed under section 223.
- Section 223 might serve as a disincentive to information sharing.

Temporary Foreign Intelligence Sections

Federal law affords foreign intelligence officials authority comparable to that enjoyed by law enforcement officials in some respects. There is a rough comparability between surveillance (wiretap) authority under the FISA and under

---

[29] *Republic National Bank v. United States*, 506 U.S. 80, 565-66 (1992)(Thomas, J. concurring), *quoting*, *Bruner v. United States*, 343 U.S. 112, 116-17 (1952); *see also*, *Landgraf v. USI Film Products*, 511 U.S. 244, 274 (1994).

[30] *Dept. of Army v. Blue Fox, Inc.*, 525 U.S. 255, 261 (1999)("the waiver of sovereign immunity is to be strictly construed"); *Lane v. Pena*, 518 U.S. 187, 192 (1996).

Title III, *compare*, 50 U.S.C. 1801-1811, *with*, 18 U.S.C. 2510-2522; there is a rough comparability between FISA physical search authority and search warrant authority in a law enforcement context, *compare*, 50 U.S.C. 1821-1829, *with*, F.R.Crim.P. 41; and there is a rough comparability between FISA trap and trace or pen register orders and their law enforcement counterparts, *compare*, 18 U.S.C. 3121-3127, *with*, 50 U.S.C. 1841-1846. There are, however, significant differences.

One of the most perplexing aspects of the law in the post-9/11 universe is the relationship of the statutory procedures and prohibitions governing wiretap and related investigative tools in the criminal law enforcement world (Title III et al.) to those in the foreign intelligence world (FISA). Title III and its auxiliaries are focused on crime (probable cause to believe that predicate offense has, is or will occur; relevancy to a criminal investigation) whether the offender is an American or not; FISA is focused on foreign powers and the agents of foreign powers (probable cause to believe that the target is a foreign power or an officer, employee, spy, saboteur, or terrorist acting on behalf of a foreign power) whether criminal activity is involved or not. The difficulty flows from the fact that an international terrorist may appropriately be the target of a order under Title III et al., or FISA, or both.

Section 206 (roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978).

Section 206 authorizes assistance for the installation and use of multi-point FISA wiretaps, 50 U.S.C. 1805(c)(2)(B). Prior to the act, a FISA wiretap order could include directions that a specifically identified communications carrier, landlord, or other individual assist in the execution of the order, 50 U.S.C. 1805(c)(2)(B) (2000 ed.). Section 206 amends FISA to permit a general command for assistance where the target of the surveillance has taken steps to thwart the identification of any specific person by "rapidly changing hotel accommodations, cell phones, Internet accounts, etc, just prior to important meetings or communications."[31] The law enforcement wiretap statute has a similar provision for law enforcement orders, 18 U.S.C. 2518(4).

Background. The Administration's original request observed that:

> This provision expands the obligations of third parties to furnish assistance to the government under FISA. Under current FISA provisions, the government can seek information and assistance from common carriers, landlords, custodians and other persons specified in court-ordered surveillance. Section 152 would amend FISA to expand existing authority to allow, "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" that a common carrier, landlord, custodian or other persons not specified in the Court's order be required to furnish the applicant information and technical assistance necessary to accomplish electronic surveillance in a manner that will protect its secrecy and produce a minimum of interference with the services that such person is providing to the target of electronic surveillance. This would enhance the FBI's

---

[31] *Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the House Comm. on the Judiciary*, 107th Cong., 1st Sess. 56 (2001); H.Rept. 107-307 at 60.

> ability to monitor international terrorists and intelligence officers who are trained to thwart surveillance by rapidly changing hotel accommodations, cell phones, Internet accounts, etc., just prior to important meetings or communications. Under the current law, the government would have to return to the FISA Court for an order that named the new carrier, landlord, etc., before effecting surveillance. Under the proposed amendment, the FBI could simply present the newly discovered carrier, landlord, custodian or other person with a generic order issued by the Court and could then effect FISA coverage as soon as technically feasible. §152, H.R. --, *Hearings* at 56.

The proposal passed through the legislative process unchanged, *see*, §152, H.R. 2975, H.Rept. 107-236 at 8, 59-60; §206, S. 1510, 147 *Cong. Rec.* S10607 (daily ed. Oct. 11, 2001).

What Does Not Expire. The subsection 224(b) exceptions provisions seem rather obviously applicable. The authority continues in effect after December 31, 2005, with respect to any foreign intelligence investigation initiated prior to that time. There have been no amendments related to section 206 since its enactment. A subsequent amendment (which does not sunset) to a different FISA section, however, permits roving surveillance by requiring a FISA order to identify the location and facilities subject to surveillance *only if they are known* at the time of the application, P.L. 107-108, 115 Stat. 1402 (2001)(50 U.S.C. 1805(c)(1)(B)).

Considerations. The Justice Department's *Report* describes section 206 and offers a hypothetical by way of justification:

> Since 1986, law enforcement officials have been able to obtain multiple-point wiretaps to keep pace with drug dealers and mobsters who, for example, frequently switch cell phones to evade surveillance. Prior to enactment of the USA PATRIOT Act, such authority was not available under FISA for cases involving terrorists. Section 206 of the act, however, now permits officers in international terrorism investigations to obtain a court order that applies to the suspect, rather than a particular phone or phone company. This new authority has put investigators in a better position to avoid unnecessary cat-and-mouse games with terrorists, who are trained to thwart surveillance. While particular examples of the use of multiple-point wiretaps pursuant to section 206 remain classified, the following hypothetical illustrates the utility of this authority.
>
> Suppose, for example, the investigators become aware of an al Qaeda plot to launch a bomb attack. Investigators also discover a recent cellular telephone number for the suspected bomber, for which they immediately obtain a FISA surveillance order. When they attempt to begin surveillance of the suspect, however, they discover that he has changed cellular telephone numbers and providers in order to thwart surveillance. Because of section 206, in cases where the subject's actions may have the effect of thwarting the identification of a service provider, investigators can now obtain a FISA multiple-point surveillance order and immediately serve it on the suspected bomber's new cellular provider, allowing undercover agents to monitor his new cellular telephone number immediately. Without section 206, however, investigators in such cases would be forced to waste valuable time returning to the FISA court just to obtain a new order containing the new provider's name. *Report* at 22-3.

Critics claim section 206 is too sweeping;[32] places unfair burdens upon those called upon to provide assistance;[33] and might raise constitutional concerns.[34]

---

[32] Chemerinsky, *Losing Liberties: Applying a Foreign Intelligence Model to Domestic Law Enforcement*, 51 UCLA LAW REVIEW 1619, 1627-628 (2004)("Section 206 authorizes the FISA court to authorize intercepts on any phones or computers that the target may use. This authority for roving wiretaps means that the police no longer need to list the phone numbers to be tapped; the police can listen to any phone that person might use. This means that the police can listen to all phones where a person works, or shops, or visits. In debates with FBI agents over this provision, they have stated that this even allows the tapping of pay phones that a person regularly walks past. There is, though, a requirement for "minimization" in that agents must stop listening when they learn that the conversation is not pertinent to the subject of their warrant. The argument for roving wiretaps is that suspected terrorists might repeatedly change cell phones. The problem with this argument is that the government, by definition, cannot listen to a phone until they know that it exists. Once they know, they could just add the new number to an existing warrant. In debates with FBI agents, the response always has been that it takes too long to add new number to existing warrants. But this calls for a faster procedure to do so, not roving wiretaps"); Lee, *The USA PATRIOT Act and Telecommunications: Privacy Under Attack*, 29 RUTGERS COMPUTER & TECHNOLOGY LAW JOURNAL 371, 398 (2003)("Until this provision sunsets in 2005, the result may be a back door to massive wiretapping); *The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 NORTH CAROLINA AW REVIEW 412, 421 (2003)("Section 206 gives the federal government excessively broad authority to intrude on the privacy of third parties other than the target of the surveillance"); *EPIC Report* ("Such 'generic' orders could have a significant impact on the privacy rights of large numbers of innocent users, particularly those who access the Internet through public facilities such as libraries, university computer labs and cybercafes. Upon the suspicion that an intelligence target might use such a facility, the FBI can now monitor all communications transmitted at the facility. The problem is exacerbated by the fact that the recipient of the assistance order (for instance, a library) would be prohibited from disclosing the fact that monitoring is occurring").

[33] Whitehead & Aden, at 1105 ("This provision is problematic in that it distorts two extremely important checks in the legal system that historically have provided a measure of accountability for the validity of a warrant. First, the amendment allows the issuance of so-called 'blank warrant,' which the parties require to respond to the order need not be listed on the face of the document. This places such communications providers in the position of having to accept the validity of the warrant and its application to them virtually without question (although the section does permit a provider to inquire with the Attorney General as to who, through his various agents, obtained the order in the first place, whether or not the order is valid). Second the order may not have been issued in the responding party's jurisdiction, creating hindrances of geography and expense for a party that desires to challenge the order in court").

[34] Kollar, *USA PATRIOT Act, the Fourth Amendment, and Paranoia: Can They Read This While I'm Typing It?* 3 JOURNAL OF HIGH TECHNOLOGY LAW 67 (2004)("Even more striking, Section 206 provides authority for the FISC to grant so-called 'roving wiretaps' not specific to a particular jurisdiction, telephone number or email address but which can cross jurisdictional boundaries. This wide latitude effectively permits the surveillance of much otherwise lawful activity, giving rise to Constitutional concerns of overbreadth and vagueness"); Hannigan, *Playing Patriot Games: National Security Challenges Civil Liberties*, 41 HOUSTON LAW REVIEW 1371, 1382 (2004)("The Fourth Amendment of the Constitution protects Americans from unreasonable searches and seizures. However, several provisions of the Patriot Act authorize federal law enforcement to skirt the line of

Summary. Section 206 permits roving FISA surveillance orders; orders need not specifically identify individuals ordered to assist where targets take actions to thwart specific individuals, 50 U.S.C. 1805(c)(2)(B).

- Comparable authority has existed under Title III (18 U.S.C. 2518(4)) for some time.
- Critics claim the provision is too sweeping, perhaps constitutionally so.
- A subsequent amendment (which does not sunset) permits roving surveillance by requiring a FISA order to identify the location and facilities subject to surveillance *only if they are known*, P.L. 107-108, 115 Stat. 1402 (2001)(50 U.S.C. 1805(c)(1)(B)).

Section 207 (duration of FISA surveillance of non-United States persons who are agents of a foreign power).

Under FISA before passage of the act, FISA wiretap orders with the agent of a foreign power as their target had a maximum duration of 90 days, and could be extended in 90 day increments, 50 U.S.C. 1805(e)(2000 ed.). FISA physical search orders and extensions were good for no more than 45 days (but up to one year if a foreign power was the target), 50 U.S.C. 1824(d)(2000 ed.). Section 207 amends the time lines. FISA wiretap orders relating to the agent of foreign power may remain in effect for up to 120 days and may be extended at one year intervals, 50 U.S.C. 1805(e). As a general rule, FISA physical search orders and extensions may be authorized for 90 days (unless they target a foreign power), but orders with an agent of a foreign power as their target may be issued for up to 120 days with extensions for up to one year, 50 U.S.C. 1824(d).

Background. As is often and understandably the case where FISA is the subject, the Administration's statement accompanying its request here is a bit cryptic:

> This section reforms a critical aspect of the Foreign Intelligence Surveillance Act (FISA). It will enable the Foreign Intelligence Surveillance Court (FISC), which presides over applications made by the U.S. government under FISA, to authorize the search and surveillance in the U.S. of officers and employees of foreign powers and foreign members of international terrorist groups for up to a year. Currently, the FISC may only authorize such searches and surveillance for up to 45 days and 90 days, respectively. The proposed change would bring the authorization period in line with that allowed for search and surveillance of the foreign establishments for which the foreign officers and employees work. The proposed change would have no effect on electronic surveillance of U.S. citizens or permanent resident aliens. §151, H.R. --, *Hearings* at 51; *see also*, H.Rept. 107-236 at 59.

---

reasonableness. For example, section 206 of the Patriot Act amends FISA and eases restrictions involving domestic intelligence gathering by allowing a single wiretap to legally roam from device to device, to tap the person rather than the phone"); *EPIC Report* ("The 'generic' roving wiretap orders raise significant constitutional issues, as they do not comport with the Fourth Amendment's requirement that any search warrant 'particularly describe the place to be searched.' That deficiency becomes even more significant where the private communications of law-abiding American citizens might be intercepted").

The Senate scaled back the Administration's request to extend the duration of orders and extensions relating to foreign agents from one year to 120 days, but with extensions for up to one year in the case of agents who are foreign nationals (not U.S. persons), §207, S. 1510, 147 *Cong. Rec.* S10607 (daily ed. Oct. 11, 2001).[35] The Senate view ultimately prevailed, §207, P.L. 107-56, 115 Stat. 282 (2001).

What Does Not Expire. The provisions of section 207 have not been amended. They would appear to remain available for use with respect to any foreign intelligence investigation predating December 31, 2005, but otherwise to expire on that date.

Considerations. The Justice Department apparently views section 207 as a matter of expediency and administrative efficiency:

> The USA PATRIOT Act has also improved the effectiveness of FISA. Under FISA, a federal court ... reviews Department requests for physical searches and electronic surveillance of foreign powers and their agents. Under prior law, the Department could only conduct FISA searches of agents of foreign powers for periods lasting up to 45 days prior to having to seek renewal of such authority from the court. That limitation required federal authorities to waste valuable time and resources by frequently renewing court orders, even when there was no question about the legal sufficiency of a particular case. Section 207 of the USA PATRIOT Act now permits the FISC to authorize physical searches of certain agents of foreign powers (including U.S. persons) for 90 days, and authorizes longer periods of searches and electronic surveillance for certain categories of foreign powers and non-U.S. persons who are agents of foreign powers. In particular for foreign governments and other foreign powers, non-U.S. person officers or employees of certain foreign powers, and non-U.S. person members of international terrorist groups, initial orders authorizing searches and surveillance may be for periods of 120 days, and renewal orders may extend for periods of one year. While the details of FISA operations are classified, the FISC has authorized 90-day and year-long surveillance of foreign powers and their agents pursuant to section 207 of the USA PATRIOT Act. Therefore, the act has not only provided additional time to government investigators targeting potential terrorist activity, it has also helped the government and the FISC to focus their efforts on more significant and complicated terrorism-related cases. *Report* at 17.

This section essentially deals with the regularity of judicial supervision. Critics might argue more not less supervision is appropriate given the increased use of

---

[35] *See*, 147 *Cong. Rec.* S10557 (daily ed. Oct. 11, 2001)(remarks of Sen. Leahy)("The Administration proposed that the period of electronic surveillance be changed from 90 days to one year in these cases. This proposal did not ensure adequate review after the initial stage to ensure that the probable cause determination remained justified over time").

FISA[36] and of the FISA court's remarkably outspoken criticism of the accuracy, candor and sufficiency of presentations to the court.[37]

Summary. Section 207 extends the permissible duration of FISA surveillance and physical search orders and extensions, 50 U.S.C. 1805(e), 1824(d).

- The Justice Department sees section 207 as a time saver that allows for more productive allocation of Department and judicial resources.
- Critics might argue more not less judicial supervision is called for.

Section 214 (pen register and trap and trace authority under FISA).

Section 214 makes several adjustments in the FISA pen register/trap and trace device procedures. FISA once permitted applications for a FISA pen register or trap and trace device order for telephone communications in order to acquire information relevant to a foreign intelligence or international terrorism investigation and upon the additional certification that the communications monitored would likely be either (1) those of an international terrorist or spy ("individual ... engaged in international terrorism or clandestine intelligence activities that ... involve a violation of [U.S.] criminal laws") or (2) those of a foreign power or its agent relating to the criminal activities of an international terrorist or spy, 50 U.S.C. 1842(a)(1), (c)(2), (c)(3), (i)(2000 ed.).

Section 214 opens the FISA pen register/trap and trace device procedure to both wire and electronic communications (e.g., telephone, e-mail, Internet communications), 50 U.S.C. 1824(i). It drops the requirement that the communications be those of international terrorists or spies or be related to their activities, 50 U.S.C. 1824(c)(2). It adds the caveat that any investigation of a U.S. person for which a order is secured "to protect against international terrorism or clandestine intelligence activities" may not be conducted based solely on activities protected by the first amendment to the Constitution, 50 U.S.C. 1842(a)(1), (c)(2).

---

[36] The FBI reported an 85% increase in FISA applications from 2001 to 2003, *The FBI's Counterterrorism Program Since September 2001: Report to the National Commission on Terrorist Attacks upon the United States*, 64 (April 14, 2004). Annual reports to Congress on the number of FISA surveillance and physical search applications, beginning with calendar year 1995, appear on the Department of Justice's website, available on Feb. 11, 2005 at [http://www.usdoj.gov/ag/readingroom/ag_foia1.htm].

[37] *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F.Supp.2d 611, 620-21 (FISC 2002)("In September 2000, the government came forward to confess error in some 75 FISA applications related to major terrorist attacks directed against the United States. The errors related to misstatements and omissions of material facts.... In November of 2000, the Court held a special meeting to consider the troubling number of inaccurate FBI affidavits in so many FISA applications. After receiving a more detailed explanation from the Department of Justice about what went wrong, but not why, the Court decided not to accept inaccurate affidavits from FBI agents whether or not intentionally false. One FBI agent was barred from appearing before the Court as a FISA affiant ... In March of 2001, the government reported similar misstatements in another series of FISA applications....").

It adds this same caveat with respect to emergency FISA pen register or trap and trace device use, 50 U.S.C. 1843(a),(b)(1).

Background. The Administration's original request sought to make pen register and trap and trace device procedures more compatible:

> When added to FISA two years ago, the pen register/trap and trace section was intended to mirror the criminal pen/trap authority defined in 18 U.S.C. §3123. The FISA authority differs from the criminal authority in that it requires, in addition to a showing of relevance, an additional factual showing that the communications device has been used to contact an "agent of a foreign power" engaged in international terrorism or clandestine intelligence activities. This has the effect of making the FISA pen/trap authority much more difficult to obtain. In fact, the process of obtaining FISA pen/trap authority is only slightly less burdensome than the process for obtaining full electronic surveillance authority under FISA. This stands in stark contrast to the criminal pen/trap authority, which can be obtained quickly from a local court, on the basis of a certification that the information to be obtained is relevant to an ongoing investigation. The amendment simply eliminates the "agent of a foreign power" prong from the predication, and thus makes the FISA authority more closely track the criminal authority. §155, H.R. --, *Hearings* at 57; *see also*, §155, H.R. 2975, H.Rept. 107-236 at 61.

The Senate added the instruction that denies pen register/trap and trace device authority in the case of an investigation predicated entirely upon its target's exercise of first amendment rights, §214, S. 1510, 147 *Cong. Rec.* S10608 (daily ed. Oct. 11, 2001).

What Does Not Expire. Except for on-going investigations, the FISA pen register/trap and trace device provisions revert to form on December 31, 2005. No relevant amendments have been enacted since passage of the act.

Considerations. The streamlined authority apparently has been used in the investigation of suspected al Qaeda agents in this country:

> The USA PATRIOT Act also has updated federal pen-trap law under FISA by making the legal requirements for obtaining court permission for pen/trap orders in international terrorism investigations more similar to the standards that apply in ordinary criminal cases. Previously, FISA-authorized pen/trap orders were available in terrorism investigations only if the suspect was, or was communicating with an "agent of a foreign power." FISA thus prevented officials from using pen/trap devices in many settings that might have revealed information relevant to a foreign intelligence investigation. Under section 214 of the act, however, the government now can obtain a pen/trap order when the information likely to be obtained is foreign intelligence information or is relevant to investigations intended to protect against international terrorism or "clandestine intelligence activities." While specific examples of the use of pen/trap devices pursuant to section 214 remain classified, the Department has utilized section 214 on several occasions in international terrorism investigations, including investigations of suspected al Qaeda operatives in the United States, and the streamlined pen/trap authority has made it easier to identify additional subjects in terrorism investigations. *Report,* at 25-6.

Critics might argue that streamlining the FISA pen register/trap and trace device procedure is particularly ill-advised. First, the procedure is already subject to a minimum of judicial supervision; orders are issued upon the FBI's certification of relevance not upon the court's finding of relevance;[38] unlike wiretap orders, there is no requirement that the targets of the order be notified after the order expires unless the results are to be used as evidence in official proceedings;[39] unlike comparable orders in the criminal sphere, there is no requirement of a subsequent report to the court of the particulars of execution;[40] criminal orders call for judicial re-examination every 60 days, FISA orders every 90 days.[41] Second, the nature and extent of the expanded authority is substantial. Where orders once permitted authorities to monitor the identification of parties to telephone conversations over particular instruments, they now permit authorities to monitor Internet use.[42] Third, in terrorism cases officials presumable enjoy adequate law enforcement authority under section 216 of the act which does not expire. Some critics find the section disquieting for constitutional reasons.[43]

---

[38] 50 U.S.C. 1842.

[39] *Compare*, 50 U.S.C. 1845, *with*, 18 U.S.C. 2517(8)(d).

[40] *Compare*, 50 U.S.C. 1842, *with*, 18 U.S.C. 3123(a)(3).

[41] *Compare*, 50 U.S.C. 1842(e), *with*, 18 U.S.C. 3123(c).

[42] Whitehead & Aden, at 1106 ("These expanded powers to monitor telecommunications [in sections 214 and 216] are particularly prone to abuse in the Internet age, since pen register and trap and trace orders now disclose not only standard telephone numbers called by or dialing in to a subject, but also Internet URLs and dedicated lines for data transmission. The ability to monitor Internet sites visited by the subject to a search, in the absence of a showing probable cause or even reasonable suspicion, is an unprecedented expansion of federal surveillance powers"); *National Security at What Price?: A Look into Civil Liberty Concerns in the Information Age under the USA PATRIOT Act of 2001 and a Proposed Constitutional Test for Future Legislation*, 12 CORNELL JOURNAL OF LAW AND PUBLIC POLICY 447, 460 (2003)("The effect of pen registers on personal rights is that pen registers can capture a great deal more information than merely a telephone number. Not requiring probable cause for these devices rested on judicial reasoning that neither the trap and trace nor the pen register devices, could, prior to the USA PATRIOT Act capture the substantive material of the communication in question. the USA PATRIOT Act's expansion of and consolidation of the definitions of pen registers and trap and trace devices endanger the original distinction upon which the lower level of scrutiny was justified. The expanded definition would now seem to cover Web surfing, e-mail messages, electronic fax distributions, and any other electronic form of communication. The FBI justifies these definitional expansions by interpreting Web traffic as substantially similar to telephone conversations. Despite the substantial differences, including the vast amount of information available from an e-mail routing protocol that cannot be gleaned from listening to a phone conversation, this issue has never been litigated and remains unresolved").

[43] *EPIC Report* ("The amendment significantly eviscerates the constitutional rationale for the relatively lax requirements that apply to foreign intelligence surveillance. That laxity is premised on the assumption that the Executive Branch, in pursuit of its national security responsibilities to monitor the activities of foreign powers and their agents should not be unduly restrained by Congress and the courts. The removal of the 'foreign power' predicate for pen register/trap and trace surveillance upsets that delicate balance").

Summary. Section 214 recasts FISA pen register/trap & trace order procedures so that they apply to electronic (e-mail and other Internet communications as well as to telephone communications), 50 U.S.C. 1842.

- The change is comparable in some respects to a similar enlargement for law enforcement in §216 which does not expire, 18 U.S.C. 3123(b), 3127(4)).
- The section precludes exercise of emergency authority or issuance in connection with an investigation based solely on the exercise of first amendment rights.
- The section is constitutionally permissible, but requires court order nonetheless and is first amendment sensitive.
- Critics might argue that the expansion to cover Internet use is dramatic; that the FISA expansion lacks some of the safeguards found in its law enforcement counterparts; and that in terrorism cases the authority available to law enforcement officials under section 216 of the act which does not expire should be sufficient.

Section 215 (access to records and other items under the Foreign Intelligence Surveillance Act).

FISA originally authorized a FISA court order (in a terrorism investigation or an effort to gather foreign intelligence information) for FBI access to the business records of hotels, motels, car and truck rental agencies, and storage rental facilities, 50 U.S.C. 1862 (2000 ed.). An application for such an order had to assert that there were "specific and articulable facts giving reason to believe that the person to whom the records pertain [was] a foreign or an agent of a foreign power," 50 U.S.C. 1862(b)(2)(2000 ed.). Section 215 expands the authority to include not only business records but any tangible item regardless of the business or individual holding the item and upon the simple assertions that the records are sought in an effort to obtain foreign intelligence (not based solely on the first amendment protected activities of a U.S. person) or in a terrorism investigation, 50 U.S.C. 1861.[44]

Background. Section 215 began as a request for administrative subpoena authority to replace a more narrowly drawn FISA procedure:

> The "business records" section of FISA (50 U.S.C. §§ 1861 and 1862) requires a formal pleading to the Court and the signature of a FISA judge (or magistrate). In practice, this makes the authority unavailable for most investigative contexts. The time and difficulty involved in getting such pleadings before the Court usually outweighs the importance of the business records sought. Since its enactment, the authority has been sought less than five times. This section would delete the old authority and replace it with a general "administrative subpoena" authority for documents and records. This authority,

---

[44] The act itself limited authority under section 215 to cases involving "investigations to protect against international terrorism and clandestine intelligence activities," but a later intelligence authorization act amended the section to include "investigations to obtain foreign intelligence information not concerning a United States person," P.L. 107-108, §314(a)(6), 115 Stat. 1402 (2001).

> modeled on the administrative subpoena authority available to drug investigators pursuant to Title 21, allows the Attorney General to compel protection of such records upon a finding that the information is relevant. §156, H.R. --, *Hearings*, at 57.

The House Judiciary Committee converted the request into an amendment of the earlier FISA procedure. In doing so it preserved at least a modicum of judicial supervision while acceding to the Administration's request for more expansive authority.[45]

What Does Not Expire. Section 215 expires on December 31, 2005, except with respect to on-going foreign intelligence investigations, at which point the law reverts to the hotel-motel-car-rental business records procedure that the predates the act. There are no subsequent amendments to the act or to FISA that alter the consequences of that reversion, but the impact of expiration may be mitigated by changes in the law governing "national security letters" that provide access to a wider range of business records after sunset.

Provisions in the Right to Financial Privacy Act, the Fair Credit Reporting Act, and chapter 121 of title 18 of the United States Code, authorize the FBI when investigating international terrorism or clandestine intelligence activities to request access to business records held by banks, credit report agencies, and communications carriers, 12 U.S.C. 3414, 15 U.S.C. 1681, 18 U.S.C. 2709. Section 374 of the 2004 intelligence authorization act amends the Right to Financial Privacy Act to give the FBI access to business records held not only by banks, but by credit card companies, car dealers, real estate agencies, stock brokers, jewelers, and certain other business occasionally marked by large cash transactions, P.L. 108-177, 117 Stat.2628 (2003) (amending 12 U.S.C. 3414 to the make the definition of "financial institution" found in 31 U.S.C. 5312 applicable).

Considerations. Section 215 has been among the more hotly debated sections of the act. Librarians and library associations have been among its more vocal critics. The Justice Department has responded that:

> The library habits of ordinary Americans are of no interest to those conducting terrorism investigations. However, historically terrorists and spies have used libraries to plan and carry out activities that threaten our national security ... Obtaining business records is a long-standing law enforcement tactic. Ordinary grand juries for years have issued subpoenas to all manner of businesses, including libraries and bookstores, for records relevant to criminal inquiries.... Section 215 authorized the FISA court to issue similar orders in national security investigations. It contains a number of safeguards that protect civil liberties.

---

[45] "The Administration had sought administrative subpoena authority without having to go to court. Instead, section 156 amends title 40 U.S.C. §1861 by providing for an application to the FISA court for an order directing the production of tangible items such as books, records, papers, documents and other items upon certification to the court that the records sought are *relevant to an ongoing foreign intelligence investigation*. The amendment also provides a good faith defense for persons producing items pursuant to this section which does not constitute a waiver of any privilege in any other proceeding," H.Rept. 107-236, at 16 (emphasis added).

> Section 215 requires FBI agents to get a court order... Section 215 has a narrow scope... It cannot be used to investigate ordinary crimes, or even domestic terrorism. Section 215 preserves First Amendment rights.... Section 215 provides for congressional oversight. *Myths* at §215.

Section 215 authority appears to have been little used. Critics decry the section's expansion beyond agents of a foreign power as well as its secrecy provisions.[46] They also question its constitutionality.[47]

Summary. Section 215 provides access to tangible items under the Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. 1861, by authorizing ex parte FISA court orders in foreign intelligence (as amended), international terrorism, and clandestine intelligence cases.

- It reverts at sunset to the vehicle rental, transportation, storage rental, and housing accommodation business records pertaining to foreign power or agent, 50 U.S.C. 1861, 1862 (2000 ed.).
- Other legislation expanding the definition of financial institution for national security letter purposes, P.L.108-177, 117 Stat. 2628

---

[46] Lee, *The USA PATRIOT Act and Telecommunications: Privacy Under Attack*, 29 RUTGERS COMPUTER & TECHNOLOGY LAW JOURNAL 371, 379-80 (2003)("By expanding the scope, Congress has now put the computer servers, records, and other property of ISPs and other telecommunications entities within greater reach of law enforcement agents. One particular concern with this and similar provisions, is that one whose records are sought need not be an agent of a foreign power. United States citizens could potentially be investigated on account of activities connecting them to an investigation of international terrorism, provided that the investigation is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution. This section is problematic in other ways. Judges, for example, have no authority to deny a request if the application meets the requirements of the section. It is unnecessary to report the actual documents seized or their usefulness to the court or Congress. While section 215(e) does not waive any privilege, persons served by an order are gagged. Furthermore, the act overrides federal privacy statutes and explicitly bars notice to the party whose records are being disclosed. Individuals would be unaware of whether the government is unfairly inquiring into their extremely private information").

[47] *The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 NORTH CAROLINA LAW REVIEW 412, 423 (2003)("The combination of eliminating the reasonable suspicion standard and expanding FISA to any United States person signifies that United States citizens can be ordered to produce records without any level of individualized suspicion of wrongdoing. By extending FISA beyond foreign powers and their agents to United States persons and by no longer requiring individualized suspicion to search United States persons and seize records, the federal government has circumvented the Fourth Amendment in the name of combating international terrorism. Even where exceptions to the warrant requirement apply, probable cause is almost always required except where special circumstances justify searches based on reasonable suspicion or suspicionless searches. Section 215 is unconstitutional in that it eliminates the reasonable suspicion type standard and extends FISA to United States persons contrary to the purpose of FISA and the spirit of the Fourth Amendment").

(2003)(12 U.S.C. 3414) might be thought to compensate for reduced authority upon reversion.
- Grand juries can subpoena the same material with fewer restrictions or protections; section 215 FISA orders demand senior official and judicial approval, explicit first amendment adherence, and Congressional reporting.
- In many instances the same material is available using national security letter (nsl) authority.
- It is only to be used in serious national security cases.
- The authority has been rarely used, i.e., there is no evidence of abuse or the section is unnecessary, depending on one's perspective.
- The section produces an environment of abuse through its elimination of safeguards (limited to third parties; requires neither probable cause nor "articulable facts;" and need not be limited to items relating to the target of the investigation) and through its use of a procedure that already carries reduced safeguards (use of a secret court, which does not weigh the evidence; and one-way gag orders of unknown breath and duration).

Section 218 (foreign intelligence information ("the wall")).

At one time, applications for a FISA wiretap or physical search order were required to certify that "the" purpose for seeking the order was to obtain foreign intelligence information, 50 U.S.C. 1804(a)(7)(B), 1823(a)(7)(B)(2000 ed.). This, and FISA's minimization requirements, among other things, led to the view that FISA required a wall of separation between law enforcement and intelligence investigations. Section 218 was designed to promote greater cooperation and information sharing among criminal and foreign intelligence investigators, to remove the "wall" that had been administratively constructed between. It does so by authorizing FISA wiretap or physical search order applications even if the acquisition of foreign intelligence information is no more than a "significant" reason for the application, 50 U.S.C.1804(a)(7)(B), 1823(a)(7)(B). The FISA review court concluded that this standard permits applications where intelligence information collection supplies some measurable reason for the application and that the provision passes constitutional muster, *In re Sealed Case*, 310 F.3d 717, 735-46 (F.I.S.Ct.Rev. 2002).

Background. The Supreme Court has held that the assertion of the President's national security powers will not excuse the failure to comply with the Fourth Amendment's warrant requirements during the course of an investigation of domestic terrorists, *United States v. United States District Court (Keith)*, 407 U.S. 297, 314-21 (1972). The Court expressly declined to address or express any opinion with regard to "the issues which may be involved with respect to activities of foreign powers or their agents," Id. at 321-22. Nor would the Court hold that standards and procedures similar those of Title III need necessarily have to be duplicated in such cases, Id. at 22.

Prior to *Keith*, "[f]or decades Presidents had claimed inherent power to conduct warrantless electronic surveillance in order to gather foreign intelligence in the interests of national security," *ACLU v. Barr*, 952, F.2d 457, 460 (D.C. Cir. 1991).

Following *Keith*, when defendants in criminal proceedings raised constitutional challenges the lower federal courts in at least three circuits "sustained the President's power to conduct warrantless electronic surveillance for *the primary purpose* of gathering foreign intelligence information, *Id.* at 461(emphasis added).[48] After Congress enacted FISA, several courts used this "primary purpose" language to respond to the arguments of criminal defendants who challenged the FISA "the purpose" certification and who argued that FISA had been used solely to avoid the more stringent Title III requirements demanded in a criminal investigation.[49]

In the aftermath of 9/11, the Administration sought to change the "the purpose" certification requirement to a "a purpose" certification requirement, §153, H.R.--, *Hearing*, at 74. Its explanation was concise, "Current law requires that FISA be used only where foreign intelligence gathering is the sole or primary purpose of the investigation. This section will clarify that the certification of a FISA request is supportable where foreign intelligence gathering is 'a' purpose of the investigation. This change would eliminate the current need continually to evaluate the relative weight of criminal and intelligence purposes, and would facilitate information sharing between law enforcement and foreign intelligence authorities which is critical to the success of anti-terrorism efforts," *Hearing* at 56-7.

Both House and Senate bills substituted the final language, "a significant purpose," §153, H.R. 2975, H.Rept. 107-236, at 8; §218, S. 1510, 147 *Cong. Rec.* S10313 (daily ed. Oct. 4, 2001). The House Judiciary Committee characterized the change as "a compromise between current law and what the Administration has proposed," H.Rept. 107-236, at 60, and the FISA review court concluded that the change "imposed a requirement that the government have a measurable foreign

---

[48] Citing, *United States v. Brown*, 484 F.2d 418 (5th Cir. 1973); *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974); and *United States v. Truong*, 629 F.2d 908 (4th Cir. 1980).

[49] *United States v. Duggan*, 743 F.2d 59, 77-8 (2d Cir. 1984)(emphasis added)("FISA permits federal officials to obtain orders authorizing electronic surveillance 'for the purpose of obtaining foreign intelligence information. The requirement that foreign intelligence information be the *primary objective* of the surveillance is plain not only from the language of §1802(b) but also from the requirements ain §1804 as to what the application must contain... [O]therwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used, as allowed by §1806(b), as evidence in a criminal trial"); *United States v. Pelton*, 835 F.2d 1067, 1075-1076 (4th Cir.1987)("We also reject Pelton's claim that the 1985 FISA surveillance was conducted primarily for the purpose of his criminal prosecution, and not primarily 'for the purpose of obtain foreign intelligence information' as required by 50 U.S.C. 1802(b) ... We agree with the district court that the primary purpose of the surveillance, both initially and throughout, was to gather foreign intelligence information"); *cf., United States v. Johnson*, 952 F.2d 565, 572 (1st Cir. 1991)("FISA applications must contain, among other things, a certification that the purpose of the requested surveillance is the gathering of foreign intelligence information.... Although evidence obtained under FISA subsequently may be used in criminal prosecutions, the investigation of criminal activity cannot be the primary purpose of the surveillance"); *but see*, *United States v. Sarkissian*, 841 F.2d 959, 964 (9th Cir. 1988)(declining to adopt the "primary purpose" standard); *United States v. Hammoud*, 381 F.3d 316, 334 (4th Cir. 2004)(construing FISA in its pre-USA PATRIOT Act form) ("even if the primary purpose requirement test applies, it is satisfied here").

intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes," *In re Sealed Case*,310 F.3d 717, 735 (F.I.S.Ct.Rev. 2002).

What Does Not Expire. Section 218 sunsets on December 31, 2005 except with respect to foreign intelligence investigations initiated before that date. Whether the wall of separation between criminal and foreign intelligence investigations will be or must be reconstructed at that point is unclear at best. Section 504 of the act (which does not sunset) adds language to the FISA wiretap and physical search schemes calling for continued cooperation and declaring cooperation no bar to the certification in a FISA application of an intelligence-gathering purpose, 50 U.S.C. 1806(k), 1825(k).[50]

Moreover, the Department of Justice and the FISA review court now appear to doubt that FISA prior to passage of the act required such a wall of separation.[51] Thus, the expiration of section 218 may not require reconstruction of the wall, although applications for FISA wiretap or search orders would once again have to certify that foreign intelligence gathering constituted "the" purpose for the application.

---

[50] "Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against – (A) actual or potential attack or other grave hostile acts of a foreign power or agent of a foreign power; (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power. (2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 104(a)(7)(B) [50 U.S.C. 1804]or the entry of an order under section 105 [50 U.S.C. 1805]," 50 U.S.C. 1805(k). Similar language appears in 1825(k) for physical searches.

[51] "[I]t is quite puzzling that the Justice Department, at some point during the 1980s, began to read the statute as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents ... Apparently to avoid running afoul of the primary purpose test used by some courts, the 1995 Procedures limited contacts between the FBI and the Criminal Division in cases where FISA surveillance or searches were being conducted by the FBI for foreign intelligence (FI) or foreign counterintelligence (FCI) purposes. The procedures stated that 'the FBI and Criminal Division would ensure that advice intended to preserve the option of a criminal prosecution does not inadvertently result in either the fact or the appearance of the Criminal Division's directing or controlling the FI or FCI investigation toward law enforcement objectives'. Although these procedures provided for significant information sharing and coordination ... they eventually came to be narrowly interpreted within the Department of Justice ... as requiring ... a wall to prevent the FBI intelligence officials from communicating with the Criminal Division regarding ongoing FI or FCI investigations. The Department's attitude changed somewhat after [internal and General Accounting Office reports] concluded that the Department's concern over how the FISA court or other federal courts might interpret the primary purpose test had inhibited necessary coordination between intelligence and law enforcement officials. [The internal] report also concluded, based on the text of FISA and its legislative history, that not only should the purpose of the investigation not be inquired into by the courts, but also that Congress affirmatively anticipate that the underlying investigation might well have a criminal as well as foreign intelligence objective," 310 F.3d at 723, 725, 727.

Considerations. Section 218 is perhaps the most fundamental of the changes accomplished by the expiring sections of the act. Therefore it is not surprising that the Justice Department's defense of the section is both extensive and explicit:

> The USA PATRIOT Act authorizes government agencies to share intelligence so that a complete mosaic of information can be compiled to understand better what terrorists might be planning and to prevent attacks. Prior law, as interpreted and implemented, had the effect of sharply limiting the ability of law enforcement and intelligence officers to share information, which severely hampered terrorism investigators' ability to connect the dots. However, the USA PATRIOT Act, along with changes in Attorney General Guidelines and Foreign Intelligence Surveillance Act (FISA) court procedures, brought down this wall separating intelligence from law enforcement and greatly enhanced foreign intelligence information sharing among federal law enforcement and national security personnel, intelligence agencies, and other entities entrusted with protecting the nation from acts of terrorism. This increased ability to share information has been invaluable to the conduct of terrorism investigations and has directly led to the disruption of terrorist plots and numerous arrests, prosecutions, and convictions in terrorism cases.
>
> The recent investigation and prosecution of members of an al Qaeda cell in Lackawanna, New York illustrates the benefits of the increased information sharing brought about by the USA PATRIOT Act. This case involved several residents of Lackawanna, who traveled to Afghanistan in 2001 to receive training at an al Qaeda-affiliated camp near Kandahar. The investigation of the "Lackawanna Six" began during the summer of 2001, when the FBI received an anonymous letter indicating that these six individuals and others might be involved in criminal activity and associating with foreign terrorists. The FBI concluded that existing law required the creation of two separate investigations in order to retain the option of using FISA: a criminal investigation of possible drug crimes and an intelligence investigation related to terrorist threats. Over the ensuing months, two squads carried on these two separate investigations simultaneously, and there were times when the intelligence officers and the law enforcement agents concluded that they could not be in the same room during briefings to discuss their respective investigation with each other.
>
> The USA PATRIOT Act, however, took down the "wall" separating these two investigations by making clear that the sharing of case-sensitive information between these two groups was allowed. As a result of key information shared by intelligence investigators, law enforcement agents were able to learn that an individual mentioned in the anonymous letter was an agent of al Qaeda. Further information shared between intelligence and law enforcement personnel then dramatically expedited the investigation of the Lackawanna Six and allowed charges to be filed against these individuals. Five of the Lackawanna Six pleaded guilty to providing material support to al Qaeda, and the sixth pleaded guilty to conducting transactions unlawfully with al Qaeda. These individuals were then sentenced to prison terms ranging from seven to ten years.
>
> Before the passage of the USA PATRIOT Act, 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 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 such coordination, the more coordination that occurred, the most likely courts would find that law enforcement, rather than foreign intelligence, had become the primary purpose of the surveillance or search.

* * *

In recent testimony before the Senate Judiciary Committee, Patrick Fitzgerald, U.S. Attorney for the Northern District of Illinois, recounted from personal experience how this "wall' between law enforcement and intelligence personnel operated in practice:

I was on a prosecution team in New York that began a criminal investigation of Usama Bin Laden in early 1996. The team – prosecutors and the FBI agents assigned to the criminal case – had access to a number of sources. We could talk to citizens. We could talk to local police officers. We could talk to other U.S. Government agencies. We could talk to foreign police officers. Even foreign intelligence personnel. And foreign citizens. And we did all those things as often as we could. We could even talk to al Qaeda members – and we did. We actually called several members and associates of al Qaeda to testify before a grand jury in New York. And we even debriefed al Qaeda members overseas who agreed to become cooperating witnesses.

But there was one group of people we were not permitted to talk to. Who? The FBI agents across the street from us in lower Manhattan assigned to a parallel intelligence investigation of Usama Bin Laden and al Qaeda. We could not learn what information they had gathered. That was the "wall."

The USA PATRIOT Act brought down the "wall" separating intelligence officers from law enforcement agents....

Section 218 of the USA PATRIOT Act eliminated the "primary purpose" requirement....

The Department has moved aggressively to implement sections 218 and 504 of the USA PATRIOT Act and bring down "the wall."

These efforts to increase coordination and information sharing between intelligence and law enforcement officers, which were made possible by the USA PATRIOT Act, have yielded extraordinary dividends by enabling the Department to open numerous criminal investigations, disrupt terrorist plots, bring numerous criminal charges, and convict numerous individuals in terrorism cases.

Examples:

- The removal of the "wall" separating intelligence and law enforcement personnel played a critical 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.... [A]t least one member of the cell [Battle] had contemplated attacking Jewish schools or synagogues and had even cased such buildings to select a target for such an attack. By the time investigators received this information from the undercover

> informant, they had suspected that a number of other persons ... 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 domestic 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 sections 218 and 504 ... 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 o 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. Charges against the seventh defendant were dismissed after he was killed in Pakistan by Pakistani troops.... Without sections 218 and 504 of the USA PATRIOT Act, however, this case like would have been referred to as the "Portland One" rather than the "Portland Seven."

- The Department shared information pursuant to sections 218 and 504 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 the world's most violent terrorist outfits....

In this case, sections 218 and 504 ... 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....

- Prosecutors and investigators also used information shared pursuant to sections 218 and 504 ... in investigating the defendant in the so-called "Virginia Jihad" case ...

- The information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 ... was useful in the investigation of two Yemeni citizens ... who were charged last year with conspiring to provide material support to al Qaeda and HAMAS....

- The Department used sections 218 and 504 to gain access to intelligence, which facilitated the indictment of Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation(BIF).... Arnaout ultimately pleaded guilty to a

racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic military groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

- The broader information sharing and coordination made possible by sections 218 and 504 ... assisted the prosecution in San Diego of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in several guilty pleas. Two defendants 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 officials. 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....

- Sections 218 and 504 were critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted ... of illegally acting as an agent of the former government of Iraq.... During this investigation, intelligence officers conducting surveillance of Dumeisi pursuant to FISA coordinated and shared information with law enforcement agents and prosecutors investigating Dumeisi for possible violations of criminal law. Because of this coordination, law enforcement agents and prosecutors learned from intelligence officers 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 Dumeisi's trial. *Report*, at 2-8.

The absence of the wall has stimulated concerns that the cooperation between law enforcement and intelligence officials creates the risk that coordination could be used to evade the restricting safeguards the law imposed upon each.

The FISA appellate court found no Fourth Amendment infirmity in section 218:

> Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close. We, therefore, believe firmly ... that FISA as amended [by section 218] is constitutional because the surveillances it authorizes are reasonable. *In re Sealed Case*, 310 F.3d 717, 746 (F.I.S.Ct.Rev. 2002).

Yet "commentators have reached differing conclusions regarding the *In re Sealed Case* court's Fourth Amendment holding. The court's Fourth Amendment analysis has been criticized for 'resting on shaky and previously unexplored ground'

and reach[ing] the wrong conclusion under Fourth Amendment principles and precedent."[52]

Summary. By virtue of section 218 FISA surveillance or physical search applications need only certify that foreign intelligence gathering is a "significant" purpose for seeking the order rather than "the" purpose, 50 U.S.C. 1804(a)(7)(B), 1823(a)(7)(B).

- The section makes it clear that a "wall" between FBI criminal and intelligence investigators is unnecessary.
- Section 504 (50 U.S.C. 1806(k); 1825(k))(law enforcement cooperation does not preclude purpose certification) which does not expire may be sufficient to prevent reconstruction of the wall.
- *In re Sealed Case*, 310 F.3d 717 (F.I.S.Ct.Rev. 2002) suggests that even prior to the USA PATRIOT Act the wall was neither constitutionally nor statutorily required.
- Facially, FISA procedure for issuance of a surveillance order seems more demanding than Title III (law enforcement wiretaps) but more accommodating after issuance.
- Use of FISA has increased dramatically over the years; Title III seems to be seldom used in terrorism cases (mostly used in drug trafficking cases).
- The existence of the wall is like trying to do one jigsaw puzzle on two separate tables.
- The wall prevented effective communication and cooperation in terrorism cases; removal has been beneficial.
- The wall was designed to guarantee that law enforcement and intelligence officer would honor the limitations placed upon their respective wiretapping and search warrant authority.

Section 223 (civil liability for certain unauthorized disclosures).

Section 223 is discussed above.

---

[52] *The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 NORTH CAROLINA LAW REVIEW 412, 425 (2003), quoting, *Foreign Intelligence Surveillance Court of Review Holds that Prosecutors May Spy on American Agents of Foreign Powers Without a Warrant – In re Sealed Case, 310 F.3d 717 (F.I.S.Ct.Rev. 2002)*, 116 HARVARD LAW REVIEW 2246, 2250 (2003), and citing, Whitehead & Aden, at 1101-104. *See also, Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 YALE LAW JOURNAL 179, 199 (2003)("sweeping opinion that contradicted longstanding interpretations of FISA across the circuits"); *The Fuss Over Two Small Words: The Unconstitutionality of the USA PATRIOT Act Amendments to FISA Under the Fourth Amendment*, 71 GEORGE WASHINGTON LAW REVIEW 291, 345 (2003)("the Review Court far from resolved the issue of whether FISA is constitutional under the Fourth Amendment and its holding remains vulnerable to collateral attack in the federal courts").

Section 225 (immunity for compliance with FISA wiretap).

Federal wiretap law immunizes those who assist in the execution of a law enforcement interception order, 18 U.S.C. 2511(2)(a), FISA supplies a similar immunity for those who assist in the execution of a FISA pen register or trap and trace device order, 50 U.S.C. 1842(f). On its face, section 225 seems to grant immunity to anyone who complies with a FISA order – surveillance (wiretap), physical search, pen register/trap and trace device, or access to tangible items – that is, providing a grant of immunity for compliance with an order under the entire Act.[53] It may be, however, the immunity is only available for compliance with a FISA surveillance order; hence, the reference to a FISA wiretap in the caption, and the subsection's placement in 50 U.S.C. 1805 which relates to the issuance of FISA wiretap orders and which empowers the court to order a "common carrier, landlord, custodian, or other specified person" to furnish "all information, facilities, or technical assistance" for execution of a surveillance order.

Background. Section 225 came late to the legislative process. It cannot be found in the Administration request, *Hearings*, at 67-90, or in S. 1501 as passed by the Senate, 147 *Cong. Rec.* S10604-630 (daily ed. Oct. 11, 2001), or in H.R. 2975 as passed by the House, 147 *Cong. Rec.* H6726-758 (daily ed. Oct. 12, 2001). It first appears at the eleventh hour in H.R. 3162, 147 *Cong. Rec.* H7166 (daily ed. Oct. 23, 2001). The section-by-section analysis that accompanied consideration of the bill simply states, "Provides immunity from civil liability from subscribers, tenants, etc. for entities that comply with FISA wiretap orders," 147 *Cong. Rec.* H7198 (daily ed. Oct. 23, 2001).

What Does Not Expire. Except for assistance provided with respect to investigations begun beforehand, section 225 immunity disappears on December 31, 2005. As with the expiring "cause of action"clauses of section 223, the expiring "no cause of action" clauses of section 225, may be subject to a number of interpretations. If the sunset exception in section 224(b) does no more than continue pending investigations in place, then it is no more likely to preserve a grant of immunity than to grant a cause of action. Conversely, both a cause of action and immunity from liability arising out of an investigation might be thought to survive because they can be characterized as matters "[w]ith respect to any particular foreign intelligence investigation" or "with respect to any particular offense or potential offense" began or occurring before December 31, 2005.

Considerations. In the absence of an explicit enforcement device, explicit immunity provisions encourage communications providers and other third parties to cooperate in the execution of a FISA order. On the other hand, immunity from civil liability removes one of the principal incentives for a third party addressed in a FISA order to petition the court to quash or modify the order.

---

[53] 50 U.S.C. 1805(h)(emphasis added)("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*").

Summary. Section 225 establishes immunity for assistance in the execution of a FISA surveillance order, and perhaps for compliance with any FISA order, 50 U.S.C. 1805(h).

- It encourages cooperation and discourages court challenges.

Section 6001 of P.L. 108-458 (individual terrorists as agents of foreign powers).

As noted at the outset, section 6006 of the Intelligence Reform and Terrorism Prevention Act of 2004, P.L. 108-458, 118 Stat. 3742 (2004), (a) amends the definition of "agent of a foreign power" for FISA purposes to include a foreign national who is preparing for or engaging in international terrorism, and (b) makes the sunset provisions of section 224 applicable to the amendment.[54] FISA makes agents of a foreign power the appropriate targets for FISA surveillance and physical search orders, 18 U.S.C. 1805, 1824. The definition of agents of a foreign power already included individuals preparing for or engaging in international terrorism *for or on behalf of a foreign power,* 50 U.S.C. 1801(b)(2)(C). Section 6001 excuses the need to show that the illicit activity is being conducted at the behest or benefit of a foreign power – as long as the target is not an American (not a U.S. person).

Background. The language of section 6001 is identical to that of section 1 of S. 113, as passed by the Senate, 149 *Cong. Rec.* S5899 (daily ed. May 8, 2003); S.Rept. 108-40 (2003).[55] On the House side, the Judiciary Committee report on H.R. 10 had recommended a comparable provision in the form of a presumption, H.Rept. 108-724, Pt. 5, at 34,170-1 (2004). Similar legislative proposals had been considered during the 107th Congress, *see e.g., S. 2586 and S. 2659, Amendments to the Foreign Intelligence Surveillance Act: Hearing Before the Senate Select Comm. on Intelligence,* 107th Cong., 2d Sess. (2002).

---

[54] Section 6001 provides, "(a) In General.– Section 101(b)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801(b)(1)) is amended by adding at the end the following new subparagraph: '(C) engages in international terrorism or activities in preparation therefore; or'. (b) Sunset. – The amendment made by subsection (a) shall be subject to the sunset provision in section 224 of Public Law 107-56 (115 Stat. 295), including the exception provided in subsection (b) of such section 224."

FISA defines international terrorism to mean "activities that – (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended – (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnaping; and (3) occur totally outside the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum," 50 U.S.C. 1801(c) .

[55] See CRS Report RS22011, *Intelligence Reform and Terrorism Prevention Act of 2004: "Lone Wolf" Amendment to the Foreign Intelligence Surveillance Act*; and CRS Report RS21472, *Proposed Change to the Foreign Intelligence Surveillance Act (FISA) under S. 113*.

The Senate report explains the rationale for the section as it appeared in S. 113:

> The purpose of S. 113 is to amend the Foreign Intelligence Surveillance Act of 1978 (FISA) ... to permit surveillance of so-called "lone wolf" foreign terrorists. S. 113 would allow a FISA warrant to issue upon probable cause that a non-United States person is engaged in or preparing for international terrorism, without requiring a special showing that the non-United States person also is affiliated with a foreign power. By eliminating the requirement of a foreign-power link for FISA warrants in such cases, S. 113 would allow U.S. intelligence agencies to monitor foreign terrorists who, though not affiliated with a group or government, pose a serious threat to the people of the United States. In light of the significant risk of devastating attacks that can be carried out by non-United States persons acting alone, individual terrorists must be monitored and stopped, regardless of whether they operate in coordination with other individuals or organizations," S.Rept. 108-40 at 2.

What Does Not Expire. Section 6001 explicitly embraces the sunset exception found in section 224(b). Thus, the amendment in section 6001 continues to apply after December 31, 2005 with respect to any particular foreign intelligence investigation begun prior to that date.

Considerations. At first blush, there might be some question of whether a provision, that declares that agents of a foreign power need not be agents of a foreign power, is sufficient to come within *Keith* case reservations concerning the fourth amendment's application in terrorism cases.[56] The multi-national definition of "international terrorism" and the limitation of the section's amendment to foreign nationals may suffice, but the question seems to have troubled some, but not all, of the witnesses who testified regarding similar legislation in the 107th Congress.[57] Some Members of the Senate Judiciary Committee also suggested that section's rationale might have to be reenforced if it is to be reauthorized.[58]

---

[56] "We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents," *United States v. United States District Court*, 407 U.S. 297, 321-22 (1972).

[57] *S. 2586 and S. 2659, Amendments to the Foreign Intelligence Surveillance Act: Hearing Before the Senate Select Comm. on Intelligence*, 107th Cong., 2d Sess. (2002), *compare*, statement of Mr. James A. Baker, United States Department of Justice Counsel for Intelligence Policy, at 24 ("The Department has concluded that S. 2586 is constitutional"), *with*, statement of Mr. Jerry Berman, Executive Director of the Center for Democracy and Technology, at 41 ("Both [S. 2586 and S. 2659] create grounds for serious constitutional challenges by defendants in criminal cases if information collected under these warrants are used as evidence in criminal prosecutions"). S.Rept. 108-40 at 98-102 reprints a more extensive explanation of the Justice Department's view of the constitutionality of S. 2586.

[58] S.Rept. 108-40 at 11-2 (additional views of Sens. Leahy and Feingold ("In many ways, S. 113 seems to be a legislative change in search of a rationale. First, we were told that this amendment to FISA would have allowed the FBI to obtain a warrant before 9-11 to search the computer and belongings of Zacarias Moussaoui. Then, after it became clear ... that the FBI had all the evidence it needed to procure such a warrant ... the rationale changed. Next, we were told that the bill was necessary to conduct surveillance of 'lone wolf terrorists,' who purportedly operate in isolation. Next, after it became clear that few, if any, international terrorists work alone and that existing criminal tools such as Title III were

Summary. Section 6001 amends the FISA definition of "agent of a foreign power" to include a foreign national who is preparing for or engaging in international terrorism thereby excusing the need to show that the illicit activity is being conducted at the behest or benefit of a foreign power – as long as the target is not an American (not a U.S. person).

- Although Justice Department believes the section is constitutional, there might be some question of whether defining an agent of a foreign power as one who need not be an agent of foreign power comes within *Keith* reservations for agents of a foreign power.

USA PATRIOT Act Sections of Title II That Do Not Expire

Subsection 224(a) cites several sections and subsections of Title II that are not subject to its declaration of sunset. They are:

- section 203(a)(authority to share grand jury information) (permitting the disclosure of matters occurring before a federal grand jury — that involve foreign intelligence or counterintelligence or foreign intelligence information — to federal law enforcement, intelligence, protective, immigration, national defense, or national security officials), F.R.Crim.P. 6(e)(3)(D);

- section 203(c)(procedures) (directing the Attorney General to establish procedures for the disclosures authorized in section 203(a)[grand jury matters] and 203(b)[relating to similar disclosure of information secured through the execution of a court order authorizing the interception of wire, oral or electronic communications for law enforcement purposes] that identify a "United States person"), 18 U.S.C. 2517 note;

- section 205 (employment of translators by the Federal Bureau of Investigation) (authorizing the Federal Bureau of Investigation (FBI) to expedite the hiring of translators to support counterterrorism investigations and operations), 28 U.S.C. 532 note;

- section 208 (designation of judges) (authorizing the expansion of the FISA court from 7 to 11 judges and insisting that at least 3 of the judges reside within 20 miles of the District of Columbia), 50 U.S.C. 1803;

---

sufficient to handle those rare cases, we were told that the measure was necessary because it was hard to prove the connection between terrorists. Now, in this report, the implication is revived that the FBI's pre-9/11 failures were due in large part to problems with the law.... It appears, however, that the search for a rationale to support this bill – and one that can be put forth without meaningful oversight of FISA's actual implementation – continues in full force. When the sunset on this measure arrives we will need stronger rationales than this to justify its extension").

- section 210 (scope of subpoenas for records of electronic communications) (expands the authority for subpoenas directing communications service providers to disclose customer-identifying information to include information concerning customer payment sources (e.g., credit card or bank account), 18 U.S.C. 2703;

- section 211 (clarification of scope) (makes it clear that when cable companies provide Internet or other communications services they are subject to the same law enforcement access procedures that apply to other communications service providers and not to the cable provider procedures that require customer notification when law enforcement access is to be afforded), 47 U.S.C. 551;

- section 213 (authority for delaying notice of the execution of a warrant) (authorizes sneak and peek warrants, i.e., warrants that call for delayed notification of their execution for a reasonable period if notification would have adverse consequences and that only permit the seizure of tangible property when reasonably necessary), 18 U.S.C. 3103a(b);

- section 216 (modification of authorities relating to the use of pen registers and trap and trace devices) ((1) modifies the pen register/trap and trace device procedure — the procedure for court orders authorizing law enforcement installation and use of pen registers or trap and trace devices (essentially surreptitious caller id devices that identify only the source and destination of telephone calls) — to apply to electronic communications (e.g., e-mail addresses and Internet URL's); and (2) permits execution of the orders anywhere within the United States, rather than only in the judicial district in which the order is issued), 18 U.S.C. 3121, 3123;

- section 219 (single-jurisdiction search warrants for terrorism) (amends the Federal Rules of Criminal Procedure to permit magistrates in terrorism cases to issue search and arrest warrants to be executed outside of the judicial district in which they are sitting), F.R.Crim.P. 41(b)(3);

- section 221 (trade sanctions) (makes it clear that the Trade Sanctions Reform and Export Enhancement Act does not limit the application of criminal and civil sanctions available for violation of various anti-terrorism provisions), 22 U.S.C. 7210; and

- section 222 (assistance to law enforcement agencies) (confirms that those who help law enforcement authorities execute an order approving the installation and use of trap and trace devices or pen registers are entitled to reasonable reimbursement and that nothing in the act is intended to impose technical obligations or requirements upon them), 18 U.S.C. 3124 note.

Table 1. Expiring USA PATRIOT Act Sections and Subsections

Section	Description	Observation
201 (18 U.S.C. 2516(1)(q))	Adds to the wiretap predicate offense list: 18 U.S.C. 229 (chemical weapons), 2332 (crimes of violence against Americans overseas), 2332a (weapons of mass destruction), 2332b (multinational terrorism), 2332d (financial transactions with terrorist countries), 2339A (supporting terrorists), 2339B (supporting terrorist organizations)	P.L. 107-197, §301(a), 116 Stat. 728 (2002) adds new crimes (18 U.S.C. 2332f (bombing public places), 2339C (financing terrorism)) to the expiring portion of the wiretap predicate list, 18 U.S.C. 2516(1)(q)
202 (18 U.S.C. 2516(1)(c))	Adds to the wiretap predicate offense list: 18 U.S.C. 1030 (computer fraud & abuse)	What does "potential offense" mean for this and other sections of the act? A suspected crime? Or conduct that may blossom into a crime? (E.g., computer trespass before 12/31/05 for purposes launching a denial of service attack thereafter?) Or both?
203(b)(18 U.S.C. 2517(6))	Authorizes disclosure of foreign intelligence, counterintelligence, and foreign intelligence information - gathered thru a Title III court ordered wiretap- to law enforcement, intelligence, protective, immigration, national defense, and national security officials	Disclosure to law enforcement officials is authorized under a permanent subsection, 18 U.S.C. 2517(1); P.L.107-296, §896, 116 Stat. 2257 (2002) permanently authorizes disclosure to foreign law enforcement officials, and in cases of counterintelligence, international terrorism, or clandestine intelligence to federal, state, and/or foreign officials, 18 U.S.C. 2517 (7), (8)
203(d)(50 U.S.C. 403-5d)	Other provisions of law notwithstanding, authorizes disclosure of foreign intelligence, counterintelligence, and foreign intelligence information -gathered in a criminal investigation - to law enforcement, intelligence, protective, immigration, national defense, and national security officials	P.L. 107-296, §897(a), 116 Stat. 2257 (2002), amends the temporary provisions of §203(d) to permit disclosure when consistent with the needs to protect sources and methods and sensitive law enforcement information; the amendment expires with its host
204 (18 U.S.C. 2511(2)(f))	Makes it clear that the general pen register/trap & trace device proscriptions do not bar foreign intelligence gathering involving foreign communications systems.	Amendment seems purely technical.

Section	Description	Observation
206 (50 U.S.C. 1805(c)(2)(B))	Authorizes directives in FISA surveillance orders commanding the assistance of individuals not specifically identified in the order (where the target has taken steps to prevent the identification of specific individuals)("roving surveillance")	Title III affords similar authority for law enforcement purposes in a permanent section, 18 U.S.C. 2518(4)
207 (50 U.S.C. 1805(e), 1824(d))	Extends the permissible duration of FISA surveillance and physical search orders directed against agents of a foreign power to 120 days and permits extensions at intervals of up to one year (up from 90 days (surveillance) & 45 days (searches) for both original orders and extensions)	The expiring section also temporarily extends the general maximum duration of FISA physical search orders from 45 to 90 days
209 (18 U.S.C. 2709, 2510(1),(14))	Makes it clear that the law enforcement access to voice mail requires only a search warrant	At least one court had held that seizure of voice mail required a Title III court order, *U.S. v. Smith*, 155 F.3d 1051 (9th Cir. 1998); except while being sent, e-mail can be seized pursuant to a search warrant, 18 U.S.C. 2703
212 (18 U.S.C. 2702, 2703)	Permits communications service providers to disclose either customer records or the content of customer communications in an emergency situation involving the immediate danger of serious bodily injury	P.L. 107-296, §225(d), 116 Stat. 2157 (2002) repeals the emergency content disclosure provision and replaces it with broader, permanent provision, 18 U.S.C. 2702(b)(7); emergency record disclosure authority expires on 12/31/05
214 (50 U.S.C. 1842, 1843)	Permits the use of FISA pen register/trap & trace device orders with respect to electronic communications (e-mail address, URL identification but not content) under procedure previous limited to wire communications (telephone number of source and addressee); eliminates the requirement that the communication either be that of terrorists or spies or related to their criminal activities	The expiring section also declares, with respect to FISA pen register/trap & trace device orders or the use of such devices in FISA emergency situations, that U.S. persons may not be targeted based solely on their 1st Amendment protected activities

Section	Description	Observation
215 (50 U.S.C. 1861, 1862)	Authorizes FISA court orders for FBI access to tangible items in investigations to protect against terrorism or spying (or per P.L. 107-108, §314(a)(6), 15 Stat. 1402 (2001) to obtain foreign intelligence information not concerning a U.S. person)	Language revived upon sunset of §215 authorizes FISA court orders in foreign intelligence information or terrorist investigations for FBI access to business records relating to public transportation, lodging, vehicle rental, or storage rental upon an assertion of the presence of specific and articulable facts giving reason to believe that the records related to a foreign power or agent of foreign power; P.L. 108-177, §374, 117 Stat. 2628 (2003) expands the Right to Financial Privacy Act's national security letter provision to allow access - in terrorism or spy investigations - to business records held by banks, credit card companies, car dealers, real estate agencies, stock brokers, jewelers, casinos and certain other business that may be party to large cash transactions, 12 U.S.C. 3414
217 (18 U.S.C. 2511(2)(i), 2510(21))	Authorizes the interception of communications to and from a trespasser within a protected computer	Does the sunset exception for a "potential" crime apply to authority under §217 with respect to trespass before but a communication after 12/31/05 relating to a denial of service attack after sunset?
218 (50 U.S.C. 1804(a)(7)(B), 1823(a)(7)(B))	Permits FISA surveillance or search orders based on a certification that foreign intelligence gathering provides a "significant" reason for seeking the order; earlier language (revived at sunset) referred to "the" reason and was one basis for the early conclusion that FISA investigations and any related criminal investigation should be sequential rather than cooperative	*In re Sealed Case*, 310 F.3d 717 (F.I.S.Ct.Rev. 2002); the Justice Dept. study cited there; and permanent FISA amendments in the USA PATRIOT Act (50 U.S.C. 1806(k), 1825(k)) suggest that perhaps the earlier intelligence/law enforcement wall of separation will/need not be reconstructed after 12/31/05
220 (18 U.S.C. 2703, 3127)	Authorizes service anywhere in the world of a court order granting law enforcement access to the content of voice mail and e-mail communications (and/or related records) held by service providers ; prior to §220 such orders had to be issued in the place where they were to be executed	Section 219, which does not sunset, allows federal magistrates in international and domestic terrorism cases to issue search or arrest warrants that may be executed anywhere in the world, F.R.Crim.P. 41(b)(3)

Section	Description	Observation
223 (18 U.S.C. 2520(f),(g), 2707(d),(g), 2712)	Creates a cause of action against the U.S. for willful violations of Title III (18 U.S.C. ch.119) or of FISA; makes it clear that the improper disclosure of information gathered in a court-ordered wiretaps, or use of a pen register or trap & trace device, or access to wire or electronic communications (e.g., e-mail, voice mail) is unlawful; confirms the authority of agency heads to take disciplinary action based on willful/intentional privacy violations	There may be some question whether any cause of action pending or unfiled dies on 12/31/05
225 (50 U.S.C. 1805(h)	Provides immunity for those who aid in the execution of FISA surveillance or search order or in the performance of an emergency FISA wiretap or search	Civil liability for FISA violations under permanent provisions is predicated upon intentional, unauthorized violation of FISA (50 U.S.C. 1810, 1809, 1828, 1827)