Order Code RL32186

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

Updated June 10, 2004

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) relating to enhanced foreign intelligence and law enforcement surveillance authority expire on December 31, 2005. Thereafter, the authority remains in effect only as it relates to foreign intelligence investigations begun before sunset or to offenses or potential offense begun or occurring before that date. There may be some disagreement of whether a "potential offense" is a suspected crime, an incomplete crime, or both.

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 attached 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).

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).

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 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 USA PATRIOT 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)?

Temporary Sections of Title II

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).

Subsection 224(b) states that, "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. Thus it would seem 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. But what is a "potential offense" in this context?

It may mean a suspected offense. In some instances, like murder or bank robbery, there is little doubt that a crime has been committed and the investigation is concerned with who committed it and how. In other instances, such as fraud or material support of a terrorist organization, the investigation may be concerned with whether a crime has occurred at all. The term "potential offense" may have been added out of an abundance of concern that in phrasing the exception so that a criminal investigation need not predate sunset (unlike foreign intelligence investigations) the exception would be limited to the type of crimes whose commission is generally known with certainty before an investigation begins.

Yet 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 or the unfulfilled or the undeveloped or unawakened possibility rather than the suspect or uncertain.[2] On the other hand, there is redundancy in construing the term "potential offense" to mean an inchoate

---

[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").

[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).

offense or an incomplete offense or conduct with some but not all of the elements needed for a crime. Such crimes are already covered as crimes that "began" before December 31, 2005.

A related amendment, enacted after the Act, raises additional questions. Section 201 adds to the wiretap predicate offense list using these words, "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'."

Public Law 107-197 (Implementation of the International Convention for the Suppression of Terrorist Bombings), however, 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) expires 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).

The language of the statute may indicate that the P.L. 107-197 amendments expire with the rest of subsection 2516(1)(q), but 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.Rep.No. 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.[3]

---

[3] *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

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 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).

The authority for disclosure under subsections 203(b) or 203(d) 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

---

it says there. When the words of a statute are unambiguous, then, this first canon is also the last: judicial inquiry is complete").

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 disclosures 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 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 of official purposes of information gathered from lawful interceptions; (B) the wiretap law elsewhere authorizes disclosure of wiretap information to law enforcement officers, 18 U.S.C. 2517(1); and (C) the subsequently-passed Homeland Security Act authorizes disclosure, in separate 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)).[4]

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 USA PATRIOT Act subsection on December 31, 2005, it embeds the amendment in subsection 203(d) thereby suggesting the amendment is

---

[4] "(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).

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).[5]

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 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).[6]

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.

---

[5] "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).

[6] 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.Rep.No. 107-307 at 55 (2001).

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."[7] The law enforcement wiretap statute has a similar provision for law enforcement orders, 18 U.S.C. 2518(4).

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.

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 1 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 1 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 1 year, 50 U.S.C. 1824(d).

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.

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 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.

The authority under section 209 terminates on December 31, 2005 except for investigations relating to offenses or potential offenses begun or occurring before then. As earlier indicated the precise reach of the "potential offense" exception is uncertain. The provisions of section 209 have not been substantively amended.

---

[7] *Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the House Comm. on the Judiciary*, 107th Cong., 1st Sess. 56 (2001); H.Rep.No. 107-307 at 60.

Section 212 (emergency disclosure of electronic surveillance).

Section 212 permits communications service providers to disclose either customer records or the content of their customers' communications in any emergency situation that involves an immediate danger of physical injury, P.L. 107-56, §212(a)(1)(D), 115 Stat. 284-85 (2001). The Homeland Security Act repeals 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 says 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 free standing emergency content disclosure provision which replaced its section 212 predecessor remains in effect.

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 to acquire information relevant to a foreign intelligence or international terrorism investigation and upon the additional certification that the telephone communications monitored would likely to 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). 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).

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.

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).[8]

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).

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 or the consent of one of the participants in the conversation, 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).

---

[8] 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).

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.

Section 218 (foreign intelligence information).

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 by approving applications where the gathering of foreign intelligence information need be 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).

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 314 of the Act adds language to the FISA wiretap and physical search schemes (which does not sunset) 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).[9] 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.[10] There

---

[9] "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 an 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. 1806(k). The language of subsection 1825(k) is essentially the same.

[10] "[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. . . . The origin of what the government refers to as the false dichotomy between foreign intelligence information that is evidence of foreign intelligence crimes and that which is not appears to have been a Fourth Circuit case decided in 1980. . . .Apparently to avoid running afoul of the primary purpose test used by some courts, the

have been no relevant amendments.

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.). This proved inconvenient and sometimes frustrating where the criminal investigation was conducted in one district and the communications provider was located in another, H.Rep.No. 107-307, at 57.

Section 220 addresses the difficulty by authorizing the court in the district where the crime occurred to issue search warrants 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.

The authority under section 220 terminates on December 31, 2005 except with respect to earlier crimes or potential crimes. Section 219, however, mitigates the impact of section 220's expiration in certain terrorism cases. Section 219 is not subject to the sunset provision. It provides for at least nation-wide, and perhaps

---

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 should 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 with 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 has 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 anticipated that the underlying investigation might well have a criminal as well as foreign counterintelligence objective . . . . In short, even though we agree that the original FISA did not contemplate the false dichotomy, the Patriot Act actually did — which makes it no longer false. The addition of the word 'significant' to section 1804(a)(7)(B) imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes," 310 F.3d at 723, 725, 727, 735 .

world-wide, service of federal search and arrest warrants in cases of international or domestic terrorism as defined in 18 U.S.C. 2331.[11]

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.

Although the federal wiretap statute outlaws use or disclosure of *unlawfull*y 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.[12]

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

---

[11] "[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).

[12] 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).

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.

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.

Under some circumstances the demise of a cause of action deprives the courts of subject matter jurisdiction. Long standing 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."[13]

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.[14]

---

[13] *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).

[14] *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).

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 the 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). Section 225 provides immunity for those who assist in the execution of a FISA wiretap order or of a FISA physical search order or in case of an emergency FISA wiretap or search, 50 U.S.C. 1805(h).

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 the 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.

Unimpaired Sections of Title II

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;

• 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 1 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 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 the 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)