Order Code RS21704
Updated June 10, 2004

USA PATRIOT Act Sunset: A Sketch

Charles Doyle
Senior Specialist
American Law Division

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 offenses begun or occurring before that date. 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 sunset provision suggests two types of interpretative challenges: (1) what is a potential offense? (2) what is the impact of amendments enacted after the Act? This report is an abridged version – without footnotes or chart – of CRS Report RL32186, *USA PATRIOT Act Sunset: Provisions That Expire on December 31, 2005*.

Temporary Sections of Title II – Sections 201 and 202: 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). Sections 201 and 202 temporarily add crimes to this predicate offense list. Section 202 places felonious computer fraud and abuse on the list; section 201 contributes crimes relating to chemical weapons, violence committed against Americans overseas, weapons of mass destruction, multinational terrorism, financial transactions with a country designated a sponsor of terrorism, providing material support to a terrorist, and providing material support to a terrorist organization.

Under the 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 that begins or occurs before December 31, 2005. But what is a "potential offense" in this context? It may mean a suspected offense or incomplete offense. The word "potential" usually contemplates the incomplete or the unfulfilled or the undeveloped or unawakened possibility rather than the suspect or uncertain. On the other hand, there is redundancy in construing the term "potential offense" to mean an inchoate offense or an incomplete offense or conduct with some but not all of the elements needed for a crime. The exception already covered them as crimes that "began" before December 31, 2005.

P.L. 107-197 (Implementation of the International Convention for the Suppression of Terrorist Bombings), perhaps inadvertently, adds the new crimes it establishes (financing terrorism and bombing public buildings and places) to the temporary subsection that section 201 creates.

Subsections 203(b) and 203(d): 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. 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. 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 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. The post-December 31, 2005 exceptions for law enforcement and foreign intelligence investigations might be thought to limit the continued authority of subsections 203(b) and 203(d) to disclosures to law enforcement and intelligence officials but 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 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; 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. 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 intended to terminate with the rest of subsection 203(d).

Section 204: Section 204 is essentially a technical amendment. Prior wiretap law makes it clear that the general prohibitions against wiretapping and against the acquisition of communications records and stored electronic communications do not preclude foreign intelligence gathering activities involving foreign communications systems. Section 204 amends the provision to add that the general prohibition against the use of pen registers or trap and trace devices is likewise no impediment to such activities.

Section 206: Section 206 authorizes assistance for the installation and use of multi-point FISA wiretaps. 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. 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." The law enforcement wiretap statute has a similar provision for law enforcement orders. 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: 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. 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). 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. 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: At one time, at least some courts felt that authorities needed a wiretap order rather than a search warrant to seize voice mail. Section 209 treats voice mail like e-mail, subject to seizure under a search warrant rather than a more demanding wiretap order law.

The authority under section 209 terminates 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.

Section 212: Section 212 permits communications service providers to disclose either customer records or the content of their customers' communications in any emergency situation. The Homeland Security Act repeals section 212's provision governing *content* disclosure in emergency situations and recasts it as a separate provision, but says nothing of the emergency disclosure of customer *records*. 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: 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.

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). It drops the requirement that the communications be those of international terrorists or spies or be related to their activities. 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. It adds this same caveat with respect to emergency FISA pen register or trap and trace device use. 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 occur since passage of the Act.

Section 215: 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. 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." 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.

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 intelligence authorization act changes in the law governing "national security letters" that provide access to a wide range of business records than available under FISA after sunset.

Section 217: 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. 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. 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.

Section 218: 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. 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.

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. 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. There have been no relevant amendments.

Section 220: 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. 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. This proved inconvenient and sometimes frustrating where the criminal investigation was conducted in one district and the communications provider was located in another. 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).

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 world-wide, service of federal search and arrest warrants in cases of international or domestic terrorism.

Section 223: Unrelated to section 223, federal law imposes criminal penalties for illegal wiretapping, unlawful access to store communications (e.g., e-mail or voice mail), or illegally using a pen register or trap and trace device. Except with respect to pen registers and trap and trace devices, the same misconduct also triggers civil liability. There is a comparable set of provisions imposing criminal and civil liability for FISA surveillance and physical search violations. Although the federal wiretap statute outlaws use or disclosure of *unlawfull*y intercepted communications, and describes narrow circumstances under which communications intercepted under a court order may be used or disclosed, without more, it does not expose to civil or criminal liability those who disclose or use communications *lawfully* intercepted under a court order.

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. It also imposes civil liability for any willful use or disclosure of information beyond that authorized by those two statutory schemes. 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.

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 that pending suits survive but none may be filed thereafter, or that regardless of when they are filed any cause of action will only survive with respect to matters occurring prior to that date.

Section 225: Federal wiretap law immunizes those who assist in the execution of a law enforcement interception order, FISA supplies the similar immunity for those who assist in the execution of a FISA pen register or trap and trace device order. 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 the case of an emergency FISA wiretap or search.

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 it 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); 203(c)(procedures for the wiretap and grand jury disclosures that identify a "United States person"); 205 (employment of translators by the Federal Bureau of Investigation); 208 (adds 3 judges to the FISA court); 210 (access payment sources in communications provider records); 211 (cable companies as communications service providers); 213 (sneak and peek warrants); 216 (law enforcement of the use of pen registers and trap and trace devices); 219 (single-jurisdiction search warrants for terrorism); 221 (trade sanctions); and 222 (pen register and trap and trace device assistance to law enforcement agencies).