Order Code RS21704
Updated June 29, 2005

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) 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, unless they are extended. 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).

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*.

Introduction

Sunset comes to a handful of communications-related sections of the USA PATRIOT Act and the Intelligence Reform and Terrorism Prevention Act on December 31, 2005. The authority of the expiring sections 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. Thereafter, the law reverts to its previous form unless it has been amended in the interim or subsequently renewed. 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."

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 the 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. With the approval of senior Justice Department 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. 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. When the orders expire, those whose communications have been intercepted must be notified.

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.

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 the installation and use of a pen register or a trap and trace device is less demanding still.

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): 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 sunset exception (224(b)) is unclear. The authority has apparently been used sparingly and in cases where other grounds for wiretapping authority may have existed. The Justice Department argues that the electronic surveillance authority should be available for the full range of terrorism-related crimes.

Subsections 203(b) (authority to share electronic, wire, and oral interception information) and 203(d) (general authority to share foreign intelligence information): 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. 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. Justice Department officials contend that to allow sections 203(b) and 203(d) to expire would send the wrong signal about the importance of information sharing among investigators.

Section 204 (clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications): Section 204 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): 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 may suggest that compatibility might have been achieved by expanding wiretap order requirements to cover unopened e-mail. Critics might also 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): 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.

Section 217 (interception of computer trespasser communications): 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." Critics might argue that 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.

Section 220 (nationwide service of search warrants for electronic evidence): Section 220 authorizes nation-wide execution of search warrants and court orders for customer communications records and the content of stored customer communications. Search warrants must ordinarily be executed in the judicial district in which they are 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 within their home federal district they must challenge in whatever district throughout the country the 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): 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 and the Attorney General has recommended that it be made permanent.

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 Title III; there is a rough comparability between FISA physical search authority and search warrant authority in a law enforcement context; and there is a rough comparability between FISA trap and trace or pen register orders and their law enforcement counterparts. 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 a predicate offense has, is or will occur; relevant 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 an 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 permits roving FISA surveillance orders; orders need not specifically identify individuals ordered to assist when targets take actions to thwart identification specific individuals or locations. Comparable authority has existed under Title III for some time. Critics claim the provision is too sweeping, perhaps unconstitutionally 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*.

Section 207 (duration of FISA surveillance of non-United States persons who are agents of a foreign power): 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 that more not less judicial supervision is called for.

Section 214 (pen register and trap and trace authority under FISA): 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). The change is comparable in some respects to a similar enlargement for law enforcement in §216 which does not expire. 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 a court order nonetheless and is First Amendment sensitive. Critics may 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): Section 215 provides access to tangible items under FISA by authorizing ex parte FISA court orders in foreign intelligence (as amended), international terrorism, and clandestine intelligence cases. It reverts at sunset to vehicle rental, transportation, storage rental, and housing accommodation business records that pertaining to foreign power or agent. Other legislation expanding the definition of financial institution for national security letter purposes 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 used sparingly and never to acquire library, bookstores, medical or gun sale records, although officials argue it would be mistake to shield from investigation the records of terrorist use of these services. On the other hand, critics might argue that 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")): 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. The section makes it clear that a "wall" between FBI criminal and intelligence investigators is unnecessary. Section 504 of the act (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* 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, some say, is like trying to do one jigsaw puzzle on two separate tables. Supporters might contend that the wall prevented effective communication and cooperation in terrorism cases; removal has been beneficial.

Section 223 (civil liability for certain unauthorized disclosures): Section 223 is discussed above.

Section 225 (immunity for compliance with FISA wiretap): Section 225 establishes immunity for assistance in the execution of a FISA surveillance order, and perhaps for compliance with any FISA order. It encourages cooperation and discourages court challenges.

Section 6001 of P.L. 108-458 (individual terrorists as agents of foreign powers) 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 the 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 a foreign power comes within the *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); 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).