HR 3199 - Sunset Provisions

Below is a summary of each of the sixteen sections set to expire this year pursuant to section 224 (the sunset does not apply to on-going investigations), an explanation of how each has been used, and any concerns related to such authorities:

Sec. 201 - Authority to intercept wire, oral, and electronic communications relating to terrorism

This section adds terrorism offenses to the list of predicates for title III wiretaps. Title III is used for criminal investigations.

Sec. 202 - Authority to intercept wire, oral, and electronic communications relating to computer fraud and abuse offenses

This section adds computer fraud and abuse offenses as predicates for title III wiretaps.

Sec. 203(b) and (d)- Authority to share electronic, wire, and oral interception information; Authority to share foreign intelligence information.

Section (b) section allows the government to share information from criminal wiretaps and electronic surveillance with federal law enforcement, immigration, and national security personnel as long as notice is given to the court after the disclosure. The recipient can only use information in the conduct of their duties subject to disclosure limitations in current law.

Section (d) allows the FBI to share intelligence information with other federal law enforcement, immigration, and national security personnel. The Attorney General must establish procedures for hte release of this information in the case of a U.S. person.

It is important to note that PATRIOT Act has already created permanent authorization for information sharing between the criminal and intelligence agencies: Section 905 requires the Attorney General to provide all "foreign intelligence"related information (not just terror related information) to the Director of National intelligence that is uncovered in the process of a criminal investigation, and section 504 allows FISA information to be given to the criminal division.[1]

In other words, Section 203 is not about letting the criminal and intelligence community communicate, but farming out information to other divisions of the government to do with as they please. One scholar has noted, "It does not limit such sharing to officials with responsibility for terrorism matters, nor are there any safeguards regarding the subsequent use or dissemination of such information by such officials (so long as the use is within the official duties of the recipient). It allows the sharing of all information that is in any way related to any American's contacts with or activities involving any foreign government, group, or individual."[2]

---

[1]Kate Martin, "Why Sections 203 and 905 Should be Modified," American Bar Association's Patriot Debates, available at http://www.patriotdebates.com/203-2#opening.

[2]*Id.*

There are also concerns that federal investigators are using grand juries to collect data that would not have probable cause to collect through criminal or FISA warrants. However, due to secrecy requirements, grand jury members cannot disclose their work, and the Justice Department has not disclosed what information it has received from grand juries. Our only record is our 2002 oversight questions, in which the Department claimed that:

> Disclosure of information obtained through grand juries convened under federal law as part of criminal investigations of matters involving foreign intelligence has been made on approximately 40 occasions. Some of this information sharing may have occurred prior to passage of the USA PATRIOT Act.[3]

It also noted that post-sharing notice given to the supervising court was filed in at least 38 districts.[4]

Sec. 204 - Clarification of intelligence exceptions from limitations on interception and disclosure of wire, oral, and electronic communications

This section carves out foreign intelligence surveillance operations from the Electronic Communications Privacy Act, which imposes limits on the placement of wiretaps.

Sec. 206 - Roving surveillance authority under the Foreign Intelligence Surveillance Act

This section allows the FBI to use roving wiretaps under FISA. This means that the FBI can use one court order to tap any phone they believe a foreign agent would use, instead of getting separate court orders for each phone. The government not need name the target.

No one disagrees that roving wiretaps are important. Indeed, they have been useful in criminal investigations since 1986. However FISA roving wiretaps go far beyond criminal wiretaps in several ways. First, criminal roving wiretaps require the law enforcement agent to "ascertain" that the target will actually using a device – FISA allows for blanket tapping, for example all the payphones in the target's neighborhood, or all of his relatives, without showing that the target will actually use the device.[5] Second, agents seeking a roving wiretap need not even identify a specific suspect and instead get "John Doe" warrants.[6] These two differences add up to roving "John Doe" warrants that require so little suspicion that they can be easily abused.

---

[3]Oversight answers, Submitted by Daniel J. Bryant, Assistant Attorney General, July 26, 2002, on file with the House Judiciary Committee.

[4]*Id.*

[5]John Podesta, "USA PATRIOT Act: The Good, the Bad and the Sunset," Human Rights Magazine, Section of Individual Rights and Responsibilities, American Bar Association, Winter 2002.

[6]"Let the Sun Set on PATRIOT," Electronic Frontier Foundation, available at www.eff.org.

The number of times this authority has been used and in what manner was classified[7] until yesterday, when the Attorney General admitted to using it 49 times.

Sec. 207 - Duration of FISA surveillance of non-United States persons who are agents of a foreign power

This section lets the FBI obtain FISA search and surveillance orders for longer initial periods of time than they could have prior to the PATRIOT Act. Before the Act, surveillance orders needed to be renewed after ninety days and search orders needed to be renewed after forty-five days. Under current law, the orders can be issued for periods of up to one year. Furthermore, a FISA search order can be executed for ninety days after issuance (the time limit was forty-five days prior to the PATRIOT Act). Some argue that the FBI does not need this authority because, prior to the PATRIOT Act, it could have sought extensions of FISA orders from the FISA court. The Justice Department claims that this provision has saved 60,000 attorney hours.

Sec. 209 - Seizure of voice mail messages pursuant to warrants

This section provides that the FBI can access voice mails the same way it accesses e-mails and authorizes nationwide service with a single search warrant.

Sec. 212 - Emergency disclosure of electronic communications to protect life and limb

This section permits ISP's to disclose to the government, without penalty, customer e-mails if they think there is a danger of death or serious injury. It also allows law enforcement to compel disclosure to third parties using a court order or search warrant. According to the Department's May 13, 2003 letter, section 212 has been used to trace a kidnapper's communications and to investigate a bomb threat against a school.[8] The Department website also states an ISP used section 212 to disclose that certain unknown persons had threatened to kill executives in another country unless a ransom was paid.

Because section 225 of the Homeland Security Act of 2002[9] independently created a similar, but broader provision, whether this section of the PATRIOT Act sunsets is moot. By all accounts, the new provision is far worse as it, "lower[s] the relevant standard from 'reasonable belief' of a life-threatening emergency to a 'good faith belief', allow[s] communications

---

[7]Oversight answers, submitted by Daniel J. Bryant, Assistant Attorney General, July 26, 2002, on file with the House Judiciary Committee; The PATRIOT Act: Myth vs. Reality, U.S. Department of Justice, September 2003.

[8]*May 13, 2003 Letter* at 22-23.

[9]Pub. L. No. 107-296 (2002).

providers to use the emergency exception to disclose data to any government entity, not just law enforcement, and drop[s] the requirement that the threat to life or limb not be immediate."[10]

Sec. 214 - Pen register and trap and trace authority under FISA

This section made it easier for the FBI to get a pen register or trap-and-trace under FISA.[11] The FBI needs to prove the order is needed to obtain foreign intelligence information not concerning a U.S. person or to protect against international terrorism or clandestine intelligence activities. Prior to the PATRIOT Act, the FBI needed to establish that the telephone line in question had been used or was about to be used in connection with terrorism or a crime; this requirement was deleted.

As the majority and the DOJ points out, search warrants are not required for pen register and trap and trace activities under the criminal law.[12] However, FISA pen register/trap and trace orders aren't necessarily targeted at an individual suspected of any wrongdoing. Before section 214, the agents had to prove that the target was an agent of a foreign power; now, they need only prove that the information is related to a terror or intelligence investigation. This extremely broad qualification of a FISA pen register/trap and trace order has led many groups to oppose it.[13]

Use of this section is classified, but was submitted to the Judiciary Committee in May of 2003 under security restrictions and is available to members and staff with the proper clearance.

Sec. 215 - Access to records and other items under the Foreign Intelligence Surveillance Act

This section expanded the FBI's ability to obtain business records under FISA. Before the Act, the government could seek records only from transportation companies; now, it can seek "any tangible thing" from any business. To obtain such records, the FBI Director (or his designee) must seek an order from the Foreign Intelligence Surveillance Court and specify that the records are sought for foreign intelligence information not concerning a U.S. person or are sought to protect against international terrorism or intelligence gathering. Upon receipt of such a request, the court must grant the order. Recipients are prohibited from disclosing to anyone but their attorneys that they have received section 215 requests.

---

[10]"Let the Sun Set on PATRIOT," Electronic Frontier Foundation, available at www.eff.org.

[11]A pen register is used to record the phone numbers that are dialed from a target phone. A trap-and-trace is used to record the phone numbers of the incoming calls to a target phone.

[12]Smith v. Maryland, 442 U.S. 735, 744 (1979) (using the phone involved a third party – the phone company – and therefore destroyed any expectation of privacy the target had).

[13]See, for example, Electronic Privacy Information Center "The USA PATRIOT Act," at www.epic.org/privacy/terrorism/usapatriot/.

On behalf of various Muslim community organization, the ACLU has filed a lawsuit in a federal court in Michigan challenging the constitutionality of this provision. The lawsuit is pending; at issue are the government's motion to dismiss and the plaintiff's motion to exclude secret evidence offered by the Department.[14]

On September 18, 2003, the Attorney General declassified a memorandum he wrote to FBI Director Robert Mueller showing that section 215 had never been used. Yesterday, the Attorney General confirmed that this section had been used 35 times. Documents acquired during an ACLU FOIA request reflecting internal FBI policy towards section 215 are available at www.aclu.org/safeandfree/SafeandFree.cfm?ID=15327&c=262.

Because the government could investigate consumers' reading and Internet habits and private records, such as credit card information, medical records, and employment histories, it is possible that the government is stepping over any number of constitutional lines. Again, the majority will argue that it already had access to these sorts of business records. But a federal court found that section 215 implicates new constitutional problems: 1) it applies to any tangible thing, and is no longer limited to business records, and 2) no longer requires "specific and articulable facts giving reason to believe that he person whom the records pertain is a foreign power or an agent of a foreign power," but only that "the records concerned are sought for an authorized investigation."[15] A court has not ruled on the merits on section 215, but is likely that it will be found to violate the First Amendment because it places a prior restrain of free speech and monitors free speech activities of its targets, and to violate the Fourth Amendment because it fails to provide notice to the target.[16]

Sec. 217 - Interception of computer trespasser communications

This section allows persons "acting under color of law" to intercept computer communications if a computer owner authorizes it, and the person acting under color of law is acting pursuant to a lawful investigation.

Sec. 218 - Foreign intelligence information

This section says the FBI needs to aver that a "significant" purpose of a FISA order request is to gather foreign intelligence; before the Act, the FBI needed to show that obtaining foreign intelligence was the "primary purpose" of the order.

---

[14]Muslim Community Association of Ann Arbor v. Gonzales (E.D. Mich.).

[15]ACLU v. Dept. of Justice, 321 F.Supp.2d 24 (D.D.C. 2004) (citing section 215 in its current form, and its original form, Pub. L. No. 105-272 (1998)).

[16]ACLU, Surveillance Under the USA PATRIOT Act, *available at* www.aclu.org/Safeandfree.

The Department has confirmed that "there was no *legal* impediment to introducing in a criminal prosecution evidence obtained through FISA before the USA PATRIOT Act."[17] Instead, the Department says these barriers resulted from "certain court decisions and administrative practice by the Department."[18] Impediments to sharing of information between intelligence and law enforcement investigators were, therefore, almost entirely the result of administrative barriers, not statutory requirements that were eased by the USA PATRIOT Act. This was confirmed by the FISC court of review.[19] Because the Court held that there was no legal "wall" to begin with, there is no reason to believe that letting this section sunset would reimpose the "wall."

Again, it is important to note that PATRIOT Act has already created permanent authorization for information sharing between the criminal and intelligence agencies: Section 905 requires the Attorney General to provide terror related information to the Director of National intelligence that is uncovered in the process of a criminal investigation, and section 504 allows FISA information to be given to the criminal division.[20]

The Justice Department has provided a small number of anecdotal stories of how FISA obtained evidence helped prosecute standard crimes, although it refuses to give a full accounting about how this provision has gone above and beyond sharing already allowed under the law.[21] The Department has also admitting to sending over 4,500 FISA files to the criminal division, although it could not account for how many of those resulted in prosecution.[22]

The effect of letting the status quo continue is that evidence obtained from a FISA warrant under FISA's statutory "probable cause" standard can be given to non-terror criminal prosecutors who are governed by the higher standard of 4th Amendment probable cause. In fact, the lower standard FISA warrant can be sought for criminal prosecution purposes, as long as terrorism or national intelligence is some small part of the reason. The long standing policy of not letting criminal prosecutors direct intelligence investigations is gone.

---

[17]*May 13, 2003* Letter at 12 (emphasis in original).

[18]*Id.* at 13.

[19]In re: Sealed Case No. 02-001, 310 F.3d 717 (F.I.S.Ct. Rev. 2002).

[20]Kate Martin, "Why Sections 203 and 905 Should be Modified," American Bar Association's Patriot Debates, available at http://www.patriotdebates.com/203-2#opening.

[21]Oversight answers, submitted by Jamie E. Brown, Acting Assistant Attorney General, May 13, 2003, on file with the House Judciary Committee; Oversight answers, submitted by Daniel J. Bryant, Assistant Attorney General, July 26, 2002, on file with the House Judiciary Committee.

[22]Oversight answers, submitted by Jamie E. Brown, Acting Assistant Attorney General, May 13, 2003, on file with the House Judciary Committee.

Sec. 220 - Nationwide service of search warrants for electronic evidence

This section allows a single court to issue a search warrant for electronic evidence that is valid nationally. According to the Department's May 13, 2003 letter, it has used this authority to track a fugitive and to track a hacker who stole trade secrets from a company and then extorted money from it.[23]

The biggest threat of this section is it allows law enforcement to "forum shop," to go to a more lenient judge in a different jurisdiction that may have little or no nexus to the actual rights of the target. It is also important to note that section 219 already authorizes nationwide search warrants in terror investigations.[24] This section expands it to standard criminal investigations, an intent that Congress probably never had in its rush to approve the PATRIOT Act in the wake of the 9/11 terror attacks.

Sec. 223 - Civil liability for certain unauthorized disclosures

This section included by Rep. Barney Frank to increase civil liability for unauthorized disclosure of pen/trap, wiretap, e-mail, or FISA information. In its May 13, 2003 letter to the Committee, the Department stated there had been no administrative disciplinary proceedings or civil actions under section 223.

Sec. 225 - Immunity for compliance with FISA wiretap

This section immunizes parties who comply with FISA orders.

"Lone Wolves" as Agents of a Foreign Power

The purpose of FISA always has been espionage and terrorism surveillance against foreign governments, foreign groups, or individuals associated with such governments or groups. This change expanded FISA to include any single person who engages in a violent act that (1) transcends national boundaries and (2) is intended to coerce the government or a civilian population.

---

[23] *Id.* at 24.

[24] *Let the Sun Set on PATRIOT*, Electronic Frontier Foundation, available at www.eff.org.