Testimony of

Daniel P. Collins

May 10, 2005

Testimony of Daniel P. Collins
before the Senate Committee on the Judiciary
May 10, 2005

Chairman Specter, Senator Leahy, and Members of the Committee, I am grateful for the opportunity to testify before you today. Three and one-half years ago, the USA PATRIOT Act was signed into law by President Bush with overwhelming support in both Houses of Congress. See Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001). That strong bipartisan consensus reflected the gravity and importance of the chief objective of that legislation, which was set forth right in the title: "providing appropriate tools required to intercept and obstruct terrorism." As the horrific events of September 11 demonstrated, there are few priorities more pressing than detecting and preventing terrorist attacks. It is critical that the men and women whose job it is to protect us have the tools they need to get that job done, and to get it done in a manner that both enhances security and respects liberty. However, as the Committee is well aware, some 16 provisions of Title II of the PATRIOT Act are scheduled to expire on December 31, 2005, absent action by Congress. Id., § 224(a), 115 Stat. at 295. In my view, these 16 provisions should be made permanent. Today, as in 2001, they are "appropriate tools" in the war on terror.

My perspective on these matters is informed by my service over the years in various capacities in the Justice Department. Most recently, I served from June 2001 until September 2003 as an Associate Deputy Attorney General ("ADAG") in the office of Deputy Attorney General Larry Thompson. During the same period, I also served as the Department's Chief Privacy Officer, and in that capacity, I had the responsibility for coordinating the Department's policies on privacy issues. I also served, from 1992 to 1996, as an Assistant United States Attorney in the Criminal Division of the U.S. Attorney's Office for the Central District of California in Los Angeles. And prior to that, I had served from 1989 to 1991 as an Attorney-Advisor in the Office of Legal Counsel in Washington, D.C. I am now back in private practice in Los Angeles, and I emphasize that the views I offer today are solely my own.

Before turning to some of the specific PATRIOT Act provisions that are up for "sunset" review, I think it is useful to outline some of the basic principles that should guide an analysis of these provisions. The overarching question whether a particular surveillance authority is an "appropriate tool" ultimately turns on whether that tool assists in detecting and preventing terrorism, and whether it does so in a manner that preserves and enhances privacy. In making that judgment, it is important not to fall into the fallacy of "zero-sum" thinking, whereby every expansion of government surveillance authority is somehow deemed inherently to represent a loss of privacy. This sort of thinking does not make much sense either from a law enforcement perspective or from a civil liberties perspective. The question instead is whether the conditions placed on the availability and use of a particular tool are sufficient to permit it to be deployed effectively when warranted, but only in a manner that is respectful of privacy and basic civil liberties.

Beyond that very general statement, there is, I think, general agreement on a number of more specific principles that help to inform any judgment about the propriety and adequacy of the conditions placed upon the use of a particular tool. I have previously outlined some of these principles in my prior testimony before this Committee, and I think it is useful to summarize them again here:

? Unwavering fidelity to the Constitution. Privacy is a cherished American right. Among the various ways in which the Constitution protects that right, the Fourth Amendment specifically reaffirms the right of the people to be free from unreasonable searches of their "houses, papers, and effects." Our laws must scrupulously respect the limits established by the Constitution. As many have said, we have to think outside the box, but not outside the Constitution. But while the Constitution sets the minimum, our laws have long properly reflected the judgment that, from a policy perspective, there should be additional statutory protections for privacy. I do not question that judgment.

? Not all privacy interests are the same. Not all privacy interests are of the same magnitude, and it makes no policy sense to act as if they were. For example, some categories of information are more important and more sensitive than others. The fact that the supermarket club could maintain a computerized stockpile of information about my personal buying habits may raise a privacy concern, but it is not on the same level as someone eavesdropping on my

phone conversations or reading my medical records. The nature and severity of the privacy intrusion at issue are certainly important factors to consider.

? Privacy is not always the most important value. It is essential to keep in mind that, while privacy is an important right, it is by no means the only important value. Human society, by its very nature, involves some loss of personal privacy. Competing concerns raised by new technology may also justify particular intrusions on privacy: no one can deny that airport inspections are essential to public safety, regardless of the cost to privacy.

? If it's good enough for fighting the mob, it's good enough for fighting terrorism. Any tool that is already available to fight any other type of crime -- be it racketeering, drug trafficking, child pornography, or health care fraud -- should be available for fighting terrorism. If the judgment has already been made that the tool is appropriate for fighting these other crimes, and that any privacy interests at stake must yield to that effort, then surely the tool should also be available to fight terrorism.

? The law of inertia must not be a principle of privacy policy. It does not make much sense to perpetuate outmoded ways of doing things simply because it has always been done that way. As times and technologies change, the judgments that are reflected in existing statutory rules may need to be re-evaluated.

? The importance of technological neutrality. In applying privacy principles to new and emerging technologies, an important benchmark is the concept of "technological neutrality." The idea is that, just because a transaction is conducted using a new technology, there should not have to be a loss of privacy when compared to similar transactions using older technologies. To use an example, the privacy protection for ordinary email should be roughly equivalent to that of an ordinary postal letter. Conversely, the emergence of new technologies should not provide criminals with new ways to thwart legitimate and legally authorized law enforcement action. Cyberspace must not be permitted to become a "safe haven" for criminal activity. The notion of technological neutrality takes into account both sides of the coin.

With these basic principles in mind, let me explain why I think each of the 16 pertinent sections of the PATRIOT Act properly enhance the abilities of law enforcement in a manner that respects and preserves our freedoms.

(1)-(2) Sections 201 and 202

Title III -- the wiretap statute -- sets forth a number of stringent requirements that must be met before a court may issue an order authorizing a wiretap. One of the requirements is that the investigation must involve an offense that is on Title III's list of offenses that are eligible for wiretapping. 18 U.S.C. § 2516. The Patriot Act modestly expands this list -- which already includes a variety of serious offenses such as money laundering and bank fraud -- to include six terrorism offenses, unlawful possession of chemical weapons, and computer fraud and abuse. Pub. L. No. 107-56, §§ 201, 202, 115 Stat. at 278. In adding these offenses to the list of those eligible to be investigated by wiretapping, the Act leaves unchanged the full panoply of substantive protections provided by Title III. Moreover, the notion that there is a rational and defensible privacy interest in precluding wiretapping to investigate terrorism -- while permitting it to be used to investigate, say, bribery in sports contests -- is very difficult to defend. Sections 201 and 202 are a straightforward application of the principle that law enforcement should have at least the same tools to fight terrorism that it has to fight organized crime.

(3)-(4) Sections 203(b) and 203(d)

These provisions, which authorize certain forms of information sharing between law enforcement officers and intelligence officials, are among the most important in the PATRIOT Act.

Specifically, section 203(b) authorizes the sharing of Title III wiretap information with intelligence and national security officials, subject to several conditions: (1) the information must have been obtained "by any means authorized by this chapter," i.e., in accordance with the strict requirements of Title III; (2) the information to be shared must "include foreign intelligence or counterintelligence" or "foreign intelligence information" as those terms are specifically defined by the relevant statutes; (3) the information may only be used by such official "as necessary in the conduct of that person's official duties"; (4) any such official must also comply with "any limitations on the unauthorized disclosure of such information"; and (5) to the extent the information "identifies a United States person," the disclosure must comply with statutorily mandated guidelines issued by the Attorney General. See Pub. L. No. 107-56, § 203(b), (c), 115 Stat. at 280-81.

Section 203(d) more generally authorizes sharing of information "obtained as part of a criminal investigation," subject to the following restrictions: (1) the information to be shared must comprise " foreign intelligence or counterintelligence" or "foreign intelligence information" as those terms are specifically defined by the relevant statutes; (2) the information may only be used by such official "as necessary in the conduct of that person's official duties"; and (3) any such official must also comply with "any limitations on the unauthorized disclosure of such information." See Pub. L. No. 107-56, § 203(d), 115 Stat. at 281.

As the 9/11 Commission and others have noted, the need for appropriate sharing of information between law enforcement and intelligence officials is absolutely critical to detecting and preventing terrorism. Moreover, the safeguards imposed by section 203(b) and section 203(d) seem properly tailored to ensure that law enforcement

officials will only share information that qualifies as " foreign intelligence or counterintelligence" or "foreign intelligence information" and will do so only subject to appropriate restrictions. It must be emphasized that these modest provisions do not, as some critics have wrongly claimed, put the CIA in the business of "spying on Americans." By definition, all information subject to sharing under sections 203(b) and 203(d) has been obtained by the lawful investigative activities of law enforcement officials either under Title III or "as part of a criminal investigation."

(5) Section 204

Section 204 is a largely technical amendment that clarifies the relationship between the authorities under the criminal statute governing "pen registers" and "trap-and-trace" devices and the authorities under otherwise applicable federal law concerning certain foreign intelligence activities. Pub. L. No. 107-56, § 204, 115 Stat. at 281. I am not aware of any substantial reason why this provision should not be made permanent.

(6) Section 206

Section 206 of the PATRIOT Act addresses the subject of so-called "roving wiretaps" under the Foreign Intelligence Surveillance Act of 1978 ("FISA"). In my view, section 206 strikes an appropriate balance on this subject and should be preserved.

Under the current version of Section 105(c)(1)(B) of FISA, a FISA order authorizing electronic surveillance only needs to specify the nature and location of each such facility or place "if known." 50 U.S.C. § 1805(c)(1)(B). Notably, the addition of the phrase "if known" was not made by the PATRIOT Act, but rather by the Intelligence Authorization Act for Fiscal Year 2002, Pub. L. No. 107-108, § 314(a)(2)(A), 115 Stat. 1394, 1402 (2001); that amendment is therefore not subject to the PATRIOT Act's sunset provision. Although current law thus dispenses with a specification requirement when the exact nature and location of the facilities or places are not known in advance, the existing version of Section 105(a)(3)(B) continues unambiguously to state that an authorizing order may only be issued if, inter alia, "there is probable cause to believe that ... each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(B). Reading these provisions together, it would seem clear that, even when it cannot be specified in advance what are the particular facilities and places that will be surveilled, the Government must nonetheless provide a sufficient description of the categories of facilities and places that will be surveilled (presumably by describing their connection to the target) so as to permit the court to make the finding that remains required by Section 105(a)(3)(B). The pertinent change made by Section 206 of the PATRIOT Act was merely to eliminate the requirement that the authorizing order in all cases specify in advance those third parties (e.g., wire carriers) who were directed to supply assistance in carrying out the order. See Pub. L. No. 107-56, § 206, 115 Stat. at 282 (amending 50 U.S.C. § 1805(c)(2)(B)). Instead, the PATRIOT Act states that, if the court finds that "the actions of the target of the application may have the effect of thwarting the identification of a specified person," the order may require the cooperation of other such persons who have not been specified. Id. This modest change makes perfect sense: the prior third-party-assistance specification requirement had the obvious potential to allow targets to defeat surveillance simply by changing, for example, from one cell phone to another. Indeed, it is hard to see why one would want to allow this specific amendment to sunset: there is no apparent advantage to requiring the Government to go back to the FISA Court merely because the target has shifted from one wire service provider to another.

Against this backdrop, the amendment that would be made by Section 2 of the SAFE Act, S. 737, seems quite significant. Section 2 appears to be clear in saying that, to avoid the advance specification requirement for "facilities and places," it is not enough to have a detailed "description of the target"; one must know "the identity of the target" (emphasis added). What this means is that, even though the Government could describe in great detail a particular agent of a foreign power of whom they are aware, if they can not identify the person, then FISA surveillance must be limited to only those physical facilities that can be specified in advance. Moreover, this would remain true even though the Government could show (as it is required by Section 105(a)(3)(B) to show) that there is probable cause that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used" by the target. The marginal effect of Section 2 would thus appear to be that, even though a "John Doe" foreign agent can be shown regularly to engage in the practice of moving from one disposable cell phone to another, the Government could not be authorized to continue to stay with him unless each such facility had been specified in advance in the order. It is hard to discern why such a rule would be desirable.

The apparent intent of Section 2 of the SAFE Act is to make the roving wiretap provisions of FISA parallel to those for ordinary criminal roving wiretaps in Title III. Under 18 U.S.C. § 2518(11), the requirement in § 2518(1)(b)(ii) to provide a "particular description of the nature and location of the facilities from which or the place where the communication is to be intercepted" does not apply if, inter alia, the application "identifies the person believed to be committing the offense." Setting aside the issue about whether the "identification" requirement thus imposed by Title III is identical to that envisioned by Section 2 of the SAFE Act, the apparent intent of Section 2 is to mimic § 2518(11) by imposing an identification requirement in any case in which the requirement to specify particular places has been waived. The analogy, however, is flawed, because Section 2 overlooks a crucial difference between § 2518(11) and Section 105

of FISA.

In addition to waiving the specification-of-places requirement in § 2518(1)(b)(ii), the roving wiretap provision of Title III also waives the requirement in § 2518(3)(d) that the court must first find probable cause to believe that "the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or common used by [the target]." See 18 U.S.C. § 2518(11) (stating that the "requirements of subsections (1)(b)(ii) and 3(d) of this section relating to the specification of the facilities from which, or the place where, the communication is to be intercepted do not apply" to roving wiretaps authorized under Title III). As I explained above, FISA's analog to § 2518(3)(d) of Title III is contained in Section 105(a)(3)(B) of FISA, which states that an authorizing order may only be issued if, inter alia, "there is probable cause to believe that ... each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." 50 U.S.C. § 1805(a)(3)(B). It is important to note that nothing in the roving wiretap provisions of FISA waives this requirement. The apparent effect of that difference is that unlike Title III, a FISA roving wiretap application must still provide, as I explained earlier, a sufficient description of the categories of facilities and places that will be surveilled (presumably by describing their connection to the target) so as to permit the court to make the additional probable cause finding that remains required by Section 105(a)(3)(B). This additional safeguard strikes a different balance from Title III, but an appropriate one, and it makes SAFE Act Section 2's analogy to Title III inapt. That is, in light of FISA's preservation of this requirement, the need for a requirement to "identify" the target is doubtful. Indeed, because it overlooks this crucial additional requirement that only FISA imposes, the clear effect of Section 2 would be to make FISA roving wiretaps harder to obtain that Title III wiretaps.

(7) Section 207

Section 207 extends the time periods for which the FISA Court can initially authorize, and later extend, electronic surveillance and physical searches. See Pub. L. No. 107-56, § 207, 115 Stat. at 282. Notably, Section 207 only permits these more generous time periods to be used with respect to a FISA target who is not "a United States person." 50 U.S.C. § 1805(e)(1)(B), (e)(2)(B) (limiting this authority to "an agent of a foreign power, as defined in section 1801(b)(1)(A) of this title"); id., § 1801(b)(1) (stating that the definition in that paragraph applies only to a "person other than a United States person") (emphasis added). Pre-existing law had already permitted more generous authorization periods for FISA orders directed at entities, organizations, and groups that constitute "foreign powers," 50 U.S.C. § 1805(e)(1)(A), (e)(2)(A), and Section 207 properly permits longer authorization periods to also be used only for that subset of agents of foreign powers who are not United States persons. There seems to be little advantage to allowing this provision to sunset; the net effect would merely be more paperwork and a diversion of scarce resources that would be more appropriately deployed on other matters.

(8) Section 209

Section 209 of the PATRIOT Act eliminates the anomalous disparity in prior law between the standards for obtaining stored email and those for obtaining stored voicemail. Under prior law, voicemail stored with a third party required a full-blown Title III order, but stored email (and voicemail on the criminal's home answering machine) could be obtained with a regular search warrant. From a technological-neutrality perspective, this did not make a lot of sense. The PATRIOT Act amends the law so that a search warrant will do in such cases. Pub. L. No. 107-56, § 209, 115 Stat. at 283. Because a stored voicemail is, by definition, not a live communication but is instead a record of a completed communication, the more stringent regime created by Title III for contemporaneous interception of communications is unwarranted here. A search warrant, with its requirement of a probable cause finding by a neutral magistrate, should be sufficient.

(9) Section 212

Section 212 of the PATRIOT Act provides a defined authority for electronic communications service providers to make voluntary disclosures of customer records or communications. Specifically, Section 212 permits voluntary disclosure of the contents of communications in certain emergency situations and also codifies the various circumstances in which an ISP may disclose customer records other than the contents of a communication. See Pub. L. No. 107-56, § 212(a)(1)(D), (E), 115 Stat. at 284-85.

Notably, the authority given by Section 212 to disclose the content of communications in emergency situations was repealed, and re-enacted in a different form, by the Homeland Security Act. See Pub. L. No. 107-296, § 225(d)(1), 116 Stat. 2135, 2157 (2002). As such, that authority is no longer subject to the PATRIOT Act's sunset provision. Allowing Section 212 to expire would thus sunset the authority to make certain voluntary disclosures of records (including disclosures of records in an emergency), thus creating the anomalous result that an ISP, in an emergency, could disclose the contents of communications, but not the less-sensitive customer records of the subscriber associated with those communications. This does not make a great deal of sense. Moreover, the additional situations (other than an emergency) in which Section 212 permits voluntary disclosures of customer records (e.g., when already authorized by 18 U.S.C. § 2703; when the subscriber consents; when necessary to protect the ISP's network

and other rights; and when made to another non-governmental entity) do not seem unreasonable. This provision should be made permanent. (I would note, parenthetically, that the voluntary disclosure authority in 18 U.S.C. § 2702(c)(5), which was added by the PROTECT Act, is permanent and would not be affected by a sunset of Section 212.)

(10) Section 214

Section 214 is one of several provisions of the PATRIOT Act that properly endeavor to ensure that there will be appropriate analogs, in foreign intelligence investigations, for the various tools that are available to assist law enforcement in criminal investigations. In particular, Section 214 addresses the use of "pen registers" and "trap and trace devices," i.e., instruments for collecting information about the address or routing of a communication (e.g., the telephone numbers of outgoing calls dialed on a telephone and the telephone numbers of incoming calls), but not the content of the communication.

The Supreme Court held long ago that that the proper use of a pen register does not implicate the Fourth Amendment, because there is no reasonable expectation of privacy in the numbers dialed on a telephone -- numbers that, by definition, the dialer has voluntarily turned over to a third party (i.e., the telephone company). Smith v. Maryland, 442 U.S. 735, 744 (1979). Since 1986, however, Congress has appropriately regulated the use of such devices, requiring (inter alia) an attorney for the Government to make an application to a court in which the attorney certifies that the information to be collected is relevant to an ongoing criminal investigation. 18 U.S.C. § 3122(b)(2).

Prior to Section 214, FISA analogously allowed the use of pen registers and trap and trace devices in foreign intelligence investigations, but the limitations imposed by FISA on such devices were much more restrictive than in the criminal context. Specifically, in contrast to the more generous "relevance" standard imposed in criminal cases, FISA limited the use of such devices to situations where the facilities in question have been or are about to be used in communication with "an individual who is engaging or has engaged in international terrorism or clandestine intelligence activities" or a "foreign power or an agent of a foreign power." 50 U.S.C. § 1842(c)(3) (2000 ed.). Section 214 amended FISA's standards to permit appropriate use of such devices upon a certification that the device is likely to obtain (1) "foreign intelligence information not concerning a United States person" or (2) information that is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities." See Pub. L. No. 107-56, § 214(a)(2), 115 Stat. at 286. In the latter context, Section 214 provides explicit protection for the First Amendment rights of United States persons. Id.

Under Section 214, the ability to use pen registers and trap and trace devices under FISA is thus rendered more analogous in scope to its criminal counterpart. With respect to information concerning a United States person, Section 214 imposes the same standard of "relevance" to an ongoing investigation, but it also specifies that the investigation must be one to protect against "international terrorism" or "clandestine intelligence activities." Given that 18 U.S.C. § 3122 imposes a relevance standard in all ordinary criminal cases, it is hard to see why that standard is not sufficient in an intelligence investigation to protect against international terrorism and clandestine intelligence activities. That is, if relevance to an ongoing investigation is a sufficient basis for authorizing a pen register in, say, a fraud case or a drug case, why would it not be a sufficient basis for permitting the use of such a device to investigate international terrorism?

(11) Section 215

Section 215 of the PATRIOT Act is another provision designed to ensure that a tool available to assist law enforcement in ordinary criminal investigations will have an appropriate counterpart in foreign intelligence investigations. For a very long time, grand juries have had very broad authority to obtain, by subpoena, records and other tangible items that may be needed during the course of a criminal investigation. Section 215 provides a narrow analog to such subpoenas in the context of certain intelligence investigations under FISA. Indeed, in many respects, Section 215 contains more protections than the rules governing grand jury subpoenas:

-- A court order is required. 50 U.S.C. § 1861(c).

-- The court is not merely a rubber-stamp, because the statute explicitly recognizes the court's authority to "modif[y]" the requested order. Id., § 1861(c)(1).

-- The section has a narrow scope, and can be used in an investigation of a U.S. person only "to protect against international terrorism or clandestine intelligence activities." Id., § 1861(a)(1), (b)(2). It cannot be used to investigate domestic terrorism.

-- The section provides explicit protection for First Amendment rights. Id., § 1861(a)(1), (a)(2)(B).

Despite what some of its critics seem to imply, this narrowly drafted business records provision has no special focus on authorizing the obtaining of "library records." On the contrary, because the provision specifically forbids the use of its authority to investigate U.S. persons "solely upon the basis of activities protected by the first amendment to the Constitution," the provision does not authorize federal agents to rummage through the library records of ordinary citizens. Moreover, it would make no sense to create a carve-out for libraries from the otherwise applicable scope of Section 215: that would simply establish libraries and library computers as a "safe harbor" for international terrorists.

Indeed, over the years, grand juries have, on appropriate occasions, issued subpoenas for library records in connection with ordinary criminal investigations. In my view, a sensible privacy policy should allow an appropriately limited analog in the FISA context, and Section 215 is just that.

Section 4 of the SAFE Act would amend the FISA so that the authority conferred by Section 215 could only be exercised if "there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power." This is much too narrow a standard. Suppose that FBI agents suspected that an as-yet-unidentified individual foreign agent may have consulted certain specific technical titles on bomb-making or on nuclear power facilities, and they are informed that 5 persons have checked out those specific titles from public libraries in the relevant area and time period. Would Section 4 bar the agents from getting those records for all 5 persons? It would seem so. Under Section 4, it must be shown that "the person to whom the records pertain" is an agent of a foreign power, i.e., that the individual whose records are sought is a foreign agent. Because it cannot be said that there are "specific and articulable facts" to suspect all 5 persons who checked out the books as all being foreign agents (the most that can be said is that one of them may be), Section 4 would seemingly require more. Even if one were to agree that the general business records authority in Section 215 might benefit from greater reticulation in the contexts of particular types of records, this particular requirement seems too strict. Given the various safeguards already in place in Section 215, which adequately take account of the difference between investigations under FISA and ordinary criminal investigations, there is insufficient justification for a standard that is so much more demanding than the ordinary "relevance" standard that has long governed grand jury subpoenas in criminal investigations (some of which, like the Versace murder and Zodiac gunman investigations, did consult library records).

(12) Section 217

Section 217 of the PATRIOT Act eliminates the loophole in prior law under which hackers were arguably protected by the wiretap law from law-enforcement monitoring authorized by the operators of the computers they invade. Pub. L. No. 107-56, § 217, 115 Stat. at 290-91. Section 217 contains appropriately drawn language that permits such monitoring only with the authorization of the owner or operator of the "protected computer" that has been hacked, and it requires that the monitoring be conducted in such a way as to ensure that it "does not acquire communications other than those transmitted to or from the computer trespasser." Id., § 217(2), 115 Stat. at 291. This sensible provision should be retained.

(13) Section 218

Despite being only one sentence long, Section 218 is one of the most important provisions in the PATRIOT Act. Prior to Section 218, an application for electronic surveillance under FISA had to contain a certification that "the purpose" of the surveillance "is to obtain foreign intelligence information." 50 U.S.C. § 1804(a)(7)(B) (2000 ed.). Section 218 changed the phrase "the purpose" to "a significance purpose," thus clarifying that the presence of other purposes (such as a possible criminal prosecution) did not preclude a FISA application. In doing so, Section 218 disapproved the "primary purpose" test that had been engrafted onto the pre-PATRIOT Act language. In re Sealed Case, 310 F.3d 717 (For. Intel. Surv. Ct. of Rev. 2002). This amendment, as many have noted, was important in tearing down the "wall" between intelligence personnel and law enforcement personnel. It should not be permitted to lapse. Moreover, allowing Section 218 to expire could potentially put the law in a state of confusion, because the Foreign Intelligence Surveillance Court of Review has cast doubt on whether the "primary purpose" test was a correct reading of the pre-PATRIOT Act statutory language. In re Sealed Case, supra. As a result, there is considerable room for argument over what exactly would be the effect of allowing this provision to lapse. The Congress should ensure clarity in this important area of the law by making Section 218 permanent.

(14) Section 220

Section 220 properly recognizes the inherently interstate nature of electronic communications by allowing nationwide service of search warrants for electronic evidence. Pub. L. No. 107-56, § 220, 115 Stat. at 291-92. No real advantage would be gained by allowing this provision to lapse. It did not change the substantive standards under which judges issue such warrants, and the change is logistically efficient, especially in a time-sensitive situation, and it reduces the disproportionate burdens that would otherwise fall on those districts which contain major ISPs (such as the Northern District of California and the Eastern District of Virginia). This provision should be made permanent.

(15) Section 223

Section 223 provides for civil liability for certain unauthorized disclosures of intercepted communications. Pub. L. No. 107-56, § 223, 115 Stat. at 293-95. This is a pro-privacy provision that, happily, has not yet had occasion to be invoked. I can think of no substantial reason why it should not be made permanent.

(16) Section 225

This section extends to the FISA statute the same immunity from civil liability that exists under Title III for wire or electronic communications service providers who assist in carrying out a court order or an emergency request for assistance under FISA. Pub. L. No. 107-56, § 225, 115 Stat. at 295-96. There is no good reason the immunity of a

service provider for carrying out court orders for surveillance should depend upon whether the order was issued under Title III or under FISA. This provision should be made permanent.

Section 213

Although it is not subject to the PATRIOT Act's sunset provision, I would also like to say a few words about Section 213 of the PATRIOT Act, because it has been the subject of much attention and discussion.

Section 213 of the Patriot Act codifies long-standing authority to delay notification of the execution of a warrant. See, e.g., United States v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990). It does so with proper safeguards: the court must independently find "reasonable cause" to justify the delay; the court must set forth in the warrant the "reasonable period" for such delayed notice; and such a deadline may be extended only upon a subsequent finding by the court that "good cause" has been shown for the additional delay. 18 U.S.C. § 3103a(b). These stringent safeguards are entirely appropriate, but they are also entirely adequate. Although the revisions that would be made by Section 3 of the SAFE Act in S. 737 are not as extensive as those that were contained in the prior version of the SAFE Act in the 108th Congress (S. 1709), I continue to believe that the changes made by Section 3 would be a mistake. In particular, there is no substantial reason why delayed notice should not be authorized when notification could result in the jeopardizing of an entire ongoing investigation. So long as the court has the ultimate ability, and the independent ability, to supervise and control the delay, and the length of the delay, immediate notification should not be required when such serious concerns are present. Moreover, there is no persuasive reason why applications for renewals of such orders must be personally reviewed by the Attorney General, the Deputy Attorney General, or the Associate Attorney General.

* * *

I would like to make one final point. Some have criticized that many of the PATRIOT Act's reforms are not specifically limited so as to apply only in terrorism cases. Once again, I think this criticism reflects a failure to appreciate what sensible policy in this area entails. For example, if the principle of technological neutrality makes general sense, there is no reason why it should be limited to terrorism cases. Is it a rational privacy policy to say that persons committing bank fraud should have a leg up over law enforcement if they use one communications technology rather than another? The fact that terrorism concerns motivated the effort to fix the problem in this area does not mean that the problem should not be fixed in a comprehensive and rational manner.

In closing, the PATRIOT Act is an invaluable and landmark piece of legislation that has worked to protect American lives while preserving American liberties. The 16 provisions that are currently subject to sunset should all be made permanent.

I would be pleased to answer any questions the Committee might have on this subject.