Testimony of

Mr. Dan Collins

Associate Deputy Attorney General and Chief Privacy Officer
U.S. Department of Justice
September 22, 2004

Testimony of Daniel P. Collins
before the Senate Committee on the Judiciary
September 22, 2004

Chairman Hatch and Members of the Committee, I appreciate the opportunity to testify here today. The prevention of terrorist attacks is a matter of the most vital importance to our Nation. The Congress has few responsibilities that are more important than ensuring that the men and women who work day in and day out to protect us all have the tools that they need to get the job done -- and to get it done in a way that both enhances security and respects liberty.

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.

In evaluating whether current law provides appropriate tools for fighting terrorism, one must begin with the USA Patriot Act, Pub. L. No. 107-56, 115 Stat. 272 (2001). This landmark piece of legislation was passed in October 2001 by overwhelming bipartisan majorities in both houses -- indeed, the vote in the Senate was a remarkable 98-1. Despite this broad consensus, some commentators have denounced the legislation as a grave threat to privacy and civil liberties. In my view, these criticisms of the Act are not well-founded. On the contrary, the Act represents a measured, responsible, and constitutional approach to the threat of terrorist activities conducted in the United States and directed against American citizens.

In evaluating any legislation in this area, whether it be the Patriot Act or the proposed SAFE Act (S. 1709), there is, I think, general agreement that the goal must be to fashion appropriate tools to fight terrorism in a manner that preserves and enhances privacy. Beyond that overarching goal, I think that there is (or should be) general agreement on a number of specific principles that should guide the effort to achieve that goal:

? 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.

? Privacy protection is not a zero-sum game. Too often, the debate over the Patriot Act, as well as over other measures, has wrongly viewed the matter as some sort of zero-sum game. Some critics seem to operate from the implicit premise that anything that helps law enforcement is necessarily a reduction in civil liberties and a loss of freedom. This sort of thinking does not make much sense either from a law enforcement perspective or from a civil liberties perspective.

? 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, using a number of examples, why I think the Patriot Act properly enhances the abilities of law enforcement in a manner that respects and preserves our freedoms, and why I think that the proposed SAFE Act does not strike the right balance.

? Section 215 of the Patriot Act enacted much-needed reforms to the provisions of the Foreign Intelligence Surveillance Act ("FISA") that govern the ability to obtain business records in connection with FISA investigations. Despite the stridency of some of the criticisms leveled at Section 215, the authority provided by this section is quite modest and, in my view, quite reasonable. 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. (Section 5 of the SAFE Act, which would carve library computers out of the national security letter authority in 18 U.S.C. § 2709, suffers from a similar flaw.) 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).

? 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. In particular, the revisions that would be made by Section 3 of the SAFE Act would be a serious mistake. There is no reason why delayed notice should not be authorized when notification could result in the intimidation of witnesses, the destruction of other evidence (i.e., evidence other than that described in the warrant), or 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, immediate notification should not be required when such serious concerns are present. Indeed, Section 3 of S. 1709 would leave the law worse than it was before the Patriot Act.

? I also believe that the Patriot Act strikes the right balance on the subject of "roving wiretaps" under FISA and that the amendments that would be made by Section 2 of the SAFE Act are unwarranted.

Section 2 of the SAFE Act would amend Section 105 of FISA to provide, in effect, that an order authorizing electronic surveillance under FISA must either (1) specify the "identity of the target of electronic surveillance" or (2) specify "the nature and location of each of the facilities or places at which the electronic surveillance will be directed." To evaluate the significance of this proposed new requirement, one needs to consider exactly how it would differ from the law as it stands today.

Under current law, 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). 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) unambiguously 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). 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 the Patriot Act here was 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 (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 very obvious potential to allow targets to defeat surveillance simply by changing, for example, from one cell phone to another.

Against this backdrop, the amendment that would be made by Section 2 of the SAFE Act 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't 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 Patriot Act makes more technologically neutral the statutes governing pen registers -- devices to capture routing and signaling information, but not content. See Pub. L. No. 107-56, § 216, 115 Stat. at 288-90. These laws now clearly apply to both electronic communications and telephonic communications. And to take account of the specific privacy concerns raised about the use of government-installed programs to implement such orders -- I am referring to the "Carnivore" debate -- the Act provides for judicial oversight by requiring detailed reporting to the court whenever such a government-installed program is used to implement a pen/trap order involving electronic communications. 18 U.S.C. § 3123(a)(3). Section 6 of the SAFE Act would sunset this provision, which seems hard to justify. Why would we want to have a legal regime in

which the addressing information on an email is treated differently from the addressing information on a postal letter? (Although that appears to be the intent of this sunset provision, it is not entirely clear that repealing Section 216, without more, will have that effect.)

? The Patriot Act eliminates unwarranted and irrational disparities in prior law, which afforded different levels of protection to similar things. For example, prior law (at least in the view of some courts) afforded different levels of protection to Internet communications based upon whether the person used a cable company, as opposed to a telephone company, to reach the Internet. This sort of disparate treatment violates the principle of technological neutrality and is very hard to justify under any rational theory of appropriate law enforcement. The Patriot Act fixes this. See Pub. L. No. 107-56, § 211, 115 Stat. at 283-84.

? The Patriot Act allows a single federal district court to issue an order authorizing the installation of a pen register or trap and trace device "anywhere within the United States." Pub. L. No. 107-56, § 216(b)(1), 115 Stat. at 288-89. In light of the inherently interstate nature of electronic communications, and the number of entities that may be involved in transmitting them, a nationwide scope makes perfect sense. And there is little gain, if any, from a civil liberties perspective, in requiring the Government to incur the shoe leather costs of getting separate orders in multiple districts.

? Similarly, the Patriot Act properly recognizes the inherently interstate nature of electronic communications by allowing nationwide service of search warrants for electronic evidence. Id., § 220.

? 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. Law enforcement should have at least the same tools to fight terrorism that it has to fight organized crime.

? 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. Again, from a technological-neutrality perspective, this didn't 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.

? The Patriot Act further 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. Id., § 217.

These provisions of the Patriot Act -- a statute passed by overwhelming bipartisan majorities in both houses -- are just a few illustrations of how the Act properly updates the law while respecting and preserving our freedoms.

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.

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