1-1-2012

The USA Patriot Act: Big Brother or Business as Usual

James B. Perrine
Gregory Todd Jones

Follow this and additional works at: http://scholarship.law.nd.edu/ndjlepp

Recommended Citation
Available at: http://scholarship.law.nd.edu/ndjlepp/vol19/iss1/6

This Article is brought to you for free and open access by the Notre Dame Journal of Law, Ethics & Public Policy at NDLScholarship. It has been accepted for inclusion in Notre Dame Journal of Law, Ethics & Public Policy by an authorized administrator of NDLScholarship. For more information, please contact lawdr@nd.edu.
THE USA PATRIOT ACT: BIG BROTHER OR BUSINESS AS USUAL?

JAMES B. PERRINE*

On September 11, 2001, terrorists hijacked jet airliners and flew them into the World Trade Center and the Pentagon. Another hijacked jet airliner crashed into a field in Pennsylvania. The "War on Terror" began. In response to, and shortly after, these attacks, Congress passed, and President Bush signed, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. A debate over the constitutionality and appropriateness of the Patriot Act has furiously raged since its enactment.

Critics argue that the Patriot Act is a knee-jerk reaction to the events of September 11th that greatly expands the powers and reach of law enforcement officials and unduly tramples upon civil liberties. Proponents of the Patriot Act contend that it updates investigative techniques to account for new technologies and the practices of terrorists—techniques needed to track and capture terrorists and thwart their attacks. This Article examines this debate with respect to provisions of the Patriot Act permitting delayed notification or "sneak-and-peek" search warrants, roving wiretaps, and compelled production of business records—three areas of particular concern to opponents and supporters of this controversial piece of legislation.

* Assistant United States Attorney, Middle District of Alabama. J.S.D., L.L.M., Yale University Law School; J.D., University of Alabama School of Law. The views expressed herein are solely the author’s personal views and do not represent the official views or policies of the Department of Justice or any of its subdivisions. The author would like to thank Jack Park, Pamela Bucy, and Matthew Berry for their comments and suggestions. Any errors in the article are solely those of the author.

This Article is copyright © 2004 by James B. Perrine. All rights reserved.

For each of these provisions, the question is the degree to which the Patriot Act expands the power of government officials or applies existing law enforcement techniques to the investigation and prosecution of terrorists. A review of the legal landscape before and after the Patriot Act shows that, at least in these three areas, Congress has neither created nor dramatically increased the purview of "Big Brother," but, rather, has made available for the investigation of terrorists tools to which law enforcement officials were already privy in other contexts. Of course, the normative question of whether law enforcement officials should even have access to such tools is a separate debate and one outside the scope of this Article.

I. DELAYED NOTIFICATION SEARCH WARRANTS

A. The Legality of Delayed Notification Search Warrants Pre-Patriot Act

The Fourth Amendment to the Constitution protects the "right of the people" to be free from "unreasonable searches and seizures" and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." Federal Rule of Criminal Procedure 41 sets forth the rules pertaining to the issuance, execution, and return of search warrants. As part of the standard search warrant procedure, law enforcement officers must provide notice of the search and the seizure of any property during such search to the individual whose premises were searched. This notice is typically provided by giving the person, or leaving at the premises, a copy of the warrant and a receipt of any property taken. Not surprisingly, situations arise, however, where law enforcement officers would rather not apprise an individual of a search and seizure. In such cases, the issue arises whether officers may

4. At least one other scholar has also concluded that the Patriot Act did not significantly expand the investigatory powers of law enforcement officials relative to their pre-Patriot Act capabilities. Orin S. Kerr, Internet Surveillance Law After the USA PATRIOT Act: The Big Brother that Isn't, 97 Nw. U. L. Rev. 607, 608 (2003) (concluding that the Patriot Act "made mostly minor amendments to the electronic surveillance laws" and "is not the Big Brother law that many have portrayed it to be").
5. U.S. CONST. amend. IV.
6. FED. R. CRIM. P. 41.
7. Id. 41(f).
8. See id.
9. Both proponents and critics of the Patriot Act agree that delayed notification warrants are justified in certain circumstances, such as where notice
search the premises but delay notifying the occupant of the search.

Prior to the Patriot Act, “delayed notification” or “sneak-and-peek” search warrants were permitted in several jurisdictions.10 The Ninth Circuit, in United States v. Freitas,11 was the seminal court to address directly the legality of delayed notification search warrants. In Freitas I, agents of the Drug Enforcement Administration (“DEA”) first obtained a number of standard search warrants to search a target’s home for evidence of his manufacturing of methamphetamine. The day after obtaining these standard search warrants, but prior to executing them, a DEA agent applied for and received a “surreptitious entry” warrant for the target’s house. The warrant authorized the agents to enter the house while no one was there and look around for evidence of a methamphetamine lab but forbade them from seizing any tangible property. The warrant did not contain a notice requirement. The agents executed this warrant on the same day the magistrate issued it. Approximately one week after executing the surreptitious warrant, the agents executed the standard search warrants, found evidence of a methamphetamine lab, and arrested the defendant.12

The defendant moved to suppress the evidence seized pursuant to the standard search warrants claiming that such evidence was the fruit of an unconstitutional search executed under the surreptitious warrant.13 The district court granted the defendant’s motion to suppress because the surreptitious warrant violated the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure.14 Moreover, the district court ruled that the “good faith” exception to the exclusionary rule announced in United States v. Leon15 did not support admission of the evidence.16

The Ninth Circuit reversed the district court’s decision. The appellate court concluded that the surreptitious warrant was

---

11. 800 F.2d 1451 (9th Cir. 1986) [hereinafter Freitas I].
12. Id. at 1453.
13. Id. at 1453–54.
14. Id. at 1454.
15. 468 U.S. 897 (1984) (holding that evidence seized pursuant to a defective warrant is still admissible as long as a reasonable officer would have relied in good faith on the validity of the warrant).
16. See Freitas I, 800 F.2d at 1454.
defective and violated Rule 41 and the Fourth Amendment because it did not provide any means of notice to the person whose premises were to be searched.\(^{17}\) In particular, the court held that “the warrant was constitutionally defective in failing to provide explicitly for notice within a reasonable, but short, time subsequent to the surreptitious entry. Such time should not exceed seven days except upon a strong showing of necessity.”\(^{18}\) The court, however, remanded the case to the lower court for a decision on whether Leon saved the evidence from suppression.\(^{19}\)

On the subsequent appeal from the district court’s decision that Leon did not apply, the Ninth Circuit held that the agents had, indeed, reasonably relied in good faith on the surreptitious warrant and that evidence from the search was admissible.\(^{20}\) The court further explained that even though it found the surreptitious warrant constitutionally defective in its first opinion, that error was not a “clear constitutional violation.”\(^{21}\) The court reiterated that the “constitutional infirmity did not emanate from the surreptitious nature of the entry, or even from the fact that the warrant failed to provide for contemporaneous notice of the search.”\(^{22}\) Rather, the warrant suffered from a complete lack of a notice requirement. Simply stated, if the warrant “had provided for post-search notice within seven days, it would not have crossed over the constitutional line.”\(^{23}\)

Four years later in 1990, the Second Circuit analyzed the legality of delayed notification warrants. In United States v. Villegas, DEA agents suspected that individuals were using a farm to manufacture cocaine powder. To confirm their suspicions, agents applied for a search warrant “to take photographs but not physically to seize any tangible items of evidence.”\(^{24}\) The agents also asked to postpone giving notice of the search for seven days,

\(^{17}\) Id. at 1456.

\(^{18}\) Id.

\(^{19}\) Id. at 1457–58.

\(^{20}\) United States v. Freitas, 856 F.2d 1425, 1432 (9th Cir. 1988) [hereinafter Freitas II]; see also United States v. Johns, 948 F.2d 599, 605–06 (9th Cir. 1991) (applying Leon to delayed notification search warrant); United States v. Ludwig, 902 F. Supp. 121, 127 (W.D. Tex. 1995) (also applying Leon to delayed notification warrants and finding the evidence admissible).

\(^{21}\) Freitas II, 856 F.2d at 1433 (citing United States v. Stefanson, 648 F.2d 1231, 1235 (9th Cir. 1981)).

\(^{22}\) Id. (citing Dalia v. United States, 441 U.S. 238, 247–48 (1979) (rejecting as “frivolous” the argument that “covert entries are unconstitutional for their lack of notice”)).

\(^{23}\) Id.

\(^{24}\) 899 F.2d 1324 (2d Cir. 1990).

\(^{25}\) Id. at 1330.
or for a longer period if the court so permitted. The district court issued the delayed notification search warrant and required notice to the person whose premises were searched within seven days. The court, however, would permit an extension of the notice period for good cause shown. The agents executed the warrant and thereafter requested eight separate extensions of the notice period to permit them to continue their investigation unbeknownst to the targets. The district court granted each extension such that notice was not given to the individuals until they were arrested after the execution of a standard search warrant at the farm.

The defendants sought to suppress the evidence seized during the execution of the standard search warrant on the grounds that it was the product of the allegedly unconstitutional delayed notification warrant. The district court rejected this argument and the Second Circuit affirmed the lower court’s decision.

The court started its analysis by noting that “[w]hen nondisclosure of the authorized search is essential to its success, neither Rule 41 nor the Fourth Amendment prohibits covert entry.” Such entry without notice to the defendant is permissible provided that certain safeguards are in place. “First, the court should not allow the officers to dispense with advance or contemporaneous notice of the search unless they have made a showing of reasonable necessity for the delay.” This showing is not as rigorous as that required for a wiretap but still must provide good reason for the delay in notification. “Second, if a delay in notice is to be allowed, the court should nonetheless require the officers to give the appropriate person notice of the search within a reasonable time after the covert entry.” Though what constitutes a “reasonable time” is a fact-specific determination, the Villegas court agreed with the Ninth Circuit that such period should not exceed seven days, absent good cause for extending the notification period. Since the warrant at issue satisfied each of these safeguards, the court held that the delayed notific-
tion warrant was constitutional and any evidence seized as a product of such warrant was admissible.\textsuperscript{35}

Importantly, the \textit{Villegas} court commented that a "covert-entry search for only intangibles" is, comparatively, not a particularly intrusive search. In particular, the court noted several limitations of a delayed notification warrant:

It is less intrusive than a conventional search with physical seizure because the latter deprives the owner not only of privacy but also of the use of his property. It is less intrusive than a wiretap or video camera surveillance because the physical search is of relatively short duration, focuses the search specifically on the items listed in the warrant, and produces information as of a given moment, whereas the electronic surveillance is ongoing and indiscriminate, gathering in any activities within its mechanical focus. Thus, several of the limitations on wiretaps or videotape surveillance, such as duration and minimization, would be superfluous in the context of a physical search.\textsuperscript{36}

The Second Circuit subsequently confirmed its approval of delayed notification warrants in \textit{United States v. Pangburn}.\textsuperscript{37} In that case, the appellate court upheld the validity of two surreptitious warrants that permitted agents to search a storage locker, even though the warrants did not contain a notice provision.\textsuperscript{38}

Though the Ninth Circuit in \textit{Freitas I} held that the complete omission of a notice provision rendered a warrant constitutionally defective, the \textit{Pangburn} court stated that the panel in \textit{Villegas} did not subscribe to this position.\textsuperscript{39} The difference between the positions of the Ninth and Second Circuits lies in the source of the notice requirement. The Ninth Circuit grounds the notice requirement in the Fourth Amendment,\textsuperscript{40} while the Second Circuit grounds it in Rule 41.\textsuperscript{41} Accordingly, the Second Circuit views a warrant’s failure to speak to notice as a statutory, but not constitutional, violation.\textsuperscript{42}

\textsuperscript{35} Id. at 1338.
\textsuperscript{36} Id. at 1337.
\textsuperscript{37} 983 F.2d 449 (2d Cir. 1993).
\textsuperscript{38} See id. at 449–50.
\textsuperscript{39} See id. at 454.
\textsuperscript{40} Freitas I, 800 F.2d 1451, 1456 (9th Cir. 1986).
\textsuperscript{41} See Pangburn, 983 F.2d at 455.
\textsuperscript{42} See id.; see also United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000) (recognizing the split between the Ninth and Second Circuits and agreeing with the Second Circuit that Rule 41, not the Constitution, requires notice of an executed search).
A violation of Rule 41 leads to exclusion of evidence only where:
(1) there was "prejudice" in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision in the Rule.

Since the agents would have conducted the search in exactly the same way if notice had been given within seven days of the search and did not intentionally disregard the notice requirement, having sought review of the warrant from a district attorney and magistrate, the Second Circuit held that the violation of Rule 41 for not providing notice to the defendant did not justify suppression of the challenged evidence.

B. The Patriot Act Codifies Existing Law on Delayed Notification Warrants

The Patriot Act, as shown by its express provisions, merely codifies much of the existing law relating to delayed notification warrants. More specifically, section 213 of the Patriot Act added the following section to 18 U.S.C. § 3103a:

(b) Delay.—With respect to the issuance of any warrant or court order under this section, or any other rule of law, to search for and seize any property or material that constitutes evidence of a criminal offense in violation of the laws of the United States, any notice required, or that may be required, to be given may be delayed if—
(1) the court finds reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse result (as defined in section 2705);
(2) the warrant prohibits the seizure of any tangible property, any wire or electronic communication (as defined in section 2510), or, except as expressly provided in chapter 121, any stored wire or electronic information, except where the court finds reasonable necessity for the seizure; and
(3) the warrant provides for the giving of such notice within a reasonable period of its execution, which period

43. Pangburn, 983 F.2d at 455 (citing United States v. Burke, 517 F.2d 377, 386–87 (2d Cir. 1975)).
44. Id.
45. Of course, the Patriot Act in no way altered the probable cause and particularity requirements for search warrants under the Fourth Amendment. See U.S. CONST. amend. IV.
may thereafter be extended by the court for good cause shown.\textsuperscript{46}

An "adverse result" referenced in § 3103a(b)(1) justifying delayed notification occurs where immediate notification may cause:

(A) endangering [of] the life or physical safety of an individual;
(B) flight from prosecution;
(C) destruction of or tampering with evidence;
(D) intimidation of potential witnesses; or
(E) ... serious[ ] jeopardy[ ] [to] an investigation or unduly delaying a trial.\textsuperscript{47}

A comparison of the pre-Patriot Act case law and section 213 of the Patriot Act shows that Congress did not broaden greatly, if at all, the circumstances in which law enforcement officials may request a court to delay notice of a search warrant.\textsuperscript{48} Section 213 authorizes a court to issue a delayed notification warrant only where reasonable cause exists that immediate notification will lead to one or more of the "adverse results" listed above. This requirement is akin, if not identical, to the "good reason" safeguard delineated by the \textit{Villegas} court.\textsuperscript{49} In fact, in \textit{Villegas}, the Second Circuit ruled that the agents' representation that surveillance on the target's farm was "extremely difficult" was a permissible justification for the issuance of the delayed notification warrant.\textsuperscript{50} Section 213 does not list the ineffectiveness of other investigatory techniques as a reason to authorize a delayed notification warrant, though such a standard is similar to the more

\textsuperscript{48} In a hearing before the Senate Judiciary Committee, Senator Feinstein states thus:

But I think many missed the fact that 213 is, for the most part, as I understand it, a codification of authority that was created by case law in the United States Court of Appeals for the Ninth Circuit in 1996 and the U.S. Court of Appeals in the Second Circuit in 1990. If I understand what we did in 213, it was actually narrower than the authority that existed before the Patriot Act in the Ninth Circuit and the Second Circuit, and that we provided in this bill certain additional safeguards in the area of sneak and peek so that civil liberties are actually better protected now in California, Idaho, New York and in other states that fell under those jurisdictions than before the Patriot Act.

\textsuperscript{49} United States v. Villegas, 899 F.2d 1324, 1337 (2d Cir. 1990).
\textsuperscript{50} Id. at 1338.
rigorous certification agents must make to obtain a wiretap. The Freitas court specifically held that the Fourth Amendment did not mandate a showing that other investigatory techniques were inadequate prior to the issuance of a delayed notification warrant. Section 213 also adopted the requirement in Freitas and Villegas that law enforcement officers provide notice of the search within a reasonable period of its execution. Congress, unlike the Freitas court, did not limit this time period to seven days. Like the Ninth and Second Circuits, section 213 permits the court to extend the notice period for good cause shown. Though not expressly stated in section 213, prior precedent suggests that agents will need to make a “fresh showing” of an adverse result from providing notice to justify an extension of the notice period.

The “reasonable necessity” standard for seizure of property under a delayed notification warrant is a feature of section 213 not readily evident from a review of case law. The law enforcement agents in Freitas and Villegas requested permission from the court only to enter the premises, look around, and take photographs, but did not seek to seize any tangible property within the premises. Consequently, neither the Ninth nor the Second Circuit addressed the legality of the seizure of property pursuant to a delayed notification warrant, though the Villegas court noted that a covert search for surveillance was less intrusive than a conventional search and seizure of property. The Fourth Circuit, however, has held that the Fourth Amendment was not contravened where agents seized property pursuant to a search warrant that required immediate notification, but where the agents did not provide such notice until forty-five days after the seizure of property. The Patriot Act’s requirement for the seizure of

51. See supra note 32.
52. Freitas I, 800 F.2d 1451, 1456 (9th Cir. 1986).
53. See Villegas, 899 F.2d at 1337.
54. See Freitas I, 800 F.2d at 1456.
55. See id.; see also Villegas, 899 F.2d at 1337.
56. Villegas, 899 F.2d at 1337 (“[T]he applicant should be required to make a fresh showing of the need for further delay.”) (referring to Berger v. New York, 388 U.S. 41, 59-60 (1967)).
57. Freitas I, 800 F.2d at 1453; Villegas, 899 F.2d at 1330.
58. Villegas, 899 F.2d at 1337.
59. United States v. Simons, 206 F.3d 392, 397, 403 (4th Cir. 2000) (“[W]e conclude that the failure of the team executing the warrant to leave either a copy of the warrant or a receipt for the items taken did not render the search unreasonable under the Fourth Amendment.”). See also United States v. Heal, No. 91-30349, 1992 WL 203884, at *2 (9th Cir. Aug. 20, 1992) (discussing approvingly a delayed notification search warrant permitting the actual seizure of controlled substances).
property under a delayed notification warrant is thus more stringent than what the Fourth Amendment otherwise mandates for seizures under conventional warrants (i.e., probable cause of criminal activity). This higher burden reflects Congress's sensitivity toward delayed notification warrants and addresses the Ninth Circuit's concern that "surreptitious entries be closely circumscribed." The "reasonable necessity" requirement in section 213 also reduces the probability of seizure during the execution of a delayed notification warrant because agents may decide to use the covert entry only to gain additional information that could then be used to support a later conventional search warrant.

The Patriot Act has thus clarified the jurisprudence on delayed notification warrants. Section 213 provides uniformity across the federal districts on the standards governing the issuance of a delayed notification warrant, the time period for notice to be provided to the affected persons, and the extension of the notice period. As the Ninth Circuit observed in Freitas, Congress's involvement in this area is preferable to a case-by-case modification of Rule 41 across the different circuits.61 In fact, section 213 directly answers the request of one scholar:

Perhaps one day Rule 41 will be amended to specifically mention surreptitious entry warrants and provide guidance in their use. Such amendments would promote uniformity among the circuits and set in place a concrete procedure to follow. The case-by-case, circuit-by-circuit approach to these warrants fails to assist law enforcement officers, prosecutors, and the courts in those circuits where the issue has not yet been sufficiently litigated.62

One issue still outstanding post-section 213 is whether an error in giving notice pursuant to a delayed notification warrant is a constitutional or statutory violation. Arguably, after the passage of the Patriot Act, a court will not issue a search warrant without abiding by section 213's requirement that notice be given "within a reasonable period of its execution."

60. See Freitas I, 800 F.2d at 1456.
61. Id. at 1455 ("[T]he adjustments to Rule 41 necessary to regulate surreptitious entries can better be accomplished by the rulemakers and Congress than by the case-by-case work of courts.").
court found to be a violation of the Fourth Amendment. Other errors relating to the notice provided pursuant to a delayed notification warrant should be analyzed, as the Ninth and Second Circuits have held, under the test discussed supra for "technical," "non-fundamental" violations of Rule 41.

C. Criticisms of Section 213 of the Patriot Act

Despite the benefits of section 213 in clarifying the law relating to delayed notification warrants, critics seek to repeal and/or amend its provisions. The proposed "Security and Freedom Ensured Act (the "SAFE Act") is representative of the proposals to amend section 213. First, the SAFE Act would shorten the list of "adverse results" justifying the issuance of a delayed notification warrant. Under the SAFE Act, a delayed notification warrant could issue only where immediate notification would (1) "endanger the life or physical safety of an individual," (2) "result in flight from prosecution," or (3) "result in the destruction of, or tampering with, the evidence sought under the warrant." Under the SAFE Act, an "adverse result" would no longer include a situation where immediate notice would result in the intimidation of potential witnesses or otherwise seriously jeopardize an investigation or unduly delay a trial.

Striking the last two definitions of "adverse result" under section 213 seems unprincipled. The intimidation of potential witnesses is just another form of the "destruction of evidence" justification for the issuance of a delayed notification warrant that is included in the SAFE Act. As every prosecutor knows, a live witness is frequently the best, and sometimes the only, evidence of a fact, and preservation of a credible witness to testify to a defendant's activities is as important as preserving physical evidence of a defendant's crime. Elimination of the "catch-all provision" of section 213 for an adverse result also appears to be unfounded. A criminal investigation, especially one involving terrorists, is fraught with nuances making it more of an art than a science. Delaying notice for a reasonable time subsequent to the surreptitious entry to address a concern that "seriously jeopardizes an investigation" is akin to the other "adverse result" categories untouched by the SAFE Act because they all seek to aid investigatory efforts.

65. Id.
66. See 18 U.S.C. §§ 2705 & 3103a(b) (defining "adverse result").
The SAFE Act also sets as seven days the maximum length of
time to delay notice of the surreptitious entry and allows an
extension of this period only if immediate notice would produce
one or more of its justifications for the initial issuance of a
delayed notification warrant. Amending section 213 to mandate
notice within seven days rather than within a "reasonable
period" after execution of the warrant limits a court's ability to
tailor a delayed notification warrant to the particular facts of an
investigation. In most instances, as the Freitas and Villegas courts
held, seven days is an appropriate period for agents to provide
notice of the search. In an exceptional case, however, seven days
may not be a "reasonable period" within which to provide notice.
As is always the case with an objective standard, "reasonableness"
is a fact-specific characteristic dependent upon the vagaries of
any given situation.

Ironically, the same critics of the Patriot Act who complain
that it makes the federal judiciary subservient to the executive
branch of government seek to divest judges of the discretion to
set a reasonable period for notice to be given of a surreptitious
search. Limiting the bases for which a court may extend the
notification period to the three instances specified in the SAFE
Act, rather than for "good cause shown" as provided in section
213, only further reduces the autonomy of judges to adapt a
delayed notification warrant to the particular facts of any given
case. Courts have always been the doorkeeper for the warrant
process, and Congress, in the Patriot Act, has wisely given federal
judges the discretion to fashion the details of providing notice of
a covert search.

The SAFE Act would also require the Attorney General to
submit a report to Congress, made available to the public, every
six months summarizing the number of requests for, and grants
and denials of, delayed notification warrants. The Patriot Act
requires such reporting to Congress for other law enforcement
techniques, but its sudden application to delayed notification
warrants would be unusual. Delayed notification warrants pre-
data the Patriot Act by at least fifteen years and prosecutors did
not have to inform Congress of their issuance. Fifteen years of

67. Id.
Durbin).
69. For example, section 215 of the Patriot Act requires the Attorney
General to inform Congress of the number of times agents have sought an
order from the FISA Court of Review for the production of tangible things from
businesses and other entities. Patriot Act § 215, 115 Stat. at 286–88 (to be codi-
practice with delayed notification warrants did not spur a need for congressional oversight of their issuance. Since the Patriot Act only codified existing law, one wonders why passage of section 213 would now trigger congressional concern about surreptitious searches where no such concern previously existed.

Finally, the SAFE Act would sunset the delayed notification warrant provisions of section 213 on December 31, 2005—the sunset date for other provisions in the Patriot Act. This proposal of the SAFE Act is puzzling as well, given the pedigree of delayed notification warrants. One issue raised by such a repeal of section 213 would be its effect on the validity of Freitas and Villegas. Arguably, these cases would remain good law, but their legitimacy would certainly be questioned. At the least, sunsetting section 213 would introduce much uncertainty into the area of delayed notification warrants—an area where courts and scholars have requested guidance, not ambiguity, from Congress.

The SAFE Act does not represent the only challenge to section 213 and delayed notification warrants. The Otter Amendment was an attempt to bar federal law enforcement agencies from using their budgeted funds to seek delayed notification warrants. This proposal would not repeal or amend section 213, but would render it meaningless by refusing to allow law enforcement agents to request, and judges to issue, delayed notification warrants. Arguably, such a tactic would not only be more draconian than the SAFE Act, which would permit the issuance of delayed notification warrants, but would more severely hamstring the judiciary’s right to decide the contours of the Fourth Amendment. Completely proscribing the issuance of delayed notification warrants differs practically little, if at all, from holding them unconstitutional. The House of Representatives approved the Otter Amendment on July 23, 2003, but the Senate did not move this legislation out of the upper chamber. Efforts to pass measures similar to the Otter Amendment during the current congressional session have not been successful.

II. ROVING WIRETAPS

A. Roving Wiretaps Under FISA

In 1978, Congress passed the Foreign Intelligence Surveillance Act (“FISA”), which established rules and procedures for the government’s gathering of foreign intelligence information.

70. See supra Part I.B.
71. H.R. 2799, 108th Cong. § 804 (1st Sess. 2003) ("None of the funds made available in this Act may be used to seek a delay under section 3103a(b) of Title 18, United States Code.").
through electronic surveillance.\textsuperscript{72} Electronic surveillance includes the interception of wire or radio communications such as a “wiretap” of a telephone call.\textsuperscript{73} To obtain a wiretap, a federal officer must make the appropriate showing in an application to the Foreign Intelligence Surveillance Court (the “FISA Court”), which can issue the wiretap order ex parte.\textsuperscript{74} Prior to the Patriot Act, the government could seek, and the FISA Court could issue, a wiretap only for a particular communication facility (e.g., a particular phone).

Section 206 of the Patriot Act amended FISA to permit “roving wiretaps” (e.g., a wiretap that follows the target from phone to phone) in certain circumstances.\textsuperscript{75} In particular, section 206 permits a roving wiretap only where “the [FISA] Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified [communication facility].”\textsuperscript{76} The advantage to law enforcement from a roving wiretap as compared to a static wiretap is that with a roving wiretap, “the government need not return to court for a new surveillance order every time the target changes location, but instead can present a generic order to the new carrier, landlord, or custodian, directing their assistance to assure that the surveillance may be undertaken as soon as technically feasible.”\textsuperscript{77}

Critics claim that the Patriot Act, by permitting roving wiretaps for foreign intelligence purposes, “has place[d] innocent individuals at risk for intrusive government surveillance.”\textsuperscript{78} The Patriot Act, however, is not the progenitor of roving wiretaps. Indeed, roving wiretaps have long been permitted in criminal investigations of certain enumerated offenses (e.g., controlled substance offenses). The Patriot Act, in large part, merely enabled the government to use a tool, roving wiretaps, in terrorism

\begin{itemize}
\item \textsuperscript{74} 50 U.S.C. § 1805 (delineating the requirements for the FISA Court to issue an order for electronic surveillance, including a wiretap).
\item \textsuperscript{75} Patriot Act, 115 Stat. at 282 (to be codified at 50 U.S.C. § 1862); see also ACLU v. U.S. Dep’t of Justice, 265 F. Supp. 2d 20, 23 (D.D.C. 2003) (“With a roving wiretap, the government can intercept all of a suspect’s communications relating to the conduct under investigation, regardless of the suspect’s location, and regardless of what particular phone or e-mail account he may be using.”).
\item \textsuperscript{76} 50 U.S.C. § 1805(c)(2)(B).
\item \textsuperscript{77} ACLU, 265 F. Supp. 2d at 23 (citing H.R. Rep. No. 107–236, pt. 1, at 60 (Oct. 11, 2001)).
\end{itemize}
investigations that law enforcement officers already had employed in sundry criminal investigations.

B. Roving Wiretaps Under Title III

In 1967, the United States Supreme Court held that the Fourth Amendment permitted wiretapping in certain circumstances.\(^7\) Congress codified the requirements for wiretapping in Title III of the Omnibus Crime Control and Safe Streets Act of 1968 ("Title III").\(^8\) Initially, Title III only permitted a "fixed wiretap" of a particular phone line. In 1986, Congress amended Title III to account for updated technologies.\(^8\) The amendments to Title III permitted "roving wiretaps," but only where the requesting official could show the court that the person believed to be committing the criminal offense had a purpose "to thwart interception by changing [communication] facilities."\(^8\) In 1998, Congress changed the standard to justify a "roving wiretap" to one where the court finds that "there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified [communication] facility."\(^8\)

Courts have held that a "roving wiretap" under Title III does not violate the Fourth Amendment.\(^8\) In United States v. Petti, the Federal Bureau of Investigation ("FBI") applied for and received judicial authorization for wiretap surveillance of the phones the defendant was suspected of using to further a money laundering scheme.\(^8\) The roving wiretap was used because the defendant had taken steps to prevent interception of his communications,

---

8. 18 U.S.C. §§ 2510–2520 (2000) (delineating requirements to permit electronic surveillance including probable cause that an individual is committing a particular enumerated offense and that normal investigative procedures have been tried to obtain the information but were unsuccessful).
12. United States v. Bianco, 998 F.2d 1112, 1128 (2d Cir. 1993) (holding that "roving bug" surveillance for the interception of oral communications under Title III does not violate the Fourth Amendment); see also Petti, 973 F.2d at 1445 (holding that "roving wiretap" under Title III does not violate the Fourth Amendment).
13. Petti, 973 F.2d at 1442.
including thwarting the use of a body wire on a confidential source. With the roving wiretap, the FBI monitored the defendant's conversations over various and changing public telephones for approximately a year and a half. Based in part on information gained through the roving wiretap, the United States indicted the defendant on money laundering and currency reporting offenses. The defendant moved to suppress the information gained through the roving wiretap on the grounds that such interception violated the particularity requirement of the Fourth Amendment.

The Ninth Circuit affirmed the district court's holding that the roving wiretap provision of Title III did not violate the Fourth Amendment and that evidence gained through the roving wiretap was admissible at trial. In particular, the court found that "the absence of a description of the specific telephone facilities from which the suspect's conversations are to be intercepted" did not violate "the Fourth Amendment's requirement that no warrant shall issue except one 'particularly describing the place to be searched.'" The particularity requirement of the Fourth Amendment requires:

The description of the place to be searched must not be so broad as to allow the search of places for which probable cause to search has not been demonstrated, or so vague that an executing officer might mistakenly search a place for which authorization was not granted. If the description of the place to be searched avoids these dangers, it may comply with the particularity requirement even though it does not specify the physical location of the place to be surveilled.

According to the Ninth Circuit, the roving wiretap provision of Title III assuaged the dangers the particularity requirement sought to avoid. The statute did not permit a "wide-ranging exploratory search" and eliminated the "possibility of abuse or mistake." Title III required that law enforcement officers surveil only the telephone facilities used by an identified speaker

86. Id. at 1445 n.7.
88. Id.
89. Petti, 973 F.2d at 1445 ("[T]he district court correctly found the provision permitting roving wiretaps to be constitutional.").
90. Id. at 1444 (quoting U.S. CONST. amend. IV).
91. Id.
92. Id. at 1445.
93. Id.
and employ "minimization procedures to ensure that only conversations relating to a crime in which the speaker is a suspected participant are intercepted." In addition, a roving wiretap could be obtained only where the government could convince a court that the suspect purposefully thwarted interception by changing communication facilities. Given these safeguards, the roving, as well as fixed, wiretap interceptions under Title III did not constitute a "greater invasion of privacy than necessary to meet the legitimate needs of law enforcement."96

C. A Comparison of Roving Wiretaps Under Section 206 and Title III

In 2002, the United States Foreign Intelligence Surveillance Court of Review (the "FISA Court of Review") considered whether FISA, as amended by section 206 of the Patriot Act permitting roving wiretaps, passes constitutional muster under the Fourth Amendment. Significant to the analysis was the similarity between the roving wiretap provisions of Title III and FISA. The FISA Court of Review compared FISA with Title III with respect to the three traditional requirements for reasonableness under the Fourth Amendment: (1) a warrant issued by a detached, neutral magistrate, (2) probable cause to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense, and (3) a particular description of the things to be seized and the place to be searched.

As to the first requirement, both FISA and Title III "require prior judicial scrutiny of an application for an order authorizing

94. Id.
95. See id.
97. The United States appeals unfavorable rulings from the FISA Court to the FISA Court of Review. See 50 U.S.C. § 1803(b) (2000) (establishing the FISA Court of Review).
99. Id. at 737 ("[I]n asking whether FISA procedures can be regarded as reasonable under the Fourth Amendment, we think it is instructive to compare those procedures and requirements with their Title III counterparts.").
100. Id. at 738 (discussing Fourth Amendment reasonableness standard) (citations and quotations omitted).
electronic surveillance."101 Moreover, prior precedent has established that a FISA judge is a neutral and detached magistrate.102

Moving to the second requirement, Title III and FISA differ in their respective showings of probable cause necessary to obtain a roving wiretap.103 Under Title III, the government must demonstrate probable cause "that an individual is committing, has committed, or is about to commit" a specified predicate offense.104 "FISA by contrast requires a showing of probable cause that the target is a foreign power or an agent of a foreign power."105 A U.S. person106 cannot be "an agent of a foreign power" without a showing of criminal activity unless that person is engaged in espionage and clandestine intelligence activities of a foreign power.107 In that case, the government need only show that the person's activities "may involve a violation of the criminal statutes of the United States."108

Congress lowered the probable cause standard in espionage and clandestine intelligence cases involving a U.S. person because "it was fully aware that such foreign intelligence crimes may be particularly difficult to detect."109 Notably, this lower standard does not apply in other FISA areas (e.g., terrorism investigations). In addition, even in the U.S. person espionage case, FISA, but not Title III, requires a probable cause showing that the target is acting "for or on behalf of a foreign power."110 Without a probable cause showing that the person is an agent of a foreign power, FISA forbids use of a roving wiretap. Further, "no U.S. person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States."111 Title III does not contain any First Amendment exceptions.112

101. Id.
102. Id.
103. Id.
105. Sealed Case, 310 F.3d at 738 (citing 50 U.S.C. § 1805(a)(3)).
107. 50 U.S.C. § 1801(b)(2); Sealed Case, 310 F.3d at 738.
108. Sealed Case, 310 F.3d at 738.
109. Id. at 739.
110. 50 U.S.C. § 1801(b)(2); Sealed Case, 310 F.3d at 739.
111. 50 U.S.C. § 1805(a)(3)(A) (2000); Sealed Case, 310 F.3d at 739 (listing examples where FISA would not permit a roving wiretap).
Thus, "FISA applies only to certain carefully delineated, and particularly serious, foreign threats to national security."113

The particularity requirements of Title III and FISA likewise pertain to different aspects of the interception of communications. One aspect is the nexus between the facility and the communications coming across that facility. "Title III requires probable cause to believe that particular communications concerning the specified crime will be obtained through the interception."114 On the other hand, FISA "requires an official to designate the type of foreign intelligence information being sought, and to certify that the information sought is foreign intelligence information."115 A national security officer, typically the FBI Director, must make, and the Attorney General or the Attorney General's Deputy must approve, this certification.116 "When the target is a U.S. person, the FISA judge reviews the certification for clear error"117—a standard lower than a probable cause finding by a judge reviewing a Title III application. Another aspect of particularity that differs between the two statutes is the connection between the target and the pertinent communications. Generally, Title III requires probable cause to believe that the facilities subject to surveillance are either (a) "being used or are about to be used in connection with the commission of a crime,"118 or (b) "are leased to, listed in the name of, or used by the individual committing the crime."119 In the former situation, Title III requires only that an individual, not necessarily the target, use the facility in connection with a crime.120 Under a roving wiretap, Title III permits only the interception of conversations to which a targeted individual is a party.121 In contrast, FISA requires a showing of probable cause to believe that the target (i.e., the foreign power or agent) is using, or about to use, "each of the facilities or places at which the surveillance is directed."122 Ordinarily, "FISA requires less of a nexus between the facility and the pertinent communications

113. Id.
114. Sealed Case, 310 F.3d at 739 (citing 18 U.S.C. § 2518(3)(b)).
116. Sealed Case, 310 F.3d at 739; see also 50 U.S.C. § 1804(a) (2000).
117. Sealed Case, 310 F.3d at 739.
118. Id. at 739–40 (citing 18 U.S.C. § 2518(3)(d)).
119. Id.
120. Id. at 740.
122. Sealed Case, 310 F.3d at 740 (citing 50 U.S.C. § 1805(a)(3)(B)).
than Title III, but more of a nexus between the target and the pertinent communication" than does Title III.123 In the context of roving wiretaps, however, both Title III and FISA require a link between the target and the communication captured by the surveillance.

Title III and FISA are comparable in other respects as well. For example, 

"[b]oth statutes have a 'necessity' provision which requires the court to find that the information is not available through normal investigative procedures."124 With respect to the duration of the surveillance, Title III orders run for thirty days, while a FISA order for a U.S. person may last up to ninety days.125 Each statute also provides for "minimization" procedures on the information intercepted. Under Title III, agents must operate the wiretap "in such a way as to minimize the interception of communications not otherwise subject to interception."126 That is, the government may only intercept criminal conversations and must discontinue the interception when the targets engage in non-criminal conversations.127 FISA requires minimization of what is "acquired, retained, or disseminated,"128 though normally these surveillance devices intercept without interruption and agents "minimize" the communications only after they acquire them.129 The post-acquisition minimization requirements for FISA reflect the nature of intelligence investigations which often involve ambiguous and/or coded communications.130

Finally, Title III and FISA each have notice requirements of the interception of communications after surveillance has ended. Title III requires notice to the target, and the judge may order notice to other persons whose communications were intercepted.131 FISA, on the other hand, does not require notice of

123. Id.
127. Scott v. United States, 436 U.S. 128, 140 (1978) (holding that an objective standard governs the decision whether to "minimize" a conversation under Title III).
129. See Sealed Case, 310 F.3d at 740 (discussing minimization procedures under FISA).
130. See id. at 741 (quoting Scott, 436 U.S. at 140).
131. See 18 U.S.C. § 2518(8)(d) (2000); see also Sealed Case, 310 F.3d at 741.
the interception “unless the government ‘intends to enter into evidence or otherwise use or disclose’ such communications in a trial or other enumerated official proceedings.” Consequently, if evidence obtained through a FISA roving wiretap is used at a criminal proceeding, the government must provide notice of the interception to the defendant. Absent official use of the intercepted information, however, the need for secrecy in foreign intelligence matters outweighs a target’s interest in notification.

After analyzing these two statutes, the FISA Court of Review concluded that they were equivalent in “many significant respects.” The court, however, stopped short of deciding whether a FISA order for electronic surveillance satisfies the requirements of Title III. The close similarities of the two statutes helped lead the court to answer in the affirmative the dispositive question—“whether FISA, as amended by the Patriot Act, is a reasonable response based on a balance of the legitimate need of the government for foreign intelligence information to protect against national security threats with the protected rights of citizens.” According to the court, “FISA as amended is constitutional because the surveillances it authorizes are reasonable.”

The FISA Court of Review reached the correct result in permitting roving wiretaps under FISA pursuant to the Patriot Act. Certainly, if government agents can use a roving wiretap within the confines of the Fourth Amendment to investigate controlled substance offenses, the same surveillance tool should be available to the government to gather foreign intelligence to protect national security. Again, this Article focuses not so much on the normative question of whether a roving wiretap should be permitted at all but, rather, on the issue of the degree to which the Patriot Act expanded the government’s power to conduct surveillance. If a roving wiretap can be used to investigate, disrupt, and take down a cocaine distribution conspiracy composed of American citizens, then, surely, its use to investigate, disrupt, and dissemble a foreign terrorist plot to kill American citizens is justified. The differences between a roving wiretap under Title III and one under FISA are justified by the differences between

132. Sealed Case, 310 F.3d at 741 (quoting 50 U.S.C. § 1806(c)).
133. See id.
134. See id. (quoting S. REP. NO. 95-701, at 12 (1978)).
135. Id. at 741.
136. See id. at 742.
137. Id.
138. Id. at 746.
investigating a criminal enterprise and investigating the activities of a foreign power or its agents.

Congress recognized the appropriateness of using a roving wiretap in terrorist investigations when it initially enacted Title III in 1986. In discussing the standard to justify issuance of a roving wiretap, the Senate Report accompanying the Title III legislation used a terrorism investigation as an apropos application of this law enforcement tool:

[T]he application [for a roving wiretap] must show that the person committing the offense has a purpose to thwart interception by changing facilities. In these cases, the court must find that the applicant has shown that such a purpose has been evidenced by the suspect. An example of a situation which would meet this test would be an alleged terrorist who went from phone booth to phone booth numerous times to avoid interception. A person whose telephone calls were intercepted who said that he or she was planning on moving from phone to phone or to pay phones to avoid detection also would have demonstrated that purpose.139

The Patriot Act amended FISA to permit a roving wiretap in just this situation—where the court, not the government agent, determines that the target of the surveillance is changing facilities to thwart interception.140

In making roving wiretaps available in foreign intelligence investigations, Congress, in the Patriot Act, merely made available in this area a tool that government agents had long employed in certain criminal investigations. Thus, the roving wiretap provision of the Patriot Act did not expand government power but, rather, equipped national security officers with a tool that Congress had long endorsed for terrorist investigations. Given the purpose of FISA, most Americans would be surprised, if not outraged, to learn that roving wiretaps have only recently become available in foreign intelligence gathering operations.141

D. Criticisms of Section 206 of the Patriot Act

As with delayed notification search warrants, critics of the Patriot Act seek to amend, if not repeal, its provision for roving

141. See Sealed Case, 310 F.3d at 746 (stating that “FISA’s general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers, has from its outset been distinguishable from ‘ordinary crime control’”).
wiretaps. Once again, the SAFE Act is representative of such criticism. The SAFE Act seeks to eliminate so-called “John Doe” roving wiretaps under FISA—a roving wiretap that specifies neither the identity of the target, nor the specific facilities the target is using. The SAFE Act seeks to accomplish this goal by amending 50 U.S.C. § 1805(c) to require “a description of the target and the nature and location of the facilities and places at which the electronic surveillance will be directed” when “the identity of the target is not known.” Furthermore, when “the facility or place at which the surveillance will be directed is not known at the time the order is issued,” then “the surveillance [can] be conducted only when the presence of the target at a particular facility or place is ascertained by the person conducting the surveillance.”

The SAFE Act, despite its protestations to the contrary, circumscribes section 206 of the Patriot Act too greatly, at least relative to roving wiretaps under Title III. First, the SAFE Act need not address an “unknown target” situation because FISA already requires the government agent to provide either the target’s identity or description. Where the government agent does not know the target’s name, the FISA Court must receive a description of the person. A “phantom target” cannot be the subject of a roving wiretap. Moreover, once described, that person is the target of the roving wiretap, and the government agent must apply to the FISA Court for a new surveillance order if a new, different target emerges. The ability of a national security officer only to describe, but not identify, a target involved with an agent of a foreign power does not justify narrowing the scope of roving wiretaps under FISA given that the participants in such clandestine activities are typically quite adept at cloaking their identities.

The second change that the SAFE Act would make to section 206 circumscribes roving wiretaps under FISA more closely than roving wiretaps under Title III—a result that seems to be exactly opposite to the relative risks of national security investigations under FISA compared to routine criminal investigations under Title III. Surely, national security officers tasked with keeping

---

143. Id.
144. Id.
the United States free from foreign terrorist activities should be given at least the same investigative tools as law enforcement officers seeking to ferret out the local marijuana distributor. The SAFE Act, however, would permit a roving wiretap under FISA only when the government agent could ascertain with certainty that the target of the investigation is present at a particular facility or place.\textsuperscript{147} Title III is not so strict. Under Title III, a roving wiretap can be employed for "such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted."\textsuperscript{148} Title III permits an officer to analyze the facts and presume that the target is present at, or in reasonable proximity to, the facility or place to be surveilled. The SAFE Act would preclude government agents in a national security investigation from acting based on the facts and their intuition and force them to be certain of the target's presence, not just proximity, before utilizing a roving wiretap order from the FISA Court.

FISA should not be so narrowly cabined. National security concerns strongly favor broader boundaries for FISA surveillance than for Title III surveillance, but at a minimum, these boundaries should be co-extensive. Again, the normative question whether roving wiretaps should be permitted is not the issue. Rather, the point made is that the Patriot Act has merely provided national security agents with law enforcement tools that criminal investigators freely use on a daily basis without criticism and hyperbole. Critics of the Patriot Act, such as the supporters of the SAFE Act, would limit the roving wiretap provision of the Patriot Act so greatly as to make roving wiretaps under FISA less available and less effective than those issued under Title III. The logic of such a result is questionable both in jurisprudential and practical terms. For the same reasons, Congress should not sunset section 206 of the Patriot Act as scheduled on December 31, 2005, while maintaining roving wiretaps under Title III.\textsuperscript{149}

III. Seizure of Business Records

Section 215, the provision of the Patriot Act permitting the FISA Court to order the production of "any tangible thing," has attracted the ire of many critics of the legislation. In particular, critics of the Patriot Act argue that section 215 greatly expands

\textsuperscript{147} See SAFE Act, S. 1709, § 2.
\textsuperscript{149} See Patriot Act § 224 (codified at 50 U.S.C. § 2510) (delineating the provisions of the Patriot Act that are to sunset on December 31, 2005).
the authority of law enforcement officials because a person's library records are now potentially discoverable under FISA.\textsuperscript{150} A comparison of section 215 with the traditional powers of a grand jury reveals, however, that the authority of the FISA Court under the Patriot Act to compel the production of documents, including library records, is not nearly as broad as the power of a grand jury in an ordinary criminal investigation. Section 215 by its terms vests the FISA Court with significantly less power than that enjoyed by a grand jury under the common law.

A. Use of Grand Jury Subpoena To Compel Production of Records and Things

The United States Supreme Court has recognized that the "grand jury sits not to determine guilt or innocence, but to assess whether there is an adequate basis for bringing a criminal charge."\textsuperscript{151} In performing its role, the grand jury receives evidence only from the prosecutor—a venerable practice from English common law and one consistently upheld by the Supreme Court.\textsuperscript{152} The grand jury has broad investigatory powers and can consider evidence derived from a number of sources.\textsuperscript{153}

The information from these sources is generally obtained through the issuance of a subpoena requiring a person to appear to testify before, and/or to produce documents to, the grand jury. Typically, a grand jury subpoena is prepared by a prosecutor, issued by a court clerk with little or no oversight by a judge, and served by a law enforcement officer.\textsuperscript{154} Not uncommonly, a grand jury subpoena for documents permits the source of the information to deliver the documents directly to the law enforcement agent, rather than to make delivery to the grand jury.\textsuperscript{155} The agent will then report his receipt of the documents to the


\textsuperscript{152} See Williams, 504 U.S. at 51.

\textsuperscript{153} See Calandra, 414 U.S. at 344.

\textsuperscript{154} See In re Grand Jury Matters, 751 F.2d 13, 16 (1st Cir. 1984) (discussing grand jury subpoenas).

\textsuperscript{155} United States v. Nathan, 816 F.2d 230, 234 (6th Cir. 1987) (finding that a recipient of a grand jury subpoena may disclose the requested information to a government employee who then makes the disclosure to the grand jury).
grand jury and request its permission to retain the documents to further his investigation. The grand jury may never actually see the documents produced from the issuance of its subpoena, though it has the right to request their physical production.

Importantly, in the vast majority of cases, the grand jury issues its subpoenas with no judicial involvement. The court does not approve the scope or substance of the subpoena and is not informed of a source's compliance with the subpoena. Additionally, the grand jury is not limited in the type of entities from which it can request information or testimony or the type of documents to be produced. An important caveat to the foregoing principle, however, is that a grand jury cannot violate a privilege that is created by the United States Constitution, statutes, or case law (e.g., Fifth Amendment privilege against self-incrimination, attorney-client privilege). Thus, generally speaking, issuance of a grand jury subpoena is proper unless "there is no reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation," or a judge determines that the subpoena is "unreasonable and oppressive." First Amendment activities rarely, if ever, of themselves provide a defense or shield against production of documents in response to a grand jury subpoena.

Finally, a grand jury is cloaked in secrecy. Generally speaking, only the prosecutor, court reporter, and witness are permitted before the grand jury. Disclosure to the public of matters occurring before the grand jury is forbidden, except that many jurisdictions, including the federal courts, permit a witness to discuss his testimony before the grand jury.

---

156. *Calandra*, 414 U.S. at 343 (noting the lack of judicial monitoring over grand jury proceedings).

157. *See Grand Jury Matters*, 751 F.2d at 16 (noting that grand jury subpoenas are instruments of the United States Attorney's Office or some other executive branch department though they are issued in the name of the United States district court).

158. *Calandra*, 414 U.S. at 343 (discussing the types of information a grand jury may subpoena).

159. *Id.* at 346 (discussing limits on a grand jury's subpoena power).


161. *Grand Jury Matters*, 751 F.2d at 18 (quoting *FED. R. CRIM. P.* 17(c)).


163. *Id.*

164. *See id.* 6(e)(3) (discussing disclosure rules of a federal grand jury).
B. Section 215 Permits Production of Tangible Things Pursuant To Court Order

The Patriot Act expanded the power of the FISA Court to issue orders compelling the production of information, in particular business records. Prior to the Patriot Act, the FISA Court could order the production of "records" only from "a common carrier, public accommodation facility, physical storage facility or vehicle rental facility." Moreover, the government official had to certify that "there were specific and articulable facts giving reason to believe that the person to whom the records pertain was a foreign power or the agent of a foreign power." Section 215 of the Patriot Act changed both the scope of, and standard for, a court order for the production of records and documents.

Under section 215, the Director of the FBI or a designee of the Director, who cannot be ranked lower than Assistant Special Agent in Charge, "may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities." Now, the scope of the court order is not limited to "records," but can cover "any tangible thing," including any type of business record. Section 215 also eliminated the previous restriction on the type of entity from which information could be obtained and the certification requirement for the nexus between the target and the records to be produced. Presently, tangible things sought under section 215 must either (1) pertain to foreign intelligence information not concerning a United States person or (2) protect against international terrorism or clandestine intelligence activities. Section 215 is scheduled to sunset on December 31, 2005.

Unlike prior law, section 215 expressly provides for First Amendment protection against a court order for the production

---

167. Id. § 1862(b)(2)(B).
171. See Patriot Act § 224 (codified at 50 U.S.C. § 2510) (delineating the provisions of the Patriot Act that are to sunset on December 31, 2005).
of documents. In particular, section 215 prohibits the FISA Court from ordering production of documents or records for an international terrorism or clandestine intelligence investigation of a United States person based solely on "activities protected by the first amendment to the Constitution of the United States." Section 215 also requires the Attorney General to report every six months to Congress on the number of times agents have sought a court order under this section as well as the number of times such requests were granted, modified, or denied. As of the date of this writing, the FBI has yet to act upon a FISA application filed under section 215. Importantly, one constant both pre- and post-Patriot Act is that the FISA Court, not the government agent, is the authority that issues the order compelling the production of records pursuant to a foreign intelligence or terrorism investigation.

C. Criticisms of Section 215 of the Patriot Act

Like other provisions of the Patriot Act, section 215 has also been the subject of much criticism and attack. The SAFE Act exemplifies this criticism by proposing to amend section 215. In particular, the SAFE Act would reinstate the previous test to permit the FISA Court to order the production of documents, viz., the government agent must provide "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." The SAFE Act would retain the Patriot Act's expansion of the scope of a FISA Court order to "any tangible things" and to any type of entity, including libraries and bookstores. The SAFE Act's proposed modification of section 215 purportedly responds to allegations that the Patriot Act permits government

177. See 149 CONG. REC. S12,386 (daily ed. Oct. 2, 2003) (statement of Sen. Durbin) (noting that the SAFE Act "retains the expansion of the business record provision to include all business records, including library records").
ment agents to seize the library records of innocent Americans in violation of their civil liberties.\textsuperscript{178}

The proposed modification of section 215 is unjustified since an order compelling the production of documents under this section is significantly more limited in scope and frequency than a grand jury subpoena in an ordinary criminal investigation. The FBI’s ability to seek disclosure of tangible items in a national security/foreign terrorism investigation under section 215 is not as great as an ordinary law enforcement officer’s ability to seek the production of documents in routine criminal investigations. The FISA Court has significantly less authority to order the production of business records than does a grand jury. Certainly, if a grand jury can compel a library to produce the records for a patron while investigating the possible commission of a garden variety crime, the FISA Court should have the authority to order the production of these same records pursuant to a foreign terrorism or clandestine intelligence investigation under the limited circumstances set forth in section 215. Once again, the Patriot Act has not fueled Big Brother but, rather, provided national security investigators with a tool, in this case an application to the FISA Court for an order to produce documents, similar to one that criminal investigators and prosecutors have long had at their disposal in the form of a grand jury subpoena.

A FISA Court order under section 215 is more limited than a grand jury subpoena in several respects. First, as mentioned supra, a grand jury subpoena is subject to little or no judicial oversight. A grand jury is an independent body operating outside the direct purview of the judiciary. Judicial involvement, on the other hand, is an indispensable aspect of section 215, since the FISA Court is the authority that orders the production of documents. The FISA Court is free to deny the FBI’s application for an order under section 215. Second, section 215 applies only to foreign intelligence or terrorism investigations—domestic terrorism investigations, much less ordinary crimes, are categorically excluded from its domain. Of course, a grand jury has authority to issue a subpoena for the investigation of any criminal offense. Third, section 215 expressly disavows a FISA Court order in any investigation of a United States person conducted solely upon the basis of First Amendment activities.\textsuperscript{179} The First Amendment does not similarly constrain a grand jury investiga-

\textsuperscript{178} See id. at S12,387 (statement of Sen. Durbin) (“The SAFE Act would permit the FBI to obtain the records related to the suspected terrorists, but not records related to innocent Americans who are not suspected terrorists.”).

tion. Fourth, applications made under section 215 are subject to strict congressional oversight, while Congress does not scrutinize the scope and subject matter of grand jury subpoenas.

A grand jury's authority to force a public library to produce its records, a bone of considerable contention for the critics of section 215, shows that Congress, in enacting section 215, did not grant the FISA Court with a heretofore unknown power. Rather, the passage of section 215 merely gave the FISA Court a considerably more circumscribed authority to compel the production of documents in a foreign intelligence investigation relative to the subpoena power of a grand jury. Grand juries have long enjoyed the power to order a public library to produce its records, including the records of a particular patron's activities at the facility.

For example, in Brown v. Johnston, a county prosecutor was investigating certain mutilations of cattle occurring in the area.180 The prosecutor, pursuant to state law, served on a public library a subpoena duces tecum "requiring the custodian of library records to appear and present 'all records of persons who have checked out the books described in [the] State's application.'"181 The books pertained to witchcraft and related topics.182 Upon the library's receipt of the subpoena, a library patron and the library board filed suit seeking to quash it.183 The claimants argued that the subpoena contravened the state statute mandating the confidentiality of library records.184 In addition, they asserted the existence of a "library patron's privilege" and that the subpoena infringed on their privacy interests protected by the First and Fourteenth Amendments to the United States Constitution.185

The Supreme Court of Iowa rejected the claimants' arguments.186 At the outset, the court noted that a patron's right of privacy in library records must give way to the weightier public interest in effective criminal investigations.187 The court expressly found, "The county attorney's investigative authority is comparable to and in some instances in lieu of the grand jury. As such, the county attorney's investigative power must be broad

181. Id.
182. Id.
183. Id.
184. Id. at 512 (discussing the state statute requiring confidentiality of all records of a library which would reveal the identity of a patron seeking an item from the library).
185. Id.
186. See id. at 513.
187. Id. at 511–12.
to adequately discharge his public responsibility."

Moreover, the state statute cloaking library records in secrecy expressly permitted disclosure upon the order of a court. The prosecutor's subpoena duces tecum qualified as such an order.

In rejecting the claimants' constitutional arguments, the court looked to United States Supreme Court precedent on the constitutional restrictions on a grand jury's subpoena power. In particular, the court noted that the Supreme Court held in *Branzburg v. Hayes* and *United States v. Nixon* that a reporter's First Amendment privilege and the presidential executive privilege, respectively, were subordinate to the power of the grand jury in a criminal investigation. Given the Supreme Court's position on the power of a grand jury, the court, assuming arguendo that a "library-patron's privilege" exists, ruled that "[t]he State's interest in well-founded criminal charges and the fair administration of criminal justice must be held to override the claim of privilege here." Consequently, the court upheld the subpoena duces tecum and ordered the library to disclose to the county prosecutor the requested records as part of the cattle mutilation investigation. The court ordered such production of records even though "the State's investigation was only preliminary . . . no suspects [had been] identified . . . [and] the search for information was [not] limited to any named library patrons." The court was solicitous of the prosecutor's need for the information to narrow and focus his investigation.

Certainly, the government's interest in conducting foreign terrorism investigations is at least as weighty as an Iowa county prosecutor's interest in tracking down unlawful cattle killers. In fact, national security agents in foreign terrorism investigations, unlike prosecutors at the local, state, and federal levels, are limited by First Amendment concerns under section 215 of the Patriot Act from requesting a court to order businesses, including public libraries, to produce records. This feature of section 215, in and of itself, belies any argument that the Patriot Act, by permitting the forced disclosure of library records in certain cir-

188. *Id.* at 512 (citations omitted).
189. See *id*.
190. See *id*.
194. *Id.* at 513.
195. *Id*.
196. *Id*.
197. *Id*.
cumstances, greatly expanded the power of law enforcement agencies. Persons upset with the enactment of section 215 should be equally, if not more, appalled at the issuance of grand jury subpoenas in a host of criminal investigations seeking the production of a vast spectrum of private and public documents.

The Patriot Act through section 215, rather than extending the reach of law enforcement beyond pre-existing limits, has, once again, merely equipped national security agents with the ability to request the FISA Court to order the production of tangible things that a grand jury secretly conducting a routine criminal investigation could easily obtain. The logical consistency of sunsetting section 215 in light of the traditional power of grand juries is questionable at best. Though some would certainly argue otherwise, a majority of Americans would likely support granting the FISA Court—the judicial body overseeing foreign terrorism investigations—with the same quantum of the power that grand juries enjoy when investigating criminal offenses. Permitting a grand jury to compel the production of library records in the investigation of the slaying of cattle while denying the production of such records in the investigation of terrorism activities that threaten to kill thousands of American citizens seems both practically and intellectually unreasonable. Congress, in passing section 215, merely updated the power of the FISA Court in light of the real threat posed by foreign terrorists. An examination of section 215 through the prism of traditional grand jury functions shows that such congressional action was not Orwellian but, rather, a rational response to the real dangers of terrorism.

CONCLUSION

After the events of September 11, 2001, the world changed. Congress realized that the threat to U.S. citizens from foreign terrorists is real. Consequently, Congress enacted the Patriot Act. Few pieces of legislation have ever been attacked as harshly as the Patriot Act on the grounds that the statute emasculates civil liberties. The foregoing review of the provisions of the Patriot Act pertaining to delayed notification warrants, roving wiretaps, and court-ordered production of business records shows that, at least as to these three areas, critics of the Patriot Act are misguided and misinformed.

Rather than expanding the power of government to heretofore unknown levels, the Patriot Act merely allows investigators of foreign terrorism and clandestine intelligence activities to request a court to issue orders that are relatively common in ordinary criminal investigations. In these three areas, the Patriot Act
has neither created nor exacerbated Big Brother, but has only
made available to investigators tools long employed in routine
criminal matters. In fact, a true airing of the effect of these pro-
visions is more likely to draw the approval, rather than the ire,
of a majority of Americans. 198 Given the sacrifices made on and
after 9/11, Congress and our fellow citizens deserve no less than
a clear exegesis of the Patriot Act, rather than political hyper-
bole. This Article has sought to make such a presentation and
concludes that, whatever else the Patriot Act might be, in regards
to delayed notification warrants, roving wiretaps, and document
production orders, Big Brother it is not.

198. The reasonableness of the Patriot Act was noted by the 9/11 Com-
mmission charged with investigating the terrorist attacks on September 11, 2001.
In particular, the 9/11 Commission found many of the provisions of the Patriot
Act to be “relatively noncontroversial” such as those that updated the country’s
“surveillance laws to reflect technological developments in a digital age.” NAT’L
COMM’N ON THE TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION
REPORT 394 (2004). The Commission’s finding reflects the testimony of many
witnesses who appeared before it and lauded the Patriot Act as a key weapon in
the country’s arsenal against the war on terror. See Transcript: 9/11 Commission
wpdyn/articles/A9088-2004Apr13.html (on file with the Notre Dame Journal of
Law, Ethics & Public Policy) (transcribing testimony before the 9/11 Commis-
ion on April 13, 2004). In particular, former United States Attorney General
Janet Reno told the Commission that “generally everything that’s been done in
the Patriot Act has been helpful I think while at the same time maintaining the
balance with respect to civil liberties. . . .” Id. Reno did state, however, that she
would like to learn more about the current administration’s position on “FISA
searches” under section 215. Id.