FIGHTING TERRORISM IN AN ELECTRONIC AGE: DOES THE PATRIOT ACT UNDULY COMPROMISE OUR CIVIL LIBERTIES?

CHRISTOPHER P. RAAB[1]

ABSTRACT

The USA PATRIOT Act is tremendously controversial, both lauded by law enforcement and decried by civil liberties groups. This iBrief considers two of the Act's communications monitoring provisions, concluding that each compromises civil liberties to a greater degree than is necessary to combat terrorism. Accordingly, Congress should revise the USA PATRIOT Act, bringing it into line with the Constitution.

INTRODUCTION

¶1 The USA PATRIOT Act[2] seemed a popular bill. Passed less than two months after the terrorist attacks of 9/11, the bill garnered an unusual 98 yeas in the Senate, 357 in the House.[3] After all, very few lawmakers wished to be on the wrong side of legislation that was so obviously "patriotic."

¶2 Since its passage, however, the Act's popularity has been polarized. The Bush administration lauds its effectiveness, claiming that the Act "has increased our ability to share intelligence information, updated the law to adapt to changes in technology, and provided federal law enforcement agencies [with] critical tools to investigate terrorists and spies."[4] Civil liberties proponents have been less sanguine: according to the Electronic

---

[1] J.D. Candidate, 2007, Duke University School of Law; B.A. in Pre-law, 2004, Bob Jones University. The author would like to thank Professor Christopher Schroeder and Chin Pann for their assistance in writing this iBrief.

[2] USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of the United States Code). The bill's official title is "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001." Throughout this iBrief, the statute will be referred to as the "Patriot Act" or simply the "Act."

[3] 147 CONG. REC. D1053-02 (2001); 147 CONG. REC. H7224-01 (2001). The terrorist attacks occurred on September 11, 2001.

[4] OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, STATEMENT OF ADMINISTRATION POLICY: H.R. 3199—USA PATRIOT AND TERRORISM PREVENTION REAUTHORIZATION ACT OF 2005 (2005), http://www.whitehouse.gov/omb/legislative/sap/109-1/hr3199sap-h.pdf.

Frontier Foundation, "The USA PATRIOT Act broadly expands law enforcement's surveillance and investigative powers and represents one of the most significant threats to civil liberties, privacy and democratic traditions in U.S. history."[5]

¶3 Although some criticisms of the Act are unfounded, many stem from legitimate concerns. For one thing, the bill was passed without meaningful debate: in the House, members were not permitted to offer amendments, nor were most even given a chance to read the bill before being asked to vote on it.[6] Many of the provisions had been proposed previously and rejected "because of civil liberties concerns," and many of them were not limited to combating terrorism.[7] This dubious history understandably gave rise to claims that law enforcement used the hysteria surrounding 9/11 to procure a grab bag of long desired powers.[8]

¶4 Those claims of unwarranted power inspired this iBrief. The iBrief first evaluates sections 210 and 505 of the Act, which deal with the surveillance of electronic communications.[9] For each section, the law prior to the Patriot Act is discussed, along with the changes that the Act made. Next, the civil liberties implications of that provision are considered, along with any abuses that have occurred to date. The iBrief concludes that both sections infringe upon citizens' civil liberties to a degree incommensurate with their value for fighting terrorism.

¶5 The iBrief then considers the future of the Patriot Act. It discusses the current debate surrounding the Act's reauthorization and proposes improvements to both sections.

I. SECTION 210: THE SCOPE OF SUBPOENAS FOR COMMUNICATIONS RECORDS

¶6 Section 210 expands the scope of administrative and grand jury subpoenas for gathering communications records.[10] These changes infringe

---

[5] Electronic Frontier Foundation, The USA PATRIOT Act, http://www.eff.org/patriot (last visited Jan. 25, 2006).

[6] *See* 147 CONG. REC. H7159, 7206 (2001) ("This bill, ironically, which has been given all of these high-flying acronyms, it is the PATRIOT bill, it is the U.S.A. bill, it is the stand up and sing the Star Spangled Banner bill, has been debated in the most undemocratic way possible, and it is not worthy of this institution [Representative Barney Frank].").

[7] Robert O'Harrow, Jr., *Six Weeks in Autumn*, WASH. POST, Oct. 27, 2002, at W06.

[8] *Id.*

[9] For the purposes of this iBrief, "electronic communications" refers to the use of telephones, cellular phones, e-mail, and the Internet.

[10] USA PATRIOT Act of 2001, § 210, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of the United States Code). Communications

upon civil liberties by making sensitive personal information available to the government with few or no procedural safeguards. Although these expanded subpoenas may have some value for fighting terrorism, their widened scope unnecessarily compromises civil liberties.

A. Subpoenas pre-Patriot Act

¶7 An administrative subpoena is issued by a government agency to compel an individual to testify or to produce documents that will aid the agency in the performance of its duties.[11] Although administrative subpoenas are issued without judicial oversight, the Supreme Court has consistently held them to be constitutional so long as they meet basic criteria such as reasonableness and specificity.[12] Traditionally, administrative subpoenas have been used by administrative agencies, not by law enforcement; however, federal statutes authorize their use in certain criminal cases concerning "health care fraud, child abuse, Secret Service protection, controlled substances cases, and Inspector General investigations."[13] Additionally, states may also grant administrative subpoena power to their own agencies via state statutes.[14]

¶8 Like administrative subpoenas, grand jury subpoenas are used to compel the production of evidence or testimony, and are valid unless

---

records are those kept by phone companies and Internet service providers ("ISPs"). They typically contain a subscriber's name, address, and billing information, as well as other information, such as telephone connection records or length of time online. *See* 18 U.S.C. § 2703(c)(2) (2000).

[11] CHARLES DOYLE, CRS REPORT FOR CONGRESS, ADMINISTRATIVE SUBPOENAS AND NATIONAL SECURITY LETTERS IN CRIMINAL AND FOREIGN INTELLIGENCE INVESTIGATIONS: BACKGROUND AND PROPOSED ADJUSTMENTS (2005), *available at* http://www.fas.org/sgp/crs/natsec/RL32880.pdf; Lara Flint, *Administrative Subpoenas for the FBI: A Grab for Unchecked Executive Power*, CTR. FOR DEMOCRACY & TECH., Sept. 24, 2003, http://www.cdt.org/security/usapatriot/030924cdt.shtml.

[12] *See* Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 208 (1946) (holding that neither the Fourth Amendment nor the Fifth Amendment's protection against self-incrimination creates an obstacle to the enforcement of a reasonable administrative subpoena); *see also* United States v. Powell, 379 U.S. 48, 57–8 (1964) (holding that no standard of probable cause must be met to issue a valid administrative subpoena).

[13] DOYLE, *supra* note 11, at Summary.

[14] *See* 18 U.S.C. § 2703(c)(2) (2000); *see also, e.g.,* DEBORAH K. MCKNIGHT, MINNESOTA HOUSE OF REPRESENTATIVES RESEARCH DEPARTMENT, INFORMATION BRIEF: ADMINISTRATIVE SUBPOENAS 2, 5–9 (2005) (listing the various Minnesota agencies with administrative subpoena power), *available at* http://www.house.leg.state.mn.us/hrd/pubs/adminsup.pdf.

unreasonable or oppressive.[15] Despite the name, a grand jury does not actually issue the subpoena; rather, grand jury subpoenas are issued by the court clerk after being filled out by the prosecutor.[16] The prosecutor uses these subpoenas to marshal evidence in front of the grand jury while seeking an indictment.[17] The scope of the grand jury's subpoena is virtually unlimited: "[T]he grand jury 'can investigate merely on suspicion that the law is being violated, or even because it wants assurance that it is not.' It need not identify the offender it suspects, or even 'the precise nature of the offense' it is investigating."[18]

¶9 Prior to the Patriot Act, federal law limited the amount of information that the government could obtain from a communications company by means of an administrative or grand jury subpoena.[19] Under section 2703(c) of Title 18 of the United States Code, subpoenas could only be used to obtain basic information, such as a subscriber's name, address, length of service, and records of numbers called and received.[20] If additional information was required, the government needed to obtain a warrant, a court order, or the subscriber's consent.[21]

B. Subpoenas post-Patriot Act

¶10 The Patriot Act made several changes with regard to acquiring communications records by administrative or grand jury subpoena. The previous law was written with telephones in mind; now the law makes clear that all electronic communications are covered, including the Internet.[22] Thus, in addition to telephone connection records, a subpoena will also apply to "records of session times and durations."[23] The provision dealing with the disclosure of telephone numbers has also been modernized—it now

---

[15] DOYLE, *supra* note 11, at 12–13.
[16] Susan Brenner & Lori Shaw, *Federal Grand Juries*, U. DAYTON SCH. L., http://www.udayton.edu/~grandjur/faq/faq9.htm, (last visited Jan. 25, 2006).
[17] DOYLE, *supra* note 11, at 12.
[18] United States v. Williams, 504 U.S. 36, 48 (1992) (internal citations omitted).
[19] *See* § 2703(c)(2); *Field Guidance on New Authorities that Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, DEP'T OF JUST. [hereinafter *Field Guidance*], http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last visited Jan. 25, 2006).
[20] § 2703(c)(2) (prior to amendment by the Patriot Act). In the context of this iBrief, the word "subpoena" refers solely to an administrative or grand jury subpoena.
[21] § 2703(c)(1). See also § 2703(c)(1)(D), which provides a limited exception to provisions (A) through (C) when the subscriber is engaged in telemarketing fraud.
[22] *See* § 2703(c)(2).
[23] *Id*.

covers "temporarily assigned network address[es]," as well.[24] The Act also permits the government to request payment information by subpoena, including "any credit card or bank account number."[25]

C. Subpoenas and Civil Liberties

¶11 In a recent document titled "Report from the Field: The USA Patriot Act at Work," the Department of Justice ("DoJ") offers real life examples of how the Patriot Act has been used to protect American citizens.[26] The report gives five examples illustrating the effectiveness of section 210.[27] In four instances, the law was used to obtain convictions for child pornography or child molestation;[28] in one case, section 210 was used to prevent a "Columbine-like attack" on a school.[29] The report sums up the impact of section 210 as follows:

> [I]n section 210 . . . Congress authorized the use of administrative and grand-jury subpoenas to obtain [communications] information . . . without requiring investigators first to undertake the time-consuming step of applying to the courts. (As is true of all subpoenas, recipients of a section 210 subpoena are free to go to court to quash it.) The speedy acquisition of this information has allowed authorities to identify perpetrators more easily and keep pace with terrorists and other criminals.[30]

¶12 Essentially, the DoJ's position is that by eliminating the necessity of a warrant, section 210 permits law enforcement personnel to find and prosecute criminals more effectively.[31] The DoJ's praise for section 210 has

---

[24] *Id.*
[25] *Id.*
[26] DEP'T OF JUST., REPORT FROM THE FIELD: THE USA PATRIOT ACT AT WORK (2004) [hereinafter REPORT], *available at* http://www.lifeandliberty.gov/docs/071304_report_from_the_field.pdf.
[27] *Id.* at 19–20. For additional information regarding the government's use of section 210, see DEP'T OF JUST., OFFICE OF LEGISLATIVE AFFAIRS, REPLY TO APRIL 1, 2003 LETTER FROM THE HOUSE COMMITTEE ON THE JUDICIARY 22 (2003) [hereinafter REPLY 2003], *available at* http://www.lifeandliberty.gov/subs/congress/hjcpatriotwcover051303final.pdf ("[T]his new subpoena authority has allowed for quick tracing of suspects in numerous important cases, including several terrorism investigations and a case in which computer hackers attacked over fifty government and military computers.").
[28] *Id.*
[29] *Id.* at 19.
[30] *Id.* at 18–19.
[31] *See* REPORT, *supra* note 26, at 18–19. Implicit in this claim, of course, is the assumption that communications information is special—that police are unable to identify or keep pace with terrorists and criminals unless permitted to access

some merit. Without a doubt, section 2703 needed to be updated to encompass computer communications. To fight terrorism in an electronic age, the law must keep pace with technology. To the extent that section 210 brought technology and the law into alignment, the amendment was necessary and appropriate.

¶13 However, section 210 did more than simply apply communications law to the Internet. Several changes granted the government expanded powers, powers that have caused concern among civil libertarians. First, section 210 places payment information (such as bank account and credit card numbers) within the purview of a governmental subpoena.[32] This is disturbing because neither administrative nor grand jury subpoenas require a warrant or probable cause.[33] With identity theft on the rise, any law that expands access to citizens' account numbers should be viewed with caution, especially one as broad as section 210.[34]

¶14 The DoJ contends that access to account numbers is necessary, since "[i]n many cases, users register with Internet service providers using false names. In order to hold these individuals responsible for criminal acts committed online, the method of payment is an essential means of determining true identity."[35] There are, however, less intrusive solutions to that problem. For example, the law could require that the name and address listed on a communications account match the name and address associated with the source of payment.[36] Alternatively, section 210 could be worded to provide the government with the name and address associated with

---

their communications information free from the burdens of a warrant. Otherwise, the DoJ's argument would seem to attack the use of warrants in general, since all crime could be fought more effectively absent warrant requirements. The Fourth Amendment was designed to protect civil liberties. This and other constitutional protections represent a calculated balance intended to protect our valued liberties, even if preserving those liberties is sometimes at the expense of efficient law enforcement.

[32] 18 U.S.C. § 2703(c)(2)(F) (2000).

[33] *See* REPORT, *supra* note 26, at 18.

[34] Since 18 U.S.C. § 2703(c)(1) permits *any* governmental entity (state or federal) with subpoena power to view this billing information, the number of people with access to it is necessarily quite large. Permitting the disbursement of sensitive financial information to this large class of people without any judicial oversight or showing of probable cause is a recipe for abuse. See MCKNIGHT, *supra* note 14, at 5–9, for a list of the agencies with administrative subpoena power in just one state.

[35] *Field Guidance, supra* note 19.

[36] *E.g.,* a phone line registered to John Smith could not be paid for with a credit card (or check) belonging to Jane Doe.

payment, but not the account numbers themselves.[37] Either of those options would achieve the desired result (identifying the true users of the communications services) without compromising citizens' payment information absent a showing of probable cause.

¶15 Second, the DoJ is misguided when it asserts that the ability to contest a subpoena in court is an adequate safeguard to abuse.[38] After all, these subpoenas are issued to communications companies, not to the individual whose information is being requested.[39] The company has full immunity if it complies with the subpoena,[40] and therefore very little incentive to protest. It is unlikely that many companies in such a position would spend money on a lawyer to keep a customer's information private.[41]

¶16 The third problem with section 210 is that its actual utility for fighting terrorism is unclear. If the section were useful in accomplishing that goal, one would expect the DoJ to publicize that fact. Yet if the July 2004 "Report from the Field" is any indication, section 210 has been of far more value for rounding up sexual predators than suspected terrorists.[42] While such individuals are reprehensible and should be apprehended, such use alone is not sufficient justification for a power billed as "Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."[43] Far more evidence of its usefulness is needed to justify section 210's continued existence under the guise of a tool for fighting terrorism.[44]

¶17 Because section 210 is unnecessarily broad, lacks adequate procedural safeguards, and is of unknown value for fighting terrorism, Congress should revisit and substantially revise that provision.

---

[37] Of course, the government could access any account numbers that it truly needed by procuring a warrant.

[38] *See* REPORT, *supra* note 26, at 18.

[39] Flint, *supra* note 11.

[40] 18 U.S.C. § 2703(e) (2000).

[41] *See* Flint, *supra* note 11.

[42] *See* REPORT, *supra* note 26, at 19–20. Of the five cases mentioned, four involved sexual predators; only one (a Columbine-like attack on a school) was even remotely terrorist-related. *Id.*

[43] *See* USA PATRIOT Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of the United States Code).; s*ee also* O'Harrow, *supra* note 7 (noting that some provisions of the Patriot Act granted powers that law enforcement officers had desired for years).

[44] One of the chief rationales for giving law enforcement special powers to fight terrorism is that terrorists are highly mobile and extremely lethal. Other kinds of criminals don't embody that special combination. When ordinary protections of civil liberties are suspended in the name of fighting terrorism, such suspensions ought to actually help fight terrorism. Utility for fighting other crimes is irrelevant, since the protections were not suspended under the pretext of fighting those other crimes.

II. SECTION 505: NATIONAL SECURITY LETTERS

¶18 Section 505 of the Patriot Act[45] has proved silent but powerful. The little known provision titled "Miscellaneous National Security Authorities" altered the standard of proof necessary for issuing National Security Letters ("NSLs").[46] NSLs are information-gathering devices that allow the government to access phone and e-mail records, financial information, and lists of Internet sites visited.[47] Although much more attention has been given to section 215, the so-called "library records" provision, these new and improved NSLs have become the government's tool of choice,[48] issued at a rate of more than 30,000 a year.[49] The prolific use of NSLs represents the most egregious instance of abuse to date under the Patriot Act.

A. National Security Letters pre-Patriot Act

¶19 National Security Letters were first created in the late 1970s to aid agents in gathering foreign intelligence data.[50] As with administrative subpoenas, NSLs allow an agency to demand certain information to aid in its investigations without obtaining a warrant.[51] Unlike administrative subpoenas, however, NSLs are typically the tool of law enforcement agencies (like the FBI); furthermore, the recipient of an NSL is prohibited from disclosing its existence to any person.[52] Statutes authorize the use of NSLs to obtain information from financial institutions, communications providers, and credit agencies.[53]

---

[45] USA PATRIOT Act § 505.
[46] *Id*.
[47] Hope Yen, *FBI Use of Patriot Act Concerns Lawmakers,* WASH. POST, Nov. 6, 2005.
[48] *See* DEP'T OF JUST., OFFICE OF LEGISLATIVE AFFAIRS, REPLY TO JUNE 12, 2002 LETTER FROM THE HOUSE COMMITTEE ON THE JUDICIARY 4 (July 26, 2002), *available at* http://www.epic.org/privacy/terrorism/usapatriot/foia/doj_submission1.pdf ("If the FBI were authorized to obtain . . . information [from a library or bookstore] the more appropriate tool for requesting electronic communication transactional records would be a National Security Letter (NSL).").
[49] Barton Gellman, *The FBI's Secret Scrutiny: In Hunt for Terrorists, Bureau Examines Records of Ordinary Americans*, WASH. POST, Nov. 6, 2005, at A01, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/11/05/AR2005110501366.html; Yen, *supra* note 47.
[50] Gellman, *supra* note 49.
[51] Flint, *supra* note 11.
[52] 18 U.S.C. § 2709(c) (2000).
[53] 18 U.S.C. § 2709 (Electronic Communications Privacy Act); 12 U.S.C. § 3414 (2000) (Right to Financial Privacy Act); 15 U.S.C. § 1681(u)–(v) (2000) (Fair Credit Reporting Act); 50 U.S.C. § 436 (2000) (permits use of NSLs to investigate leaks of classified information).

¶20 Congress conferred the first NSL authority via the Right to Financial Privacy Act of 1978.[54] The creation of NSLs reflected Congress's attempt "to protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity."[55] When Congress passed the Electronic Communications Privacy Act in 1986,[56] those same considerations led to the inclusion of NSL authority in section 2709 of title 18 of the U.S. Code.[57]

¶21 Prior to the passage of the Patriot Act, all NSLs required the approval of the director of the FBI or one of his deputy assistant directors.[58] For an NSL to be valid, the approving official was required to certify in writing that the "records sought are relevant to an authorized foreign counterintelligence investigation; and [that] there are specific and articulable facts giving reason to believe that the person or entity [whose information is being requested] is a foreign power or an agent of a foreign power."[59] If the subject of the investigation was not a foreign agent, then "specific and articulable facts" were needed to demonstrate that the person was in communication with an individual or government engaged in international terrorism.[60] Thus, an NSL could only be used if a high-ranking FBI official could cite specific and articulable facts giving him reason to believe that the person subject to the search was either a terrorist or a spy, or else in communication with one.

B. National Security Letters post-Patriot Act

¶22 Section 505 of the Patriot Act altered the procedure for issuing NSLs to obtain records from communications services, financial providers, and credit agencies.[61] The Act made three alterations or additions to the existing law.[62]

---

[54] DOYLE, *supra* note 11, at 19; Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3706 (1978).
[55] H.R. Rep. 95-1383, at 28, *reprinted in* 1978 U.S.C.C.A.N. 9273, 9305.
[56] Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1867 (1986).
[57] Doe v. Ashcroft, 334 F. Supp. 2d 471, 480 (S.D.N.Y. 2004). Because this iBrief focuses only on Patriot Act provisions affecting electronic communications, the Act's effect on section 2709 will be the sole subject of the following discussion. *See infra*, note 62.
[58] DOYLE, *supra* note 11, at 22 n.75 (quoting 18 U.S.C. 2709(b)(1) prior to amendment by the USA PATRIOT Act).
[59] *Id.*
[60] *Id.*
[61] USA PATRIOT Act of 2001, § 505, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified in scattered sections of the United States Code). The Patriot Act standardized the language of the various NSL statutes, making them identical.

¶23 First, approval power has been extended beyond the FBI director or his deputy to include designees of the director.[63] A designee may be either a person at the Bureau's headquarters or one of the Special Agents in charge of a field office.[64]

¶24 Second, the Patriot Act eliminated the requirement that the subject of an NSL be a foreign agent or in communication with a foreign agent.[65] Instead, the Act merely requires relevance "to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[66] Furthermore, this "relevance" is not judicially assessed, but simply asserted by the issuing official.[67]

¶25 Third, to counteract the removal of the "foreign agent" requirement, the amendment mandated that no United States person is to be investigated "solely on the basis of activities protected by the first amendment."[68]

C. National Security Letters and Civil Liberties

¶26 Whether the government has abused its newly strengthened NSL powers is difficult to evaluate, since recipients of the letters are prohibited from speaking about them. According to "unnamed government sources," the FBI issues more than 30,000 NSLs yearly, a number that the Justice Department would neither confirm nor deny.[69] If true, such a number would represent a "hundred-fold increase over historic norms."[70] As of May 13, 2003, the Justice Department reported that no litigation had resulted from the issuance of an NSL.[71] Since that time, however, two cases have emerged that provide some insight into the workings and the constitutionality of NSLs. Appeals of both cases were heard by the U.S. Court of Appeals for the Second Circuit on November 2, 2005; neither appeal had yet been decided as of the publication of this iBrief.[72]

Thus, although this iBrief focuses on 18 U.S.C. § 2709, the same analysis applies to the other statutes. The Act did not, however, change 50 U.S.C. § 436, which authorizes NSLs to investigate leaks of classified government information.

[62] DOYLE, *supra* note 11, at 22 & n.75.

[63] *Id.*

[64] *Id.*

[65] *Id.* at 22.

[66] *Id.* at 22 n.75.

[67] 18 U.S.C. § 2709(b) (2000).

[68] DOYLE, *supra* note 11, at 22 & n.75; § 2709(b)(1).

[69] Yen, *supra* note 47; *see also* Gellman, *supra* note 50.

[70] *Id.*

[71] REPLY 2003, *supra* note 27, at 4.

[72] Alison Leigh Cowan, *Judges Question Patriot Act in Library and Internet Case*, N.Y. TIMES, Nov. 3, 2005, at B5.

¶27 In *Doe v. Ashcroft*, a New York Internet service provider ("ISP") sued the FBI, claiming that the NSL it had received violated its First, Fourth, and Fifth Amendment rights.[73] The plaintiff attacked section 2709 as unconstitutional, both facially and "as applied to the facts of this case."[74] The ISP's chief contentions were that, "first, [section] 2709 gives the FBI extraordinary and unchecked power to obtain private information without any form of judicial process, and, second, that [section] 2709's non-disclosure provision burdens speech categorically and perpetually, without any case-by-case judicial consideration of whether that speech burden is justified."[75]

¶28 The District Court held "that [section] 2709 violates the Fourth Amendment because, at least as currently applied, it effectively bars or substantially deters any judicial challenge to the propriety of an NSL request."[76] The court held that such a challenge was essential to "vindicate important rights guaranteed by the Constitution."[77] The court additionally held that section 2709(c), which indefinitely prohibits disclosure of its receipt to "any person" (presumably even an attorney), was a "prior restraint on speech in violation of the First Amendment."[78] Because it found this provision to be inseparable from the remainder of section 2709, the court held the entire section to be facially unconstitutional.[79] Accordingly, the court granted the plaintiff's request for summary judgment and enjoined the government from issuing any more NSLs under section 2709.[80]

¶29 *Doe v. Gonzales* addresses NSLs in the context of a suit filed by a library in Connecticut.[81] Doe brought suit after receiving an NSL that demanded "any and all" information associated with a specific library computer over a particular period of time.[82] In addition to the basic constitutional arguments, Doe's suit alleged that the gag orders imposed by

---

[73] Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004).
[74] *Id.* Legal doctrine allows challenges to a law as either patently unconstitutional on its face or as unconstitutional in the specific circumstances presented by the case. Succeeding with the former challenge would strike down the law in its entirety, while succeeding with the latter would hold the law inapplicable to the specific circumstances presented by the case at hand.
[75] *Id.*
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *Id.* at 475.
[80] *Id.* at 527. The court stayed its prohibition of the government's use of NSLs pending appeal.
[81] Doe v. Gonzalez*,* 386 F. Supp. 2d 66 (D. Conn. 2005). For information regarding Doe's actual identity, see Gellman, *supra* note 49.
[82] *Gonzales,* 386 F. Supp. 2d at 70; *see also* Doe v. Gonzalez, 126 S. Ct. 1, 2 (2005).

section 2709(c) caused him "irreparable harm" by denying him an opportunity to participate in the public debate surrounding the renewal of the Patriot Act.[83] He accordingly sought a preliminary injunction lifting the gag order.[84]

¶30 The District Court in *Gonzales* found that Doe had indeed suffered irreparable injury.[85] The court found section 2709(c) to be a prior restraint on speech, and thus valid under the First Amendment only if the government could demonstrate "that the law is narrowly tailored to meet a compelling state interest."[86] Although the court considered the government's interests in national security and in fighting terrorism, it found that there was no evidence in the record to demonstrate that keeping Doe's identity a secret was necessary for national security purposes.[87] Accordingly, the court found section 2709(c) to be unconstitutional and granted Doe's requested injunction.[88]

¶31 These cases highlight the three primary problems with NSLs in the wake of the Patriot Act. First, NSLs provide no meaningful opportunity for judicial review. No review is called for in the statute; in fact, the wording of section 2709 seems to indicate that the recipient may tell no one, not even a lawyer or a judge, of the NSL's existence. According to the *Ashcroft* court, this utter lack of judicial review violates the Fourth Amendment's prohibition against unreasonable searches and seizures.[89] The fact that only two NSLs have been contested over the last four years—out of a possible 120,000 served[90]—demonstrates the magnitude of this problem. Even if the statute *can* be read to allow for judicial review, NSL recipients are obviously unaware that they have the ability to contest the security letters in court. Either that, or 119,998 of the letters served were valid and reasonable.

---

[83] *Gonzales*, 386 F. Supp. 2d at 70; *see also Gonzales,* 126 S. Ct. at 2.
[84] *Gonzales,* 386 F. Supp. 2d at 69.
[85] *Id.* at 72.
[86] *Id.* at 74–75.
[87] *Id.* at 82.
[88] *Id.* The injunction was stayed by the District Court pending the government's appeal to the Second Circuit. *Id.* at 83. The plaintiff appealed that stay to the Supreme Court; however, Justice Ginsburg found vacatur to be unwarranted, since 1) the appeal was already being expedited, and 2) the gag order only applied to Doe—the American Library Association, of which Doe was a member, was free to disclose that one of its members had received an NSL. *See Gonzales,* 126 S. Ct. at 3–4.
[89] Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004).
[90] The figure of 120,000 is an estimate, reached by multiplying the commonly reported figure of 30,000 NSLs per year by the four years since the Patriot Act's passage.

¶32 Second, the gag order contained in section 2709(c) is unconstitutionally broad. Both the *Ashcroft* and *Gonzales* courts held the provision to be unconstitutional, since it categorically prohibits NSL recipients from exercising their First Amendment right to free expression, regardless of the threat posed by their speech.[91] Although there might be times when a gag order would be appropriate, that determination should be made on a case-by-case basis, and such an order should be narrowly tailored. In its present form, section 2709(c) removes essential freedoms from many more people than is necessary to combat terrorism. For that reason alone, it ought to be rejected.

¶33 The third problem with NSLs post-Patriot Act is that the standard for issuing one is extremely low.[92] What was once a tool used for tracking spies is now being used to sweep up data on ordinary citizens, people who just happen to use the same library computer terminal as someone under investigation. This would be bad enough if irrelevant information were simply discarded, as was formerly the case; now, however, FBI guidelines permit this information to be retained indefinitely and shared with other government agencies.[93] When such unbridled discretion is combined with secrecy and a lack of judicial review, the result is a recipe for abuse. While they may be useful for fighting terrorism, the FBI's NSL powers are far too great. Congress should curtail these abuses by providing appropriate protections for citizens' First and Fourth Amendment freedoms.

III. THE FUTURE OF THE PATRIOT ACT

¶34 As 2005 drew to a close, considerable drama surrounded the Patriot Act. Initially, the Act's drafters set sixteen of its most controversial provisions to expire on December 31, 2005, if not renewed by Congress.[94] Thus, Congress was already gearing up for a debate when several events brought reauthorization to the forefront of the national consciousness.

---

[91] *Ashcroft*, 334 F. Supp. 2d at 475; *Gonzales*, 386 F. Supp. 2d at 82.

[92] NSLs have always been intrusive and secretive. Prior to the Patriot Act, however, the "foreign agent" requirement in 18 U.S.C. § 2709(b) ensured that very few of those receiving NSLs would be American citizens. By removing the "foreign agent" requirement, the Patriot Act lessened the standard for issuing NSLs, leading to their prolific use. What was once a reasonable tool for gathering foreign intelligence data has become an easy way to acquire sensitive information on American citizens.

[93] Gellman, *supra* note 49.

[94] Electronic Privacy Information Center, USA PATRIOT Act Sunset, http://www.epic.org/privacy/terrorism/usapatriot/sunset.html (last visited Jan. 25, 2006). Neither section 210 nor section 505 is among the number that sunset. *Id.*

A. Possible Abuses of the Patriot Act

¶35 On October 24, the Electronic Privacy Information Center ("EPIC") sent an open letter to the Senate Judiciary Committee alleging FBI abuses of Patriot Act powers.[95] EPIC, a civil liberties watchdog group with an emphasis on electronic communications, filed a Freedom of Information Act ("FOIA") request with the FBI in March 2005 asking for records regarding the Bureau's use of a number of Patriot Act powers.[96] EPIC hoped to use the information uncovered to participate in the Congressional hearings on the Patriot Act that were scheduled for that spring.[97] In October, the FBI released a small number of the requested records.[98] In EPIC's words: "The documents reveal thirteen cases in 2002–2004 in which the FBI's Office of General Counsel investigated alleged FBI misconduct during intelligence activities, and reported these matters to the Intelligence Oversight Board (IOB). It appears from the case numbers assigned to each matter that the FBI reported to the IOB at least 153 instances of alleged misconduct occurring in 2003 alone."[99]

¶36 Not all of the alleged violations were serious—many of them hinged upon agents' failure to keep their paperwork up to date.[100] Yet others were more substantive: "[A]ccording to the AP, the violations included an alleged violation of bank privacy laws . . . improper physical

---

[95] Letter from the Electronic Privacy Information Center to the Senate Judiciary Committee (Oct. 24, 2005) [hereinafter Senate Letter], http://www.epic.org/privacy/terrorism/usapatriot/judiciary_102405.pdf.

[96] Letter from the Electronic Privacy Information Center to David Hardy, Chief of the FBI's Record/Information Dissemination Section (March 29, 2005), http://www.epic.org/privacy/terrorism/usapatriot/sunset_request.pdf.

[97] Electronic Privacy Information Center, The USA PATRIOT Act, http://www.epic.org/privacy/terrorism/usapatriot (last visited Jan. 25, 2006).

[98] Electronic Privacy Information Center, Freedom of Information Documents on the USA PATRIOT Act, http://www.epic.org/privacy/terrorism/usapatriot/foia (last visited Jan. 25, 2006). Although the FBI agreed to expedite EPIC's request, it did not release any documents until October, months after the Congressional debates were over and after both houses of Congress had already drafted their reauthorization bills. In November, a federal judge found that "[the FBI's] efforts [had] been unnecessarily slow and inefficient" and ordered the agency to release the remainder of the documents at the rate of 1,500 pages every fifteen days. Electronic Privacy Information Center v. Department of Justice, No. 05-845 (D.D.C. Nov. 16, 2005) (memorandum order), *available at* http://www.epic.org/privacy/terrorism/usapatriot/kessler_order.pdf.

[99] Senate Letter, *supra* note 95.

[100] Terry Frieden, *Watchdog Says FBI Violated Surveillance Rules,* CNN.COM, Oct. 25, 2005, http://www.cnn.com/2005/LAW/10/25/2fbi.surveillance.

search, and improper collection of e-mails after warrants expired."[101] More importantly, the revelations flew in the face of the DoJ's repeated assurances that "there had been no abuses of PATRIOT Act authority."[102] In the words of David Sobel, EPIC's general counsel, "We're seeing what might be the tip of the iceberg at the FBI and across the intelligence community. . . . It indicates that the existing mechanisms do not appear adequate to prevent abuses or to ensure the public that abuses that are identified are treated seriously and remedied."[103]

B. The Patriot Act Debate

¶37 It was in this climate of mistrust that debate over the Act's reauthorization began in earnest. That debate was punctuated by a sense of urgency from both sides. Those in favor of the Act urged Congress to reauthorize the law quickly lest any of its valuable provisions be allowed to lapse;[104] those opposed pointed to the recent allegations of FBI abuse and called for a public reckoning.[105]

¶38 Both the House and Senate passed reauthorization bills, which were sent to a joint conference committee to reconcile the two proposals.[106] In the area of civil liberties, the Senate version seemed preferable to that of the House: while the Senate made some efforts to rein in certain governmental powers, the House used the reauthorization process to grant additional ones, including a seemingly extraneous provision making it easier for prosecutors to seek the death penalty in certain cases.[107]

---

[101] *Id.*

[102] Senate Letter, *supra* note 95 ("Attorney General Alberto Gonzalez testified on April 27 that '[t]here has not been one verified case of civil liberties abuse' arising from PATRIOT Act authority. FBI Director Robert Mueller agreed: 'I as well am unaware of any substantiated allegation that the government has abused its authority under the PATRIOT Act.'" *USA PATRIOT Act of 2001: Hearing Before the Senate Select Comm. On Intelligence,* 109th CONG. (Federal News Service 2005).).

[103] Dan Eggen, *FBI Papers Indicate Intelligence Violations*, WASH. POST, Oct. 24, 2005, at A01 (quoting David Sobel, Electronic Privacy Information Center general counsel).

[104] *See, e.g.,* Edwin Feulner, *Protect the Patriot Act,* HERITAGE FOUND., July 18, 2005, http://www.heritage.org/Press/Commentary/ed071805a.cfm.

[105] *See, e.g.,* Eggen, *supra* note 103 (listing alleged instances of FBI violations).

[106] George H. Pike, *Congress Extends USA PATRIOT Act by 1 Month*, INFO. TODAY, Dec. 26, 2005, http://www.infotoday.com/newsbreaks/nb051226-1.shtml.

[107] S. 1389, 109th CONG. (2005); H.R. 3199, 109th CONG. (2005); *see U.S.: House Amendment Tilts Playing Field for Death Penalty,* HUMAN RIGHTS WATCH, Oct. 27, 2005, http://hrw.org/english/docs/2005/10/26/usdom11924.htm.

¶39 On December 8, the conference committee released a compromise version of the reauthorization bill.[108] The House quickly passed the proposal, but it hung up in the Senate, where it was filibustered by key Democrats.[109] The bill "came before the Senate at a time of increasing concern and skepticism about the PATRIOT Act and the Bush administration's impact on civil liberties in responding to terrorism."[110] Both concern and skepticism were fueled by a story in the New York Times that the President had authorized illegal spying on American citizens by the National Security Agency;[111] that story was released the very day that the renewal bill was to be voted on. Attempts by Senate Republicans to invoke cloture and bring the proposal to a vote were defeated.[112]

¶40 And so, with both sides at loggerheads, and with the legislative session (and 2005) coming to a close, Congress reached a compromise of desperation. At the last possible instant, with only one Senator left in the Capitol, Congress passed Senate bill 2167 (which the President later signed).[113] The bill extended the Patriot Act's sunset provisions until February 3, 2006.[114] Nothing was actually decided; the debate was simply put off for another five weeks.

C. Proposed Changes to the Patriot Act

¶41 Real debate, that is, open and informed debate, is exactly what is needed to effect the necessary changes to the Patriot Act.[115] Each provision should be evaluated, not merely those that are due to sunset. An investigation should be made into the uses of each provision, the extent to which it infringes on civil liberties, and its utility for fighting terrorism. Excessively weak provisions should be expanded; those provisions that are harmful (or simply unnecessary) should be eliminated.

---

[108] Pike, *supra* note 106.
[109] *Id.;* Declan McCullagh and Anne Broache, *Patriot Act Renewal Draws Filibuster Threat,* CNET NEWS.COM, Dec. 8, 2005, http://news.com.com/Patriot+Act+renewal+draws+filibuster+threat/2100-1028_3-5987892.html.
[110] Pike, *supra* note 106.
[111] *Id.*
[112] *Id.* To stop a filibuster, 60 votes are needed. In this case, the Senate leadership was only able to garner 52. *See id.*
[113] *Id.;* Sheryl Stolberg, *Postponing Debate, Congress Extends Terror Law 5 Weeks*, N.Y. TIMES, Dec. 23, 2005.
[114] Stolberg, *supra* note 113.
[115] Recall that the Act was initially passed very quickly, before most Congressman even had a chance to read (let alone consider) its provisions. *See* Harrow, *supra* note 7.

¶42 Such a comprehensive review will clearly take longer than the short time remaining before February 3. Some longer-term compromise will need to be reached regarding the expiring provisions. What is most important is that a true evaluation of all the Act's provisions actually occurs. That begs the question, however, of what an appropriate Patriot Act should look like. The remainder of this section will outline the changes that should be made to sections 210 and 505 to bring them into conformity with principles of freedom and good government.[116]

¶43 Section 210 is not amended by the conference report,[117] and because it does not sunset, the current law will remain in place after February 3. Prosecutors and other officials will still be able to use administrative and grand jury subpoenas to access communications records without judicial review.

¶44 An appropriately revised subpoena provision should allow access to financial information only when necessary, and then only with the proper procedural safeguards. Section 210 should be amended to provide financial information via subpoena only upon a judge's determination that such information is needed. The standard of review need not be as high as the probable cause required for a warrant; a lesser standard would suffice. The important thing is that an impartial judge be required to verify that the information is actually needed; the issuing agent's say-so is not sufficient. This basic judicial review would go a long way toward guarding against potential abuse of subpoena power by prosecutors and other government agents. Additionally, the law should be amended to require communications providers to ensure that the name and address listed on an account match the name and address associated with the billing information. If the billing information were needed solely to verify identity, such a law would satisfy that need without compromising customers' financial information.

¶45 Unlike section 210, section 505 is addressed in the conference report.[118] The proposal would permit NSL recipients to challenge their NSLs in court; courts would be authorized to set aside NSL requests that

---

[116] This iBrief does not take issue with administrative subpoenas and national security letters *per se*. While it is true that administrative subpoenas pre-Patriot Act did not entail judicial review, neither did they provide the government with access to sensitive financial information. Carte blanche access to customers' names and addresses is substantially different from access to their bank account numbers. Similarly, although NSA's have always been intrusive, they could originally only be used to investigate foreign agents. This iBrief takes issue, not with the tools themselves, but with their widened scope as a result of the Patriot Act.

[117] H.R. CONF. REP. NO. 109-333 (2005).

[118] *Id*. at 50-75.

were "unreasonable, oppressive, or otherwise unlawful."[119] The bill would also allow recipients to contact an attorney.[120] The NSL nondisclosure provision could also be contested and set aside if the court found it to be unnecessary; however, the FBI's certification that nondisclosure is needed "shall be treated as conclusive unless the court finds that the certification was made in bad faith."[121] The bill contains an explicit enforcement provision, and would make the willful violation of the nondisclosure provision a crime punishable by up to five years in prison.[122]

¶46 Though seemingly substantive, the changes to section 505 fail in several respects. First, the proposal lacks meaningful judicial review.[123] At first blush, it *appears* to provide such review—after all, recipients would be able to challenge both the NSL and its nondisclosure provision in court. Yet although the NSL itself could be challenged, the court could only overturn the request if it was unreasonable or oppressive. The case law surrounding administrative subpoenas makes it clear that a court will rarely overturn a request on those grounds.[124] Furthermore, under the proposal, the government would not be required to provide any evidence that the information sought was necessary; the FBI official's certification would be sufficient.[125] Although the gag order could be challenged as unnecessary, an FBI agent's certification to the contrary would be conclusive absent evidence of bad faith.

¶47 A proper NSL provision should avoid abuse or capriciousness by incorporating meaningful judicial review throughout the data-gathering process. Before issuing an NSL, an agent should be required to meet with a judge to outline the evidence that justifies the NSL's issuance. The evidence should be such that it gives "reason to believe" that the person being

---

[119] *Id.* at 50.
[120] *Id.* at 56.
[121] *Id.* at 62.
[122] *Id.* at 66.
[123] Adequate judicial review is vital for an NSL provision that lacks a "foreign agent" requirement. If the realities of fighting global terrorism require expanding NSLs to American citizens, those citizens must be afforded the opportunity to contest the NSLs in court. The prevention of terrorism is no excuse for denying citizens their constitutional rights.
[124] *See* Oklahoma Press Pub. Co. v. Walling, 327 U.S. 186, 208 (1946) (holding that neither the Fourth Amendment nor the Fifth Amendment's protection against self-incrimination creates an obstacle to the enforcement of a reasonable administrative subpoena); *see also* United States v. Powell, 379 U.S. 48, 57–8 (1964) (holding that no standard of probable cause must be met to issue a valid administrative subpoena).
[125] *See* H.R. CONF. REP. NO. 109-333 (2005).

investigated is involved in espionage or international terrorism.[126] If the person under investigation is later cleared, the information gathered should be destroyed. If the NSL is challenged, it should then be evaluated by the court for unreasonableness or oppressiveness as applied in that particular case. Finally, a judge should once again review the NSL when evaluating whether to impose a gag restriction. Unlike the present law, which imposes such gag orders universally, such a decision should be made on a case-by-case basis. If the government feels that a gag order is needed for reasons of security or national policy, it should bear the burden of affirmatively showing that such a measure is necessary. Absent a showing of necessity, the default should be in favor of free expression.

CONCLUSION

¶48 Over two hundred years ago, James Madison penned these prescient words:

> If men were angels, no government would be necessary. If angels were to govern men, neither external nor internal controls on government would be necessary. In framing a government which is to be administered by men over men, the great difficulty lies in this: you must first enable the government to control the governed; and in the next place oblige it to control itself. A dependence on the people is, no doubt, the primary control on the government; but experience has taught mankind the necessity of auxiliary precautions.[127]

¶49 As Congress begins yet another series of debates on the propriety of the Patriot Act's powers, it would do well to keep Madison's words in mind. Even if possessed of the best intentions, our government officials are human, and they sometimes make mistakes. And sometimes, those officials that we rely upon for protection are corrupt and self-interested.[128]

---

[126] This "reason to believe" standard is less than the probable cause needed to issue a warrant, allowing agents to acquire NSLs more easily than traditional warrants.

[127] THE FEDERALIST NO. 51 (James Madison).

[128] For that reason, it is not sufficient to be told that the government has no intention of abusing its broad powers, as the DoJ is prone to do. *See, e.g.,* Attorney General John Ashcroft, Protecting Life and Liberty, Address in Memphis, Tennessee (Sept. 18, 2003), http://www.usdoj.gov/archive/ag/speeches/2003/091803memphisremarks.htm ("You might . . . believe the hysteria behind this claim: 'Your local public library is under siege by the FBI.'. . . The fact is, with just 11,000 FBI agents and over a billion visitors to America's libraries each year, the Department of Justice has neither the staffing, the time nor the inclination to monitor the reading habits of Americans. No offense to the American Library Association, but we just don't care.").

¶50 To compensate for that possible self-interest, our country needs laws that give the government only the powers that it requires to accomplish its legitimate purposes. Sections 210 and 505 of the Patriot Act both fail in that regard. The two failures are not of equal magnitude: compared to the constitutional stature of the section 505 abuses, the release of financial account information may seem minor. Yet both provisions encroach upon citizens' freedoms unnecessarily; for that reason, they should be equally rejected.

¶51 Fighting terrorism is a serious task, and our government needs the tools necessary to do so effectively. However, when it is possible to obtain security without compromising liberty, any concession of liberty is too great. It's time for Congress to reinstate some of those "auxiliary precautions " that Madison spoke of by substantially revising the Patriot Act. Sections 210 and 505 are good places to start.