Volume VI - Article 8

DOE V. ASHCROFT AND ITS PLACE IN THE JUDICIAL TREND: HOW THE COURTS HAVE ADVANCED CIVIL LIBERTIES IN STEP WITH ADVANCES IN TECHNOLOGY

Craig M. Glasgow[1]

Spring 2006

As many jurists and scholars have noted, the United States has a long-standing history of encroaching upon the civil liberties of its citizens, especially during times of war or conflict.[2] For instance, during the Civil War, President Lincoln unilaterally suspended the writ of *habeas corpus* in response to increased violence and the threat of Southern succession.[3] During World War I, Postmaster General Albert Burleson used the Espionage Act to suspend mailing privileges for certain "non-mailable" materials, such as newspapers and other dissident publications critical of the war effort.[4]

The United States' most egregious twentieth-century civil liberties violation occurred during World War II: the Japanese Internments. Executive Order 9066, signed by President Roosevelt on February 19, 1942, and confirmed by Congress shortly thereafter, authorized west coast military commanders to impose curfews upon, and

[1] University of Pittsburgh School of Law, J.D. expected 2006.
[2] WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME (1998); *see also* MICHAEL LINFIELD, FREEDOM UNDER FIRE: U.S. CIVIL LIBERTIES IN TIMES OF WAR (1990).
[3] REHNQUIST, *supra* note 2, at 22-25.
[4] *Id.* at 173-75.

eventually exclude, persons of Japanese ancestry, whether citizen or alien.[5] Even the United States Supreme Court found these actions constitutional.[6]

Civil liberty curtailments were not just limited to these "traditional" restrictions. Technology was also subject to the federal government's reoccurring civil liberties violations. During the Civil War, President Lincoln "seize[d] the telegraph lines and establish[ed] censorship over all transmissions."[7] During World War I, President Wilson seized and censored the recently developed wireless establishments.[8] Additionally, at the end of World War I, the newly formed Bureau of Investigations (later the Federal Bureau of Investigation) began to conduct wiretaps.[9] As it did with the Japanese internment, curfew, and exclusion cases, the United States Supreme Court initially found these actions permissible.[10] In fact, it was not until 1967 that the Court held that wiretapping was indeed a Fourth Amendment search, thus requiring a warrant.[11]

To more thoroughly address this concern, Congress passed the Wiretap Act in 1968.[12] This act created a comprehensive system to control and "facilitate the use of wiretapping and bugging (subject to appropriate safeguards) in federal criminal investigations."[13] However, it was not long before new technologies emerged that permitted the Government to circumvent the Wiretap Act and continue to electronically

---

[5] *Id.* at 190-92.
[6] Hirabayashi v. United States, 320 U.S. 81, 92 (1943) ("[I]t was within the constitutional power of Congress and the [Executive] . . . to prescribe this curfew order . . . ."); Korematsu v. United States, 323 U.S. 214, 217-18 (1944) ("[W]e are unable to conclude that it was beyond the war power of Congress and the Executive to exclude those of Japanese ancestry from the West Coast war area . . . .").
[7] MICHAEL LINFIELD, FREEDOM UNDER FIRE: U.S. CIVIL LIBERTIES IN TIMES OF WAR 24 (1990).
[8] *Id.* at 47.
[9] *Id.* at 59, 99.
[10] Olmstead v. United States, 277 U.S. 438 (1928) (wiretapping does not violate the Fourth Amendment since there was no searching, no seizure of anything tangible, and no physical trespass).
[11] Katz v. United States, 389 U.S. 347 (1967); Berger v. New York, 388 U.S. 41 (1967).
[12] Omnibus Crime Control and Safe Street Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-22 (2002)).
[13] United States v. Torres, 751 F.2d 875, 881 (7th Cir. 1984).

monitor individuals and groups. For instance, computers enabled the automation of "watch lists" in programs such as the National Security Agency's MINARET project,[14] while emerging video technology in the 1980s enabled the government to obtain even more intrusive and revealing information than ever before.[15]

As might have been expected, both the terrorist attacks of September 11, 2001 ("9/11") and subsequent conflicts have prompted the Government to once again expand national security measures. While some of these expansions are necessary, many commentators believe there has been an overreaction and a "targeting and scapegoating [of] civil liberties."[16] Others claim that 9/11 has "been used as a pretext to loosen constraints that law enforcement has been chafing under for years."[17]

With that said, the post-9/11 government seems to be following in the footsteps of its predecessors. There are secret detention and immigration proceedings, [18] as well as indefinite detentions of both foreign nationals and United States citizens.[19] Many of these detentions were brought without charges or judicial hearings.[20] Additionally, the post-9/11 government is using sophisticated technology now more than ever to create a surveillance society. As commentators have stated, "The explosion of computers,

---

[14] LINFIELD, *supra* note 7, at 133.
[15] *See, e.g.,* United States v. Cuevas-Sanchez, 821 F.2d 248, 251 (5th Cir.1987) ("This type of surveillance provokes an immediate negative visceral reaction: indiscriminate video surveillance raises the spectre of the Orwellian state."); Torres, 751 F.2d at 878 ("[S]ecretly televising people . . . while they are in what they think is a private place is an even greater intrusion on privacy that secretly recording their conversations.").
[16] Stephen J. Schulhofer, *No Checks, No Balances: Discarding Bedrock Constitutional Principles*, *in* THE WAR ON OUR FREEDOMS: CIVIL LIBERTIES IN AN AGE OF TERRORISM 74, 75 (Richard C. Leone & Greg Anrig, Jr. eds., 2003).
[17] Jay Stanley & Barry Steinhardt, *Bigger Monster, Weaker Chains: The Growth of an American Surveillance Society*, *in* CIVIL LIBERTIES VS. NATIONAL SECURITY IN A POST-9/11 WORLD 53, 55 (M. Katherine B. Darmer et al. eds., 2004).
[18] Aryeh Neier, *Introduction* to LOST LIBERTIES: ASHCROFT AND THE ASSAULT ON PERSONAL FREEDOM 1, 2-3 (Cynthia Brown ed., 2003).
[19] Schulhofer, *supra* note 16, at 75, 88-89.
[20] *Id*.

cameras, sensors, wireless communications, GPS, biometrics, and other technologies . . . is feeding a surveillance monster that is growing silently in our midst."[21]

One of the ways this post-9/11 government is utilizing technology is via the USA PATRIOT Act's reoccurring absence of judicial review procedures. By making slight changes to previously enacted statutes, the PATRIOT Act is able to open up the gates to stored electronic communications. As one commentator noted, "[The act] liberalizes the legal environment in which federal cops will be gathering and processing the routine informational detritus of the digital age."[22]

Specifically noteworthy is the PATRIOT Act's effect on Internet surveillance. Millions of Americans use the Internet not just to shop, "but to research topics of interest, debate political issues, seek support for personal problems, and many other purposes that can generate deeply private information about their thoughts, interests, lifestyles, habits, and activities . . . ."[23] Due to certain provisions of the PATRIOT Act enabling the government to have "automatic access to information stored and generated by Internet service providers," there is great cause for concern amongst all online citizens.[24] By utilizing relaxed requirements for investigation as well as "national security letter statutes," the Government is now able to access our Internet activities and records with little trouble, no judicial oversight, and complete secrecy.

There is hope, however. The District Court for the Southern District of New York's recent decision in *Doe v. Ashcroft* provides a strong and well reasoned precedent for putting a boundary on the Government's ability to access our online lives. In addition,

---

[21] Stanley & Steinhardt, *supra* note 17, at 54.
[22] Christian Parenti, *Fear as Institution: 9/11 and Surveillance Triumphant*, *in* CIVIL LIBERTIES VS. NATIONAL SECURITY IN A POST-9/11 WORLD 115, 118 (M. Katherine B. Darmer et al. eds., 2004).
[23] Stanley & Steinhardt, *supra* note 17, at 60.
[24] Parenti, *supra* note 22, at 118.

this case joins the ranks of many other notable decisions that have established a decades-old trend of requiring judicial review of technologically oriented curtailments of civil liberties, thereby ensuring a balance between privacy rights and national security interests.

The purpose of this note is to examine the USA PATRIOT Act's subtle effect on the government's ability to issue national security letters via 18 U.S.C. § 2709, and how one court, joining a long-standing judicial trend, declared that the Federal Government had gone too far by not providing any provisions for judicial oversight and review. Part II provides an introduction to the USA PATRIOT Act. Part III discusses the Electronic Communications Privacy Act of 1986 and details the ever-expanding scope of 18 U.S.C. § 2709, including changes made by the USA PATRIOT Act. Part IV contains an analysis of the Southern District of New York's recent *Doe v. Ashcroft* decision. Part V discusses the judiciary's decades-long trend of requiring judicial review of technologically oriented curtailments of civil liberties and how *Doe v. Ashcroft* falls right into line with, and strongly supports, that trend. Part VI summarizes and concludes the matters discussed herein.

II. An Introduction to the USA PATRIOT Act:

Congress passed the USA PATRIOT Act ("Patriot Act") on October 26, 2001, just six weeks after the 9/11 terrorist attacks.[25] Its stated purpose was "[t]o deter and punish terrorist acts in the United States and around the world, to enhance law

[25] Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

enforcement investigatory tools, and for other purposes."[26] The act found resounding support during its early days. In fact, only one United States senator voted against it, and no major newspapers opposed it editorially.[27] Some of this praise is justified since certain provisions "correct oversights in prior law or adapt technically worded statutes to new technologies and practices."[28] Examples include section 209, which gives judges authority to seize voice-mail messages pursuant to a warrant, and section 220, which allows nationwide service of search warrants for electronic evidence.

However, less justifiable provisions have been created. Particularly troublesome are the changes made to the Foreign Intelligence Surveillance Act of 1978 ("FISA"), codified as 50 U.S.C. § 1801 et. seq.[29] This act establishes procedures for the "Government's domestic electronic surveillance of foreign governments and their agents."[30] Traditionally, such surveillance is subject to less stringent standards, provided that it is "exclusively between or among foreign powers" and that "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is party."[31] However, under various Patriot Act provisions, the FBI can now, for example, obtain business and educational records without showing that the relevant customer or student is a foreign power or agent.[32]

The drafters of the Patriot Act must have also realized the ubiquitous use of the Internet because they created powerful provisions dealing with information stored by

---

[26] *Id.*
[27] Neier, *supra* note 18, at 7.
[28] Schulhofer, *supra* note 16, at 76-77.
[29] Pub. L. No. 95-511, 92 Stat. 1783 (1978).
[30] Doe v. Ashcroft, 334 F. Supp. 2d 471, 489 (S.D.N.Y. 2004).
[31] 50 U.S.C. § 1802(a)(1). *See also* Ashcroft, 334 F. Supp. 2d at 515 ("FISA orders are specifically limited to electronic surveillance of foreign governments and their agents, thus arguably not raising the heightened constitutional concerns and protections implicated when investigations involve the activities of United States nationals.").
[32] Schulhofer, *supra* note 16, at 77.

communications firms. These provisions essentially "undermine[] checks and balances by giving investigators new authority to track Internet usage . . . without having to demonstrate probable cause or obtain a judicial warrant."[33] By slightly altering national security letter statutes, like 18 U.S.C. § 2709, *infra*, the Patriot Act enables the FBI to "force anyone to turn over records on their customers or clients, giving the government unchecked power to rifle through individuals' . . . Internet usage . . . ."[34] These activities are conducted without showing suspicion of a crime, in complete secrecy, and without any judicial review.[35]

III. The History of the Electronic Communications Privacy Act of 1986 and 18 U.S.C. § 2709:

The 1968 Wiretap Act created a comprehensive system to control the Government's use of wiretap surveillance. Though the act was a major step forward in protecting citizens' privacy, it was limited to the "aural interception of wire or oral communications . . . [and it] only applie[d] where the contents of a communication [could] be overheard and understood by the human ear."[36] New technologies emerged, however, and people were soon communicating via computer-to-computer transmissions, microwaves, satellite, video, paging systems, and faxes, all of which were, by definition, outside the bounds of the Wiretap Act. In addition to these advances, the Government also had its own corresponding technological advances in surveillance. Thus, it was not

[33] *Id.*
[34] Stanley & Steinhardt, *supra* note 17, at 65.
[35] *Id.*
[36] S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556; *see also* 18 U.S.C. § 2510(4) (1968).

long before the Wiretap Act was declared "hopelessly out of date," having "not kept pace with the development of communications and computer technology."[37]

The Electronic Communications Privacy Act of 1986 ("ECPA") was created to account for these advances in technology.[38] The ECPA amended and updated Title III of the Wiretap Act so as "to protect against the unauthorized interception of electronic communications . . . [and] update and clarify Federal privacy protections and standards . . . ."[39] This was mainly achieved under Title I, which addressed "the interception of wire, oral and *electronic communications*" (emphasis added).[40]

Additionally, the drafting committee recognized that computers were being used as storage and information processing devices. To protect such data and usage, Title II was created to address "access to stored wire and electronic communications and transactional records."[41] Title II was based on the Right to Financial Privacy Act of 1978 ("RFPA"),[42] which was enacted to "protect the customers of financial institutions from unwarranted intrusion into their records . . . ."[43] The RFPA was a "response to the Supreme Court decision in *United States v. Miller* which held that a customer of a financial institution has no standing under the [Fourth Amendment] to contest Government access to financial records."[44] Fearing that subscribers of electronic

---

[37] *Id*.
[38] Pub. L. No. 99-508, 100 Stat. 1848 (1986).
[39] S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3555.
[40] *Id.* at 3557. Despite this purpose, Congress failed to expressly mention video surveillance in Title I. Thus, as discussed below, it was ultimately the courts that ended up deciding upon a regulatory scheme. *See, e.g.,* United States v. Torres, 751 F.2d 875 (7th Cir. 1984); United States v. Koyomejian, 946 F.2d 1450 (9th Cir. 1991).
[41] S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. at 3557.
[42] Pub. L. No. 95-630, Title XI, 92 Stat. 3641, 3697 (1978).
[43] H.R. REP. NO. 95-1383, at 28 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 9273, 9305.
[44] *Id.* at 9306 (citing United States v. Miller, 425 U.S. 435 (1976)).

communications services would also have no Fourth Amendment protections, Title II of the ECPA was passed in order control Government surveillance.[45]

Similar to the RFPA before it, ECPA Title II was designed to strike a balance between protecting both "privacy interests" and "the Government's legitimate law enforcement needs."[46] Thus, generally, Title II only permits the Government to acquire stored electronic communications either through the subscriber's consent or through a judicial process, such as a search warrant, court order, or subpoena.[47] However, a steadily expanding exception to this general rule was emerging: 18 U.S.C. § 2709 ("2709").

Section 2709 was enacted as part of ECPA Title II. As originally enacted, it allowed the FBI to demand that communications firms, such as wire communication service providers and Internet Service Providers, hand over certain subscriber records, such as "subscriber information" and "electronic communication transactional records."[48] The Government only had to certify that those records were "relevant to an authorized foreign counterintelligence investigation" and that there were "specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is or may be a foreign power or an agent of a foreign power."[49] The demands made under § 2709 are in the form of national security letters ("NSL"), which are a "unique form of administrative subpoenas cloaked in secrecy and pertaining to national

---

[45] *See* S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557-58.
[46] *Id.* at 3557; *see also* H.R. REP. NO. 95-1383, at 28 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 9273, 9305.
[47] 18 U.S.C. § 2703 (2005). *See also* Freedman v. AOL, 303 F. Supp. 2d 121, 124 (Dist. Conn. 2004) (describing the steps the Government must take under § 2703 when seeking information from an ISP).
[48] 18 U.S.C. § 2709 (1988).
[49] *Id*. There are a few other NSL statutes, each requiring compelled production of documents, certification of relevance to international terrorism or counterintelligence investigation, and perpetual non-disclosure. *E.g.,* 12 U.S.C. § 3414 (financial records); 15 U.S.C. § 1681u (credit records); 50 U.S.C. § 436 (government employee records).

security issues."[50] Additionally, § 2709(c) permanently bars the NSL recipient from disclosing the inquiry.

In 1993, § 2709 was broadened by a weakening of the required connection to a foreign entity. Previously, § 2709 required that the subscriber whose stored information was sought be a foreign power or agent. This requirement was necessary so that NSLs would not be issued upon persons simply because they communicated with foreign entities.[51] With this change, however, the statute required that the FBI simply show that "there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801)."[52] By referencing 50 U.S.C. § 1801, this amended provision was able to reach not just foreign individuals and entities, but also United States citizens, so long as there was a strong connection to a foreign entity.[53]

The final amendment to § 2709, which brought about the plaintiff's claim in *Doe v. Ashcroft*, *infra*, came in October 2001 with the passing of the Patriot Act. Section 505 of the act completely removed the long-standing requirement that there be a connection between the information sought under a § 2709 NSL and a foreign agent or power. It was replaced by the mere standard of relevance: the FBI must certify that the "records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities . . . ."[54] This change was made to streamline the acquisition of NSLs and thereby bring § 2709 into line with "existing criminal law where

[50] Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004).
[51] H.R. REP. NO. 103-46, at 2 (1993), *as reprinted in* 1993 U.S.C.C.A.N. 1913, 1914.
[52] 18 U.S.C. § 2709 (1994).
[53] 50 U.S.C. § 1801(b) (2005).
[54] 18 U.S.C. § 2709(b) (2005).

an Assistant United State Attorney may issue a grand jury subpoena for all such records in a criminal case."[55] Furthermore, this expanded statute still required permanent non-disclosure from the NSL recipient and was silent on the need for prior judicial review.

While efficiency and prompt action are important to national security, it is important to acknowledge that grants of power "enabling [the government] to move in secrecy to a given end with the most expedient dispatch and versatile means . . . often pose the gravest perils to personal liberties."[56] Such concerns were voiced at the Congressional hearings surrounding the adoption of the Patriot Act. One technology watchdog group stated that the section "would greatly increase access to the personal information of consumers or groups who are not agents of foreign powers" and that "the institutions granting access to consumer information would be prohibited from disclosing that information or records had been obtained."[57] These were the issues adjudicated in *Doe v. Ashcroft*.[58]

IV. An Analysis of *Doe v. Ashcroft*:

The main plaintiff, "John Doe," was an Internet access firm that received an NSL under § 2709.[59] The other plaintiffs were the American Civil Liberties Union and the American Civil Liberties Union Foundation (collectively with Doe, "plaintiffs"). Doe received an NSL stating that "pursuant to Title 18, United States Code (U.S.C.), Section

[55] H.R. REP. NO. 107-236, at 62 (2001).
[56] Doe v. Ashcroft, 334 F. Supp. 2d 471, 478 (S.D.N.Y. 2004).
[57] *Protective Constitutional Freedoms in the Face of Terrorism: Hearing Before the Subcomm. On the Constitution, Federalism, and Property Rights of the Senate Comm. On the Judiciary*, 107th Cong., S Hrg. 107-610, at 34 (2001) (Statement of Jerry Berman, Executive Director, Center for Democracy and Technology).
[58] Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).
[59] As per the Government's request, the District Court sealed the record of this proceeding in order to prevent the disclosure of Doe's identity. *Id.* at 475 n.3.

2709," Doe was "directed" to provide information to the FBI.[60] As per sections 2709(b)(1) and (c), the NSL certified that the requested information was related to "an authorized investigation to protect against international terrorism or clandestine intelligence activities," and that Doe was prohibited from disclosing that the "[FBI] has sought or obtained access to information or records."[61] Doe did not hand over the requested information, but rather consulted with ACLU attorneys and brought suit.

Plaintiffs challenged the constitutionality of § 2709 under the First and Fourth Amendments of the United States Constitution.[62] Specifically, plaintiffs argued that § 2709 gave "the FBI extraordinary and unchecked power to obtain private information without any form of judicial process, and, second, that § 2709's non-disclosure provision burdens speech categorically and perpetually, without any case-by-case judicial consideration . . . ."[63] Plaintiffs asked the Court to enjoin the Government from utilizing § 2709 as a "means of gathering information from the sources specified in the statute."[64]

After discussing the legislative history of § 2709, the Court compared NSLs with the Government's other information-gathering techniques, such as administrative subpoenas, criminal context subpoenas, "mail cover", and FISA. Essentially, when dealing with a United States citizen, all of these other information-gathering techniques allow for some form of judicial review and at least limited, if not complete, disclosure. Even other ECPA Title II provisions, independent of the § 2709 NSL, require some level

[60] Ashcroft, 334 F. Supp. 2d. at 478.
[61] *Id.*
[62] The plaintiffs also argued that § 2709 violated the Fifth Amendment by failing to give notice. Because the Court found for the plaintiffs on other grounds, it declined to address this argument, thus I do not include it in my discussion. *See* Ashcroft, 334 F. Supp. 2d at 527 n. 268.
[63] *Id.* at 475.
[64] *Id.* at 476.

of judicial review and have limited non-disclosure periods.[65] Based upon this general comparison, the Court stated that § 2709 NSLs seem to "provide fewer procedural protections to the recipient than any other information-gathering technique the Government employs to procure [similar] information."[66]

The Court then sought to determine if § 2709, as drafted, raised any constitutional concerns. It focused on two interpretive issues.[67] First, § 2709, by its language, seemed to prohibit all disclosures, even to individuals "whose assistance is necessary to comply with the demands of the NSL," such as an attorney.[68] Second, § 2709 failed to explicitly state whether an NSL recipient could "affirmatively challenge, administratively or judicially, the propriety of an NSL request."[69]

The Government argued that the text of § 2709 already permitted an NSL recipient to both consult an attorney and challenge the NSL in court. The Court concluded, however, that even if it agreed with the Government's argument, the "provisions and practices essentially force the reasonable NSL recipient to immediately comply with the request," and that the "lack of effective process, at least as applied, entails issues far too fundamental for the Court to read as having been sufficiently addressed [by § 2709]."[70] Thus, by comparing § 2709 to the Government's other information-gathering techniques, as well as considering the statute's own language, the Court, even before getting into the statute's functionality under the instant facts, was making a case against the statute because of its lack of judicial review and disclosure.

---

[65] *Id.* at 487-89.
[66] *Id*. at 484.
[67] The Court also raised the issue that § 2709 failed to explicitly impose penalties against those who did not comply with an NSL request. Because this issue did not have a bearing on the motions before the Court, the Court did not address the issue further, nor do I. *See Id.* at 492.
[68] *Id*. at 492.
[69] *Id*.
[70] *Id.* at 493.

Turning to the heart of the matter, the Court analyzed the plaintiffs' claim that § 2709 violated the Fourth Amendment by giving the FBI practical power "to issue as well as enforce its own NSLs, instead of contemplating some form of judicial review."[71] Essentially, § 2709 is silent about prior or subsequent NSL judicial review, and thus, as happened with Doe, the FBI can independently send a letter to an Internet access firm requesting the firm to relinquish subscriber records, which any reasonable recipient would do, especially in light of § 2709(a)'s use of the words "duty" and "shall comply." Additionally, this unchecked power could, pursuant to the Patriot Act's broad relevancy standard, permit the FBI to obtain the Internet records of not only a United States subscriber, but one with, potentially, a very tenuous link to 2709(b)'s requirement of relevancy "to an authorized investigation . . . against international terrorism or clandestine intelligence activities . . . ."

As mentioned above, the Government argued that § 2709 should be interpreted to allow an NSL recipient to challenge the NSL in court. While the Court acknowledged that "where an alternative interpretation of [a] statute is fairly possible, courts are obligated to construe the statute to avoid . . . problems,"[72] it nevertheless opted against this doctrine since the "anchoring of the Government's theory in the legislative scheme [was] far from clear and convincing."[73]

The Court rejected the Government's interpretation for three reasons, two of which are relevant to our concerns here.[74] First, the Court noted that Congress actually

---

[71] *Id*. at 496.
[72] Doe v. Ashcroft, 334 F. Supp. 2d 471, 498 (S.D.N.Y. 2004) (citing INS v. St. Cyr., 533 U.S. 289, 299-300 (2001)).
[73] *Id*.
[74] The third reason for not giving effect to the Government's reading is that doing so would raise separation of powers issues. *Id*. at 500 (Courts are not "legislative repair shops entrusted to perform Congress's labors, and fix Congress's purported errors or omission at the Government's bidding.").

included judicial review provisions in many of the other information-gathering statutes described above, and thus the government's interpretation "is at odds with . . . comparable competing interpretations deriving from different statutes."[75] Second, and more importantly, the Court stated that the Government's interpretation goes against a reasonable reading of Congress's intent with § 2709:

> In light of the sensitivity and overarching national priority associated with the purposes of NSL statutes . . . as well as the gravity of the events [(i.e., 9/11)] that supplied the propelling force and context for the passage and recent amendments of § 2709 [via the Patriot Act § 505], one might fairly infer that the absence of any reference to judicial review is the product of Congressional intent.[76]

Additionally, the Court stated that "the statute could be read to signal Congress's contemplation that *less weight be given to protections of personal liberties* in conflict with the acute national security interests § 2709 fosters" (emphasis added).[77]

In light of these statutory construction considerations, as well as the more practical realization that since the RFPA first permitted the Government to issue NSLs for financial records in 1978, no NSL recipient had ever challenged a request,[78] the Court stated that "in practice NSLs are essentially unreviewable because . . . the recipient would consider himself . . . obliged to comply, with no other option but to immediately obey and stay quiet."[79] Thus, the Court ultimately concluded that § 2709 "ha[d] the effect of authorizing coercive searches effectively immune from any judicial process, in violation of the *Fourth Amendment*."[80]

The Court then turned its attention to the plaintiffs' First Amendment challenge of the § 2709(c) non-disclosure provision, which bars an NSL recipient, such as Doe (an

---

[75] *Id*. at 500.
[76] *Id*.
[77] *Id*.
[78] *Id*. at 502-03.
[79] *Id*. at 503.
[80] *Id*. at 506.

Internet access firm), from ever disclosing to anybody, including subscribers whose records were sought, that the FBI made such a request. Plaintiffs argued that § 2709(c) was either a content-based speech restriction or a prior restraint on speech, either of which requires the court to analyze the provision under strict scrutiny analysis.[81] The Government argued that the provision is only subject to intermediate scrutiny.[82]

The Court deemed § 2709(c) to be both a prior-restraint on speech and a content-based restriction, thus requiring strict scrutiny analysis. First, the provision functions as prior-restraint because it prevents speech before speech even occurs. Second, the provision is a content-based restriction because it regulates an entire subject matter, and "[t]he First Amendment's hostility to content-based regulation extends not only to restrictions on particular viewpoints, but also to prohibition of public discussion of an entire topic."[83] Here, the permanent non-disclosure provision prevents Doe from discussing with anybody, including the Internet subscriber, that Doe had received an NSL and had complied with the request.

The Court then stepped through the strict scrutiny analysis to determine if the § 2709(c) speech restriction was valid. The Court readily acknowledged the Government's legitimate and compelling interest in "protecting the integrity and efficacy of international terrorism and counterintelligence investigations."[84] However, despite this compelling interest, the Court agreed with the plaintiffs that "§ 2709(c)'s categorical,

---

[81] *See, e.g.,* United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 813 (2000) (A content-based speech restriction "must be narrowly tailored to promote a compelling Government interest. If a less restrictive alternative would serve the Government's purpose, the legislature must use that alternative."); Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 70 (1963) ("Any system of prior restraint . . . comes to this Court bearing a heavy presumption against its constitutional validity.").

[82] *See, e.g.,* Turner Broad Sys., Inc. v. FCC, 520 U.S. 180, 189 (1997) (A speech restriction passes intermediate scrutiny if "it advances important governmental interests unrelated to the suppression of free speech and does not burden substantially more speech than necessary to further those interests.").

[83] Consolidated Edison Co. of New York, Inc. v. Public Serv. Comm'n, 447 U.S. 530, 537 (1980).

[84] Doe v. Ashcroft, 334 F. Supp. 2d 471, 513 (S.D.N.Y. 2004).

perpetual, and automatic ban on disclosure [was] not a narrowly-tailored means to advance those legitimate public interests."[85]

In fact, the Court even found FISA's own non-disclosure provision, 50 U.S.C. § 1861(d), to be less restrictive (i.e., more narrowly tailored) than § 2709(c). First, the language of § 1861(d), while essentially a categorical bar, is nevertheless less restrictive because it expressly allows for disclosure to "persons necessary to produce" compliance with the subpoena.[86] Second, FISA limits abuse by "requiring a clear connection to a foreign power and by sharply limiting the degree to which any United States citizen may be subject to surveillance under a secret FISA order."[87] Section 2709 completely lacks such protections for U.S. citizens, especially, as the Court pointed out, "after the significant broadening of the statute's scope effectuated by the Patriot Act."[88]

The Government contended that, while § 2709(c) might not be as narrowly drawn as other information-gathering statutes, it is nevertheless consistent with First Amendment jurisprudence in that the Government may, in many cases, impose secrecy requirements when the secrecy is limited "to facts learned only by virtue of a given person's participation in an [official] proceeding.[89] In other words, when an NSL recipient "learns that an NSL has been issued only by virtue of his particular role in the underlying investigation, . . . the case law demonstrates [that] it presumptively does little violence to First Amendment values to condition the issuance of an NSL upon the recipient's return obligation of at least some secrecy."[90]

---

[85] *Id*. at 514.
[86] *Id*. at 515.
[87] *Id*.
[88] *Id*.
[89] *Id*. at 516.
[90] *Id*. at 519.

While the Court acknowledged the importance of this idea, it stated that the "doctrine reache[d] its limit . . . when the Court consider[ed] that the NSL statutes . . . impose a permanent bar on disclosure in every case, making no distinction among competing relative public policy values over time, and containing no provision for lifting that bar when the circumstances that justify it [are gone.]"[91] Furthermore, the Court noted that "democracy abhors undue secrecy" and that "public knowledge secures freedom," and as such, "unlimited government warrant to conceal . . . has no place in our open society" since it could "become the cover for spurious ends that government may then deem too inconvenient, inexpedient, merely embarrassing, or even illicit to ever expose to the light of day."[92]

Because of these considerations, the Court ultimately concluded that "the statute simply does not allow for [a] balancing of competing public interests to be made by an independent tribunal at any point . . . [and thus,] it is conceivable that 'less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.'"[93] The Court, alluding to the case-by-case approach applied to other cases and information-gathering statutes, dismissed the Government's emphasis on heightened secrecy in terrorism investigations by simply stating that "a case-by-case evaluation of the need for secrecy 'does not mean that information helpful to terrorists will be disclosed, only that the Government must be more targeted and precise in its approach.'"[94] Thus, because less restrictive alternatives were available, § 2709(c) was deemed to be in violation of the First Amendment.

---

[91] *Id*.
[92] *Id.* at 519-20.
[93] *Id*. at 520-21 (citing Reno v. ACLU, 521 U.S. 844, 874 (1997)).
[94] *Id*. at 524 (citing Detroit Free Press v. Ashcroft, 303 F.3d 681, 692-93 (6th Cir. 2002)).

Finally, the Court addressed the question of whether § 2709(c) could be severed from the statute, thus saving sections (a) and (b). The Court had to look to Congressional intent for the answer. Upon doing so, it concluded that "Congress intended the statute to function as a secret means of gathering information from communications service providers," and therefore, Congress "could not have intended §§ 2709(a) and (b) . . . to operate absent the non-disclosure provisions contained in § 2709(c)."[95]

In its conclusion, the Court summarized its decision: "[T]he compulsory, secret, and unreviewable production of information required by the . . . application of 18 U.S.C. § 2709 violates the *Fourth Amendment*, and . . . the non-disclosure provision of 18 U.S.C. § 2709(c) violates the *First Amendment*."[96] The Government was "therefore enjoined from issuing NSLs under § 2709 or from enforcing the non-disclosure provision in this or any other case."[97]

V. *Doe v. Ashcroft* and the Judiciary's Long-Standing Trend of Technological Judicial Review:

The late Chief Justice Rehnquist wrote that "[i]n any civilized society the most important task is achieving a proper balance between freedom and order."[98] To him, it was the job of the courts to ultimately produce this balance. And despite a historical judicial reluctance to decide against the Government on national security issues during war, he believed it was "both desirable and likely that more careful attention would be

[95] *Id*. at 525.
[96] *Id*. at 526-27.
[97] *Id*. at 527.
[98] WILLIAM H. REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 222 (1998).

paid by the courts [in the future] to the basis for the government's claims of necessity as a basis for curtailing civil liberty."[99]

Some commentators question this proposition and say the courts, especially in our technologically advanced and post-9/11 world, "cannot be counted upon for robust defense of civil liberties . . . where claims of national security are invoked."[100] To them, the critical question is: "[T]o what extent [are the courts] ready to protect us against new forms of political surveillance made possible by advances in technology[?]"[101]

To this author, the answer is simple: For the past four decades, the courts have already been consistently protecting us from new technologies and they will continue to do so in the future, perhaps even more strongly. By simply requiring judicial review procedures with each new technological development, the courts have effectively shielded our civil liberties. And even in our post-9/11 United States, while some call for legislative reform of online surveillance laws,[102] the courts are already a step ahead by continuing to balance, via judicial review, Rehnquist's goals of freedom and order, as is most recently demonstrated in the *Doe v. Ashcroft* decision.

The trend of requiring judicial review of technologically oriented curtailments of civil liberties began with *Katz v. United States*.[103] In that case, the Government acquired incriminating evidence against Katz by placing, without a warrant, a listening and recording device to the outside of a public telephone booth. While the Government argued that "surveillance of a telephone booth should be exempted from the usual

---

[99] *Id*. at 225.
[100] Neier, *supra* note 18, at 6.
[101] *Id*.
[102] Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9 (2004).
[103] 389 U.S. 347 (1967).

requirement of advance authorization by a magistrate," the United States Supreme Court disagreed and held that prior judicial review was "a constitutional precondition of the kind of electronic surveillance involved in this case."[104] By so holding, the Court effectively incorporated the Fourth Amendment into the technological world.[105] *Katz*, along with *Berger v. New York*,[106] were such "watershed moment[s] for communications privacy" that Congress enacted the Wiretap Act in the following year to provide even more protection.[107]

This judicial trend received its next significant building block in 1972 with *United States v. United States District Court for the Eastern District of Michigan*.[108] The question before the Court was whether the President could authorize electronic surveillance (i.e., wiretaps) without prior judicial approval for "internal security matters."[109] The United States Supreme Court once again focused on judicial review by stating that the "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive Branch."[110] And even after giving deference to the constitutional basis of the President's role in domestic security, the Court stated that this role "must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure."[111]

---

[104] *Id.* at 358-59.
[105] *See, e.g.,* United States v. United States Dist. Court for the E. Dist. of Mich., 407 U.S. 297, 313 (1972).
[106] Berger v. New York, 388 U.S. 41 (1967) (New York wiretapping statute held unconstitutional because it did not adequately incorporate constitutional standards).
[107] Freiwald, *supra* note 102, at 26.
[108] 407 U.S. 297 (1972).
[109] *Id*. at 299.
[110] *Id*. at 317.
[111] *Id*. at 320.

The trend of requiring judicial review of technologically oriented curtailments of civil liberties continued in the 1980s and early 1990s with a series of Circuit Court decisions involving video surveillance. In *United States v. Torres*, the Seventh Circuit considered the novel issue of whether, and by what standards, the Federal Government could ever secretly videotape the interior of a private building and use that evidence in a criminal trial.[112] The Court looked to the 1968 Wiretap Act for guidance, despite the Act's failure to expressly authorize or regulate video surveillance. Judge Posner, writing for the Court, stated that "we borrow the warrant procedure of Title III, a careful legislative attempt to solve a very similar problem, and hold that it provides the measure of the government's constitutional obligations of particular description in using [video] surveillance to investigate crime."[113] Thus, by requiring judicial review for yet another advancement in technology, the courts had once again effectively protected our civil liberties.

Even after Congress passed the ECPA in 1986, with its conspicuous failure to mention video monitoring, various Circuit Courts continued to follow the reasoning in *Torres* and used the warrant guidelines in the Wiretap Act as the constitutional requirements for video surveillance.[114] In fact, it was not until 1991 that a Circuit Court specifically used the ECPA warrant provisions for video surveillance.[115] Regardless of whether the courts utilized the Wiretap Act or the ECPA, they were all applying the same

[112] 751 F.2d 875, 876 (7th Cir. 1984).
[113] *Id*. at 885; *see also* United States v. Biasucci, 786 F.2d 504, 510 (2d Cir. 1986) (borrowing, like *Torres*, standards from Title III as "guidelines for court-ordered authorization of video surveillance.").
[114] *See* United States v. Cuevas-Sanchez, 821 F.2d 248, 252 (5th Cir. 1987) (Title III provisions are "the standards under which an order for video surveillance may issue."); United States v. Mesa-Rincon, 911 F.2d 1433 (10th Cir. 1990).
[115] United States v. Koyomejian, 946 F.2d 1450, 1458 (9th Cir. 1991) ("Video surveillance in domestic criminal investigations is regulated under [ECPA] Title I in the same manner and to the same extent as bugging, wiretapping, and other expressly listed techniques.").

rationale: judicial review is required to protect the civil liberties of citizens subjected to video surveillance.

The next case adding support to this trend of requiring judicial review of technologically oriented curtailments of civil liberties was decided just three months before the 9/11 terrorist attacks. In *Kyllo v. United States*, the United States Supreme Court was asked to determine whether a thermal-imaging device aimed at a house so as to detect amounts of heat within it constituted a search.[116] Writing for the Court, Justice Scalia noted that whatever "rule we adopt must take account of more sophisticated systems that are already in use or in development."[117]

The Court ultimately held that "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[118] By accounting for technologies *both in use and newly developed*, and presuming that such technologies are *presumptively unreasonable without a warrant*, Justice Scalia had effectively stated what had been happening in the courts over the past four decades: citizens were being protected and not left "at the mercy of advancing technology."[119]

And now, even in our post-9/11 world of ongoing conflicts and potentially overreaching legislation, we are seeing this judicial trend continue. In 2004 alone, there were three powerful opinions reinforcing the need for judicial review as a protection against the curtailment of valued civil liberties. Two of these opinions are United States

[116] 533 U.S. 27 (2001).
[117] *Id*. at 36.
[118] *Id*. at 40.
[119] *Id*. at 35.

Supreme Court cases dealing with physical detentions stemming directly from the 9/11 terrorist attacks and subsequent armed conflicts.[120] The third is the case at bar: *Doe v. Ashcroft*.

In the above analysis, we have seen the District Court for the Southern District of New York focus on § 2709's complete lack of judicial process. The Court held that the statute violated the Fourth Amendment because "it effectively bar[red] . . . any judicial challenge to the propriety of an NSL request."[121] . The Court further noted that the § 2709(c) non-disclosure provision violated the First Amendment because it provided "no vehicle for the ban to ever be lifted from the recipient . . . under any circumstances, either by the FBI itself, or pursuant to judicial process."[122]

The intense focus on judicial review is consistent with the trend started four decades ago by the *Katz* and *Berger* decisions. This judicial trend, including *Doe v. Ashcroft*, has never held that the Government does not have a legitimate interest in using the latest technology to acquire information. It has never disputed the Government's claim that new technologies are often used as the vehicles for crime, and consequently must be occasionally monitored. Furthermore, it has never dismissed the notion that, at times, compelling Government interests will require the abrogation of various civil liberties. Rather, this judicial trend, including *Doe v. Ashcroft,* has simply required that the Government, when using old or new technology to abrogate civil liberties, explain its reasons for doing so. It is that simple. In this way, the judiciary has ensured that civil

---

[120] *See* Hamdi v. Rumsfeld, 124 S. Ct. 2633, 2635 (2004) (holding that "due process demands that a citizen held in the United States as an enemy combatant be given a meaningful opportunity to contest the factual basis for that detention before a neutral decisionmaker."); Rasul v. Bush, 124 S. Ct. 2686, 2699 (2004) (holding that U.S. courts have jurisdiction to hear challenges "of the Executive's potentially indefinite detention" of foreign nationals incarcerated at Guantanamo Bay).
[121] Doe v. Ashcroft, 334 F. Supp. 2d 471, 475 (S.D.N.Y 2004).
[122] *Id*. at 476.

liberties will advance in step with advances in technology and that a proper balancing of the late Chief Justice Rehnquist's ideals of personal freedom and government order will occur.

Doe v. Ashcroft is important to this judicial trend because it demonstrates that even after the unprecedented terrorist attacks of 9/11, the judiciary is still strongly committed to protecting civil liberties from advancements in technological surveillance. The decision is both comprehensive and well-reasoned, and thus provides a strong precedent for future courts to rely upon when dealing with new technologies. It has made § 505 of the Patriot Act useless, and has weakened the rationale for *all* NSL statutes, not just § 2709, by undercutting the Government's purported need for complete secrecy. Because of these reasons, the addition of *Doe v. Ashcroft* to the long-standing trend requiring judicial review of technologically oriented curtailments of civil liberties is a substantial victory for privacy advocates everywhere.

VI. Conclusion:

"[T]he law must advance with the technology to ensure the continued vitality of the [F]ourth [A]mendment."[123] This is what the "judicial trend" ensures. By requiring, often before Congress has spoken, that Government surveillance involving technology is subject to judicial review, the courts are simultaneously protecting treasured civil liberties while also enabling legitimate law enforcement and national security measures to proceed.

[123] S. REP. NO. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3559.

Through *Doe v. Ashcroft*'s focus on judicial review, it can be seen that this trend continues in our post-9/11 world. It not only moves the trend forward by adding another powerful precedent, but it also nullifies a section of the hastily enacted Patriot Act, weakens all NSL statutes, and specifically declares the § 2709 NSL authority permitting the Government to gain access to our online records unconstitutional.

With all of this in mind, the millions of Americans who routinely use the Internet to conduct their everyday activities can breathe a sigh of relief and know that their electronic records are, and will be, safe from unchecked prying government eyes.