334 F.Supp.2d 471 (2004)

John DOE; American Civil Liberties Union; and American Civil Liberties Union Foundation, Plaintiffs,
v.
John ASHCROFT, in his official capacity as Attorney General of the United States; Robert Mueller, in his official capacity as Director of the Federal Bureau of Investigation; and Marion Bowman, in his official capacity as Senior Counsel to the Federal Bureau of Investigation, Defendants.

No. 04 Civ. 2614(VM).

United States District Court, S.D. New York.

September 28, 2004.

472*472 473*473 474*474 Ann Beeson, New York, NY, Arthur N. Eisenberg, New York Civil Liberties Union Foundation, New York, NY, Jameel Jaffer, New York, NY, for American Civil Liberties Union, John Doe.

Meredith E. Kotler, New York, NY, for John Ashcroft, Marion Bowman, Robert Mueller.

OPINION

DECISION AND ORDER

MARRERO, District Judge.

TABLE OF CONTENTS

I. *INTRODUCTION*

Plaintiffs in this case challenge the constitutionality of 18 U.S.C. § 2709 ("§ 2709"). That statute authorizes the Federal Bureau of Investigation ("FBI") to compel communications firms, such as internet service providers ("ISPs") or telephone companies, to produce certain customer 475*475 records whenever the FBI certifies that those records are "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."[1] The FBI's demands under § 2709 are issued in the form of national security letters ("NSLs"), which constitute a unique form of administrative subpoena cloaked in secrecy and

pertaining to national security issues. The statute bars all NSL recipients from ever disclosing that the FBI has issued an NSL.[2]

The lead plaintiff, called "John Doe" ("Doe")[3] for purposes of this litigation, is described in the complaint as an internet access firm that received an NSL. The other plaintiffs are the American Civil Liberties Union ("ACLU") and the American Civil Liberties Union Foundation, which is also acting as counsel to Doe (collectively with Doe, "Plaintiffs"). Plaintiffs contend that § 2709's broad subpoena power violates the First, Fourth and Fifth Amendments of the United States Constitution, and that the non-disclosure provision violates the First Amendment. They argue that § 2709 is unconstitutional on its face and as applied to the facts of this case. Plaintiffs' main complaints are that, first, § 2709 gives 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 of whether that speech burden is justified. The parties have cross-moved for summary judgment on all claims.

For the reasons explained below, the Court grants Plaintiffs' motion. The Court concludes that § 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. In the Court's view, ready availability of judicial process to pursue such a challenge is necessary to vindicate important rights guaranteed by the Constitution or by statute. On separate grounds, the Court also concludes that the permanent ban on disclosure contained in § 2709(c), which the Court is unable to sever from the remainder of the statute, operates as an unconstitutional prior restraint on speech in violation of the First Amendment.

The Court's ruling is about the *process* antecedent to the substance of any particular challenge, and in that vein, it is both narrow and broad. This determination is narrow in two respects. First, although the Court recognizes hypothetically that some aspects of the interpretation of § 2709 as proffered by the Government here may be plausible, the Court's analysis of the legislative record reveals grounds at least as compelling to cast substantial doubt upon such a reading of the statute. Given its strong reservations about the sufficiency of the statutory basis upon which the Government's theory is founded, the Court in the final analysis deems it unnecessary to rule upon Plaintiff's facial challenge to § 2709 on Fourth Amendment grounds.

Second, the Court declines Plaintiffs' invitation to decide the measure of Fourth Amendment protection demanded when 476*476 the Government makes NSL requests generally or in any particular case. The Court decides only that those rights, as well as other rights attaching to protected speech content that may be revealed to the Government as a result of an NSL, are implicated to some extent when an individual receives an NSL, thus necessitating the practical availability of some form of access to the judicial system to challenge the NSL. On the record before it, the Court finds that in practice those rights are substantially curtailed by the manner in which the FBI administers § 2709.

The Court's ruling is broad in that even if § 2709 could be fairly construed in accordance with the Government's proposed reading to incorporate the availability of some judicial review, and putting aside the impairment of Fourth Amendment protections the Court finds countenanced by § 2709 as applied, other structural flaws inherent in the statute as a whole render it invalid on its face. In particular, the Court agrees with Plaintiffs that § 2709(c), the non-disclosure provision, is unconstitutional. In simplest terms, § 2709(c) fails to pass muster under the exacting First Amendment standards applicable here because it is so broad and open-ended. In its all-inclusive sweep, it prohibits the NSL recipient, or its officers, employees, or agents, from revealing the existence of an NSL inquiry the FBI pursued under § 2709 in every case, to any person, in perpetuity, with no vehicle for the ban to ever be lifted from the recipient or other persons affected,

under any circumstances, either by the FBI itself, or pursuant to judicial process. Because the Court cannot sever § 2709(c) from § 2709(a) and (b), the Court grants the remedy Plaintiffs request enjoining the Government from using § 2709 in this or any other case as a means of gathering information from the sources specified in the statute.

Considering the implications of its ruling and the importance of the issues involved, the Court will stay enforcement of its judgment for 90 days, pending appeal or measures by the Government otherwise to address the flaws in the structure and implementation of § 2709 described here.

II. *BACKGROUND*

Like most of our constitutional law's hardest cases, this dispute is about two fundamental principles: values and limits. It centers on the interplay of these concepts, testing the limits of values and the values of limits where their ends collide.

National security is a paramount value, unquestionably one of the highest purposes for which any sovereign government is ordained. Equally scaled among human endeavors is personal security, an interest especially prized in our system of justice in the form of the guarantee bestowed upon the individual to be free from imposition by government of unwarranted restraints on protected fundamental rights.[4] Efficiency, too, counts as a basic value, though it essentially serves as a tool in the service of other interests. To perform its national security functions properly, government must be empowered to respond promptly and effectively to public exigencies as they arise, and in pursuit of those necessary actions to maintain a reasonable measure of secrecy surrounding its operations and methods.

When pushed to their outer limits, these values may clash, giving rise to another form of interaction among vital societal principles. Inevitably, the resultant forces 477*477 entail, from exercise of the powers assigned to the different branches of government, judgments about how and by whom to resolve which value may have exceeded its designated bounds. This choice is always demanding, and its outcome is not always plain at first sight. But, throughout the ages when the weighing has had to be done, time, wisdom and hard experience, aided by the inherent soundness of our underlying values, have steered resolution on a fairly consistent course. One guiding principle in that path is clearly marked in tried and proved results: that, by definition, efficiency invariably serves as the quickest and most expedient way to get from here to there; but, in the protection of fundamental values, the race is not always to the swiftest or cheapest means. So the Constitution counsels.

On this point, the United States Supreme Court has imparted consistent guidance, drawn on each occasion from adjudications of the some of the most intense crises in the nation's history. Recently, for example, in addressing the reach of the President's authority to combat terrorism, the Supreme Court declared: "We have long ... made clear that a state of war is not a blank check for the President when it comes to the rights of the nation's citizens."[5] This pronouncement echoes other like counsel issued when the Court has been called upon to settle conflicts of equally high moment. In another prominent case in point the Court remarked: "[E]ven the war power does not remove constitutional limitations safeguarding essential liberties."[6]

The Supreme Court's doctrine governing these occasions embodies a value judgment not hard to comprehend in the context of a practical consideration common to most instances in which constitutional tensions affecting individual rights come into play, as is evidenced in the case before this Court. In a sense, the conflict between government efficiency interests and personal liberty is strictly not one among equals. Efficiency is a multi-edged sword; it can cut many ways. Government ordinarily possesses more than one effective means to achieve a given public end. Thus, legitimate

efficiency interests can be accommodated by various alternatives, whether legislative or administrative, generally at the government's disposal. Personal freedoms, on the other hand, are far more unique. As individualized by constitutional ideals to embody our sense of human dignity, decency, and fair play, they attach to each individual by promise of the very government which creates those basic rights and is charged to protect them, and upon whose faithful adherence to their underlying principles and aims their enduring enjoyment depends. By reason of this contingency, individual rights may operate one way, or not at all when their exercise is unduly restricted or prohibited by measures of that constituted authority. Worse still is another risk. Sometimes a right, once extinguished, may be gone for good. Few satisfying means may then be available to truly restore to the particular victim or to the larger society the value of the loss.

One concluding observation cannot be overlooked as a consideration in this case. Between the dispute and its resolution hangs a large reality, here the backdrop against which the actuating events have played out. Call it an atmospheric pressure, a heavy weight that, foglike, has loomed densely over every aspect of these 478*478 proceedings. On September 11, 2001, the United States became the target of a murderous attack of international terrorism, unparalleled in its magnitude, and unprecedented in America's national experience. Losses and remembrances of that violence are still fresh in the minds of the American people. The wounds they suffered from it have not yet healed. The Court is not unmindful of the contextual relevance of those circumstances, serving as they do as impulse for some of the Government concerns and measures that gave rise to this litigation, suffusing the legal theories elaborated in the parties' papers, and stoking the fervor and immediacy animating the arguments urged before the Court.

In consequence, the Court's ruling not only takes due account of the force and poignancy of that history but, as this Court noted on another occasion similarly grounded,[7] represents an expression of several critical implications necessarily flowing from it. First, cases engendering intense passions and urgencies to unencumber the Government, enabling it to move in secrecy to a given end with the most expedient dispatch and versatile means, often pose the gravest perils to personal liberties. As the Supreme Court admonished in connection with another event similarly momentous: it is "under the pressing exigencies of crisis[ ] that there is the greatest temptation to dispense with fundamental constitutional guarantees which, it is feared, will inhibit governmental action."[8] Second, it is these conditions that best put the strength of our principles and convictions to the test, and measure our resolve and commitment to them. Third, it is precisely times like these that demand heightened vigilance, especially by the judiciary, to ensure that, as a people and as a nation, we steer a principled course faithful and true to our still-honored founding values. The high stakes here pressing the scales thus compel the Court to strike the most sensitive judicial balance, calibrating by delicate increments toward a result that adequately protects national security without unduly sacrificing individual freedoms, that endeavors to do what is just for one and right for all.

A. *DOE'S RECEIPT OF AN NSL*[9]

After receiving a call from an FBI agent informing him that he would be served with an NSL, Doe received a document, printed on FBI letterhead, which stated that, "pursuant to Title 18, United States Code (U.S.C.), Section 2709" Doe was "directed" to provide certain information to the Government.[10] As required by the terms of § 2709, in the NSL the FBI "certif[ied] that the information sought [was] relevant to an authorized investigation to protect against international terrorism 479*479 or clandestine intelligence activities."[11] Doe was "further advised" that § 2709(c) prohibited him, or his officers, agents, or employees, "from disclosing to *any person* that the FBI has sought or obtained access to information or records under these provisions."[12] Doe was "requested to provide records responsive to [the] request *personally*" to a designated individual,[13] and to not transmit the records by mail or even mention the NSL in *any*telephone conversation.

After a subsequent conversation with the same FBI agent, Doe decided to consult ACLU lawyers. The parties dispute the nature of Doe's exchange with the FBI agent, though it is ultimately immaterial to this motion. Doe contends that the agent gave him permission to speak with an attorney; the agent claims that Doe merely informed the agent that he (Doe) would be consulting an attorney. Doe has not complied with the NSL request, and has instead engaged counsel to bring the present lawsuit.

B. *§ 2709 IN GENERAL*

As stated above, § 2709 authorizes the FBI to issue NSLs to compel communications firms to produce certain customer records whenever the FBI certifies that those records are relevant to an authorized international terrorism or counterintelligence investigation, and the statute also categorically bars NSL recipients from disclosing the inquiry.[14] In relevant part, it states:

(a) Duty to provide. — A wire or electronic communication service provider shall comply with a request for subscriber information and toll billing records information, or electronic communication transactional records in its custody or possession made by the Director of the Federal Bureau of Investigation under subsection (b) of this section.

(b) Required certification. — The Director of the Federal Bureau of Investigation, or his designee in a position not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau field office designated by the Director, may —

(1) request the name, address, length of service, and local and long distance toll billing records of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the name, address, length of service, and toll billing records sought are relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States; and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee) certifies in writing to the wire or electronic communication service provider to which the request is made that the information sought is 480*480 relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(c) Prohibition of certain disclosure. — No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section.[15]

Subsection (d) limits the FBI's ability to disseminate information collected from an NSL, and subsection (e) requires the FBI to periodically report to Congress about its use of NSLs.[16]

Section 2709 is one of only a handful of statutes authorizing the Government to issue NSLs. The other NSL statutes authorize the Government to compel disclosure of certain financial and credit records which it certifies are relevant to international terrorism or counterintelligence investigations, and to compel disclosure of certain records of current or former government employees who have (or have had) access to classified information.[17] In each case, the NSL statutes categorically bar the NSL recipient or its employees or agents from ever disclosing the Government's inquiry.[18] As stated, NSLs are distinguished from other administrative subpoenas in that NSLs pertain to national

security issues and are cloaked in secrecy. The Court discusses other administrative subpoenas in more detail below in Section I.D.1.

C. *LEGISLATIVE HISTORY*

Section 2709 was enacted as part of Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"),[19] which sought to "protect privacy interests" in "stored wire and electronic communications" while also "protecting the Government's legitimate law enforcement needs."[20] Congress modeled Title II of the ECPA upon the Right to Financial Privacy Act ("RFPA") of 1978,[21] which espoused similar privacy goals for financial records.[22] The RFPA was "intended to protect the customers of financial institutions from unwarranted intrusion into their records while at the same time permitting legitimate law enforcement activity."[23]

The RFPA was an explicit "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."[24] 481*481 In passing Title II of the ECPA eight years later, Congress feared that customers of electronic communications services would likewise find little Fourth Amendment protection from Government access to their records, thus creating the need for privacy legislation.[25]

Generally speaking, Title II (as amended) allows the Government to obtain stored electronic communications information without the subscriber's permission only through compulsory process, such as a subpoena, warrant, or court order.[26] Section 2709 is a notable exception to these privacy protections because it permits the FBI to request records upon a mere self-certification — issued to the ISP or telephone company, not to the subscriber or to any court — that its request complies with the statutory requirements.[27] As first enacted, § 2709 required electronic communication service providers to produce "subscriber information," "toll billing records information," or "electronic communication transactional records," upon the FBI's internal certification that (1) the information was "relevant to an authorized foreign counterintelligence investigation" and that (2) there were "specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains [was] a foreign power or an agent of a foreign power."[28]

Before the ECPA, the FBI had been issuing non-mandatory NSLs to communications providers, who, in most cases, complied voluntarily.[29] However, because carriers in states with strict privacy laws had recently been resisting those requests, the FBI sought to have mandatory, preemptive federal legislation supporting its issuance of NSLs.[30]The Senate Intelligence Committee agreed that federal law should mandate NSL compliance, but the Committee concluded that the FBI's *mandatory* NSL power should be more limited in scope than what the FBI had been seeking under voluntary NSL arrangements.[31] Whereas communications service providers had been volunteering to produce records which the FBI certified were merely "relevant to FBI counterintelligence activities," the Intelligence Committee's reported version of § 2709 limited the FBI's mandatory authority to "only obtain records where there are 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 482*482 agent of a foreign power."[32] The Committee stated that it believed that the strict standards of the proposed statute were consistent with both the First and Fourth Amendments and concluded that the "federal courts have not required either a judicial warrant or a probable cause standard for access to telephone subscriber information or toll billing record information."[33] The Court notes, however, that the version of § 2709 considered by the Intelligence Committee did not authorize the FBI to obtain electronic communication transactional records; that provision was added to the statute when it was integrated into the ECPA by the Judiciary Committee.[34]

In 1993, Congress broadened § 2709 by relaxing the required nexus to a foreign power.[35] The amended statute allowed the FBI to obtain records "where: (1) there is a contact with a suspected intelligence officer or a suspected terrorist, or (2) the circumstances of the conversation indicate ... that it may involve spying or an offer of information."[36] The original version of 483*483 the statute had required the FBI to certify that the communications service subscriber whose records were sought was *himself* a foreign agent or power, thereby preventing the FBI from issuing mandatory NSLs to obtain the records of, for example, persons who merely *communicated with* foreign agents regarding terrorism or clandestine intelligence information.[37] The Committee recognized that "the national security letter is an extraordinary device" and that "new applications are disfavored," but it "concluded that [the] narrow change in § 2709 to meet the FBI's focused and demonstrated needs was justified."[38]

The next and most recent major revision to § 2709 occurred in October 2001, as part of the USA PATRIOT Act of 2001 ("Patriot Act").[39] In short, the Patriot Act removed the previous requirement that § 2709 inquiries have a nexus to a foreign power, replacing that prerequisite with a broad standard of relevance to investigations of terrorism or clandestine intelligence activities.[40] In hearings before the House Judiciary Committee on September 24, 2001, the Administration submitted the following explanation for the proposed change:

NSL authority requires both a showing of relevance and a showing of links to an "agent of a foreign power." In this respect, [it is] substantially more demanding than the analogous criminal authorities, which require only a certification of relevance. Because the NSLs require documentation of the facts supporting the "agent of a foreign power" predicate and because they require the signature of a high-ranking official at FBI headquarters, they often take months to be issued. This is in stark contrast to criminal subpoenas, which can be used to obtain the same information, and are issued rapidly at the local level. In many cases, counterintelligence and counterterrorism investigations suffer substantial delays while waiting for NSLs to be prepared, returned from headquarters, and served. The section would streamline the process of obtaining NSL authority....[41]

The House Judiciary Committee agreed that "[s]uch delays are unacceptable" and stated in its October 11, 2001, report that 484*484 the Patriot Act would "harmonize[ ]" § 2709 "with existing criminal law where an Assistant United States Attorney may issue a grand jury subpoena for all such records in a criminal case."[42]

D. *NSLs AND OTHER INFORMATION-GATHERING AUTHORITY*

It is instructive to place the Government's NSL authority in the context of other means by which the Government gathers information of the type covered by § 2709 because Congress (in passing and amending the NSL statutes) and the parties here (in contesting § 2709's constitutionality) have drawn analogies to those other authorities as grounds for or against its validity. The relationship of § 2709 to other related statutes supplies a backdrop for assessing congressional intent and judging the validity of the law on its face and as applied. In addition, an analysis of these analogous information-gathering methods indicates that NSLs such as the ones authorized by § 2709 provide fewer procedural protections to the recipient than any other information-gathering technique the Government employs to procure information similar to that which it obtains pursuant to § 2709.

1. *Administrative Subpoenas*

The most important set of statutes relevant to this case are those authorizing federal agencies to issue administrative subpoenas for the purpose of executing the particular agency's function. Ordinary administrative subpoenas, which are far more common than NSLs, may be issued by most federal agencies, as authorized by the hundreds of applicable statutes in federal law. For example,

the Internal Revenue Service (IRS) may issue subpoenas to investigate possible violations of the tax code,[43] and the Securities Exchange Commission (SEC) may issue subpoenas to investigate possible violations of the securities laws.[44] More obscure examples include the Secretary of Agriculture's power to issue subpoenas in investigating and enforcing laws related to honey research,[45] and the Secretary of Commerce's power to issue subpoenas in investigating and enforcing halibut fishing laws.[46]

There is a wide body of law which pertains to administrative subpoenas generally. According to the Government's central theory in this case, those standing rules would presumably also apply to NSLs, even if not so explicitly stated in the text of the statute. Where an agency seeks a 485*485 court order to enforce a subpoena against a resisting subpoena recipient, courts will enforce the subpoena as long as: (1) the agency's investigation is being conducted pursuant to a legitimate purpose, (2) the inquiry is relevant to that purpose, (3) the information is not already within the agency's possession, and (4) the proper procedures have been followed.[47] The Second Circuit has described these standards as "minimal."[48] Even if an administrative subpoena meets these initial criteria to be enforceable, its recipient may nevertheless affirmatively challenge the subpoena on other grounds, such as an allegation that it was issued with an improper purpose or that the information sought is privileged.[49]

Unlike the NSL statutes, most administrative subpoena laws either contain no provision requiring secrecy, or allow for only limited secrecy in special cases. For example, some administrative subpoena statutes permit the investigating agency to apply for a court order to temporarily bar disclosure of the inquiry, generally during specific renewable increments or for an appropriate period of time fixed by the court, where such disclosure could jeopardize the investigation.[50]

Even absent a particular secrecy statute, someone who, with the intent to obstruct an investigation, alerts the target of an investigation that a subpoena has been issued could theoretically face criminal obstruction of justice charges under a federal statute that imposes criminal sanctions upon any person who, among other things, "corruptly ... endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States."[51]

2. *Subpoena Authority in the Criminal Context*

In its role as a party to a federal criminal proceeding (including a grand jury proceeding), the Government has broad authority to issue a subpoena to obtain witness testimony or "*any* books, papers, documents, data, or other objects the subpoena 486*486 designates."[52] Although such subpoenas "are issued in the name of the district court over the signature of the clerk, they are issued pro forma and in blank to anyone requesting them," and the "court exercises no prior control whatsoever upon their use."[53]

The court becomes involved in the subpoena process only if the subpoenaed party moves to quash the request as "unreasonable or oppressive,"[54] or if the Government seeks to compel compliance with the subpoena. The reasonableness of a subpoena depends on the context. For example, to survive a motion to quash, a subpoena issued in connection with a criminal trial "must make a reasonably specific request for information that would be both relevant and admissible at trial."[55] By contrast, a grand jury subpoena is generally enforced as long as there is a "reasonable possibility that the category of materials the Government seeks will produce information relevant to the general subject of the grand jury's investigation."[56] Considering the grand jury's broad investigatory power and minimal court supervision, it is accurate to observe, as the Second Circuit did long ago, that "[b]asically the grand jury is a law enforcement agency."[57]

While materials presented in a criminal trial setting are generally public,[58] the federal rules impose stringent secrecy requirements on certain grand jury participants, including the attorneys, court reporters, and grand jurors.[59] Those secrecy rules make no mention of a subpoena recipient or a witness, both of whom are ordinarily free to disclose to anyone the fact that a subpoena was issued or the contents of any information supplied.[60] Some courts have nevertheless permitted the Government to impose a secrecy obligation upon witnesses in cases of compelling need. The Eleventh Circuit, for example, has held that a district court's authority to protect the integrity of grand jury process gave it power to prevent witnesses from disclosing materials prepared for or testimony given in grand jury proceedings.[61] As an exception to this rule, officers of financial institutions and insurance companies face criminal penalties for disclosing, with the intent to obstruct a judicial proceeding, either the fact that a grand jury subpoena has been issued or its contents.[62] More generally, a subpoena recipient 487*487 who, with the intent to obstruct a criminal investigation, alerts the target of an investigation that a subpoena had been issued could theoretically face criminal obstruction of justice charges.[63]

In certain contexts, the Government may issue subpoenas related to criminal investigations even without initiating a formal criminal proceeding. For example, the United States Attorney General is authorized to issue administrative subpoenas, without convening a grand jury, to investigate federal narcotics crimes,[64] racketeering crimes,[65] health care related crimes,[66] and crimes involving the exploitation of children.[67] In each of these instances, the administrative process is governed by the general rules described above, providing safeguards of judicial review.[68]

3. *Background Rules Governing Disclosure of Stored Electronic Communications*

Title II of the ECPA, in which § 2709 was enacted, sets forth an intricate framework by which electronic communications providers, such as ISPs and phone companies, may be compelled to disclose stored electronic information to the Government. The framework described below operates independently of the rules governing NSLs issued pursuant to § 2709, but may aid with interpretation of § 2709.

The Government may obtain basic subscriber information[69] merely by issuing an authorized administrative subpoena, trial subpoena, or grand jury subpoena, and the Government need not notify the subscriber of the request.[70]

If the Government gives prior notice to the subscriber, or otherwise complies with certain delayed notice procedures,[71] the Government may also subpoena the *contents* of electronic communications which are either (1) retained on a system for storage purposes (*e.g.,* opened email which remains on an ISP's server), or (2) retained, for more than 180 days, in intermediate or temporary storage (*e.g.,* unopened email on an ISP's server).[72] For 488*488 the Government to obtain the contents of electronic communications kept for 180 days or less in intermediate or temporary storage (*e.g.,* unopened email on an ISP's server), it must obtain a search warrant under Federal Rule of Criminal Procedure 41, or the state equivalent.[73] In other words, the Government would have to appear before a neutral magistrate and make a showing of probable cause.[74] The Government may also obtain a court order requiring an electronic communications service provider to turn over transactional and content information by setting forth "specific and articulable facts showing that there are reasonable grounds to believe that" the information sought is "relevant and material to an ongoing criminal investigation."[75]

The ECPA permits the Government to seek a court order prohibiting the communications provider from revealing the Government's inquiry "for such period as the court deems appropriate" if the court determines that such disclosure, among other things, would result in "destruction of or tampering with evidence" or "seriously jeopardizing an investigation or unduly delaying a trial."[76]

4. *Mail*

Government law enforcement agencies are authorized to request the Postal Inspector to initiate a so-called "mail cover" to obtain any information appearing on the outside of a particular piece of mail.[77] Among other grounds, the law enforcement agency can obtain a mail cover by "specify[ing] the reasonable grounds to demonstrate the mail cover is necessary" to "[p]rotect the national security" or to "[o]btain information regarding the commission or attempted commission of a crime."[78] There is no requirement that the mail sender or recipient be notified of the mail cover.

The Government must obtain a warrant based upon probable cause to open and inspect sealed mail because the contents of mail are protected by the Fourth Amendment.[79] As the Supreme Court established long ago: "Whilst in the mail, [a person's papers] can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household."[80]

5. *Pen Registers and Trap and Trace Devices*

Pen registers and trap and trace devices record certain electronic communications data indicating the origins and destinations 489*489 of various "dialing, routing, addressing, or signaling information," *e.g.,* the phone numbers dialed to and from a telephone.[81] In criminal investigations, the Government must apply for a court order, renewable in 60-day increments, to install or collect data from such devices, though the standard for issuing such an order is relatively low.[82] The Government need only show that "the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation."[83]

The person owning the communications device is prohibited, unless otherwise directed by court order, from disclosing the fact that a pen register or trap and trace device is in effect.[84]

6. *Wiretaps and Electronic Eavesdropping*

The Fourth Amendment protects against warrantless Government wiretapping.[85]Federal legislation specifies the procedures by which law enforcement officials may obtain a court order to conduct wiretaps and other forms of electronic eavesdropping.[86]The requirements are rigorous. Among other things, the Government must show that: (1) "there is probable cause for belief that an individual is committing, has committed, or is about to commit" one of a list of enumerated crimes; (2) "there is probable cause for belief that particular communications concerning that offense will be obtained through such interception"; and (3) "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[87]Such orders are not available "for any period longer than is necessary to achieve the objective of the authorization," subject to a renewable maximum of 30 days.[88] The communications provider is prohibited from disclosing that a wiretap or electronic surveillance is in place, "except as may otherwise be required by legal process and then only after prior notification" to the appropriate law enforcement authorities.[89]

7. *Foreign Intelligence Surveillance Act*

The Foreign Intelligence Surveillance Act of 1978 ("FISA") establishes standards for the Government's domestic electronic surveillance of foreign governments and their agents.[90] The Government may conduct such surveillance, even without a court order, as long as the Attorney General certifies, among other things, that: (1) the communications at issue would be "exclusively between or among foreign powers" or involve "the acquisition of technical intelligence, other than the spoken communications of individuals, from property or premises under the open and exclusive

control of a foreign power"; (2) "there is no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party"; and (3) the Government will apply certain so-called "minimization procedures" to limit the possibility of impermissible490*490 collateral surveillance.[91] In such circumstances, the Attorney General may direct the communications provider to cooperate "in such a manner as will protect [the] secrecy" of the surveillance.[92]

To conduct any broader types of surveillance, the Government must obtain a formal order from a special FISA-created court.[93] The application must specify, among other things, the type of surveillance proposed, the facts supporting the Government's belief that the surveillance pertains to a foreign power, and the minimization procedures which would be taken.[94] The Government must also certify "that a significant purpose of the surveillance is to obtain foreign intelligence information" and that the "information cannot reasonably be obtained by normal investigative techniques."[95] Before issuing the surveillance order, the FISA court must find, among other things, that there is "probable cause to believe" that the surveillance target is a foreign power or a foreign agent, that the proposed minimization procedures meet the statutory requirements, and, if the target is a United States person, that the facts in the Government's certification are not clearly erroneous.[96]

FISA surveillance orders are issued only "for the period necessary to achieve [the] purpose" of the application, with an extendable maximum of either 90 days, 120 days, or one year, depending on the nature of the surveillance target.[97] The court's order may direct a communications provider to cooperate "in such a manner as will protect [the] secrecy" of the surveillance.[98]

The FISA also authorizes the Government to apply to the FISA court "for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities...."[99] Such an application need only specify that the inquiry is part of an authorized investigation and in accordance with the appropriate guidelines.[100] Recipients of such an order are prohibited from disclosing to anyone (except those whose assistance is necessary to comply with the subpoena) that the inquiry was made.[101]

Finally, FISA authorizes the Government to apply to the FISA court for a an order, renewable in 90-day increments, to install a pen register or trap and trace device as part of "any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[102] The Government need only certify to the court that it will likely obtain information relevant to a proper inquiry.[103] Just as in the criminal context, the person owning the 491*491 communications device is prohibited, unless otherwise directed by court order, from disclosing the fact that a pen register or trap and trace device is in effect.[104]

III. *SUMMARY JUDGMENT STANDARD*

The Court may grant summary judgment only if "there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law."[105]Here, the Court concludes that no facts material to the disposition of the case are in dispute and that this case presents pure legal questions ripe for decision on summary judgment.

IV. *DISCUSSION*

A. *SECTION 2709, AS DRAFTED, RAISES SERIOUS CONSTITUTIONAL QUESTIONS*

Besides placing in full context the parties' conflicting arguments relating to statutory construction of § 2709, the legislative history and grid cross-referencing other information-gathering laws Congress has enacted is described above in such detail to serve another purpose. The contrast of the statutory scheme reveals some similarities amid striking differences among the laws. It depicts comparable provisions inserted in some legislation but omitted from others; secrecy, enforcement and judicial review rules incorporated more in some laws, less in others; enactments reflecting mere clarifications in some instances, manifestly substance in others; and some overall requirements sometimes overlapping, sometimes at odds.

The large divergence brings to light a substantial quandary affecting the task of judicial interpretation. Are the various differences between § 2709 and other analogous statutes, extensive as the discrepancies are, simply the product of poor or hasty congressional drafting? Are the apparent gaps inadvertent or deliberate, legislative nuances or simply oversight? Or do such diverse textual approaches embody Congress's considered intent to achieve distinct objectives by varying means, while fully cognizant of the similarities among the statutes? Do the conflicts and omissions pertain to details that, as the Government here argues, can be readily filled in by the Court by application of canons of statutory construction? Or, to the contrary, as Plaintiffs contend, do the legislative distinctions implicate provisions far too substantive and fundamental to be reconciled by valid exercise of judicial power?

The very existence of such an intricate matrix of rules codified in separate statutes governing similar multidimensional issues suggests congressional design that this Court hesitates to pass judgment upon if not necessary to a sufficient adjudication of this dispute. The Court does not feel at ease with simply ascribing the disparate legislative treatment of secrecy, enforcement and judicial review procedures in these various enactments to innocuous drafting error, or to distinctions with no discernible purpose. However, the Court cannot fairly infer clear congressional intent in the enactment of § 2709 solely by comparing it with other complex, analogous statutes.[106]

492*492 The NSL statutes, particularly § 2709, present interpretive challenges in at least three respects, the first two of which have a direct bearing on the motions now before the Court. First, while two of the NSL statutes explicitly state that an NSL recipient may disclose the Government's inquiry to persons whose assistance is necessary to comply with the demands of the NSL, the other statutes, including § 2709, appear by their telltale silence on that point, to preclude any disclosures.[107] None of the statutes explain whether consulting an attorney constitutes disclosure, even where an attorney's assistance may be necessary for a recipient to comply with an NSL, and none of the statutes states whether the ban on disclosure may ever be lifted by a court. Second, the statutes contain no explicit provision for the Government to seek judicial enforcement of an NSL against a recipient who refuses to comply, nor is there any provision expressly authorizing an NSL recipient to affirmatively challenge, administratively or judicially, the propriety of an NSL request.[108] Third, there is no explicit provision in the statutes imposing penalties against a person who fails to comply with an NSL.[109]

The absence of clear enforcement mechanisms has led the Chairman of the House Subcommittee on Crime, Terrorism, and Homeland Security to express the concern that the current versions of § 2709 and other NSL statutes may be considered hortatory, and to declare the intent of H.R. 3179, a bill currently in committee, to be to cure that deficiency.[110] Significantly, 493*493 it is precisely the Government's ability to seek judicial enforcement of the subpoena, together with its corollary — the reverse side of the same coin, the ability of the recipient to seek judicial review of the FBI's issuance or enforcement of an NSL — that the Government contends in this case the Court could fairly infer to already exist under current law.[111]

Several bills pending in Congress, including H.R. 3179, demonstrate Congress's and the Government's recognition that the NSL statutes could have been drafted with greater particularity and uniformity. H.R. 3179 would address two of the issues listed above by explicitly providing for judicial enforcement of NSLs and by imposing criminal penalties of up to five years' imprisonment for persons who unlawfully disclose that they have received an NSL.[112]

Also pending in Congress is a bill, H.R. 3037, which would permit the Attorney General to issue NSLs whenever, in his judgment, the information sought would be "relevant or material" to "any investigation concerning a Federal crime of terrorism."[113] That bill avoids all of the interpretive problems associated with § 2709 detailed above. Like H.R. 3179, H.R. 3037 would authorize judicial enforcement and impose penalties upon persons who wrongfully disclosed the Government's inquiry.[114] The bill would also permit an NSL recipient to disclose the inquiry to "those persons to whom such disclosure is necessary in order to comply" with the NSL, and to "an attorney to obtain legal advice."[115]

A third bill now proceeding through the Senate, entitled the "Judicially Enforceable Terrorism Subpoenas Act of 2004,"[116] also provides clarity where § 2709 is now murky. It does so by specifically authorizing the recipient of an administrative subpoena issued pursuant to the proposed statute to consult with an attorney and "those persons to whom such disclosure is necessary in order to comply with the subpoena," and by specifically stating that judicial review is available to enforce or 494*494 modify the subpoena, or to modify the nondisclosure requirement imposed under the statute.[117]

As explained below, even if the Court were to agree with the Government that § 2709 should be read to allow: (1) an NSL recipient to consult with an attorney and others necessary to enable compliance with the letter; and (2) an NSL recipient to challenge, or the Government to enforce, an NSL in court, the Court would still hold that the statute, as currently applied by the FBI, exerts an undue coercive effect on NSL recipients. The form language of the NSL served upon Doe, preceded by an FBI phone call, directed him to*personally* provide the information to the FBI, prohibited him, his officers, agents or employees from disclosing the existence of the NSL to *anyone,* and made no mention of the availability of judicial review to quash or otherwise modify the NSL or the secrecy mandated by the letter. Nor did the FBI inform Doe personally that any such judicial review of the issuance of the NSL or the secrecy attaching to it was available. The Court concludes that, when combined, these provisions and practices essentially force the reasonable NSL recipient to immediately comply with the request. This lack of effective process, at least as applied, entails issues far too fundamental for the Court to read as having been sufficiently addressed in the operation of § 2709 in this case. In the Court's judgment, as further elaborated below, that absence renders § 2709, as applied, unconstitutional, in violation of the Fourth Amendment.

B. *AS APPLIED HERE, SECTION 2709 LACKS PROCEDURAL PROTECTIONS NECESSARY TO VINDICATE CONSTITUTIONAL RIGHTS*

1. *Section 2709 And The Fourth Amendment*[118]

The Fourth Amendment prohibits the Government from conducting "unreasonable searches and seizures," which generally means that any search or seizure must be performed pursuant to a valid 495*495 warrant based upon probable cause.[119] As the Second Circuit has declared: "It is fundamental that governmental searches and seizures without warrant or probable cause are per se unreasonable under the Fourth Amendment unless they fall within one of the Amendment's few established and well-delineated exceptions."[120] The Fourth Amendment's protection against unreasonable searches applies to administrative subpoenas, even though issuing a subpoena does not involve a literal physical intrusion or search.[121] In so doing, the Supreme Court explained that

the Fourth Amendment is not "confined literally to searches and seizures as such, but extends as well to the orderly taking under compulsion of process."[122]

However, because administrative subpoenas are "at best, constructive searches," there is no requirement that they be issued pursuant to a warrant or that they be supported by probable cause.[123] Instead, an administrative subpoena needs only to be "reasonable," which the Supreme Court has interpreted to mean that (1) the administrative subpoena is "within the authority of the agency;" (2) that the demand is "not too indefinite;" and (3) that the information sought is "reasonably relevant" to a proper inquiry.[124]

While the Fourth Amendment reasonableness standard is permissive in the context of administrative subpoenas, the constitutionality of the administrative subpoena is predicated on the availability of a neutral tribunal to determine, after a subpoena is issued, whether the subpoena actually complies with the Fourth Amendment's demands. In contrast to an actual physical search, which must be justified by the warrant and probable cause requirements occurring *before* the search, an administrative subpoena "is regulated by, and its justification derives from, [judicial] process" available *after* the subpoena is issued.[125]

Accordingly, the Supreme Court has held that an administrative subpoena "may not be made and enforced" by the administrative agency; rather, the subpoenaed party must be able to "obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply."[126] In sum, longstanding Supreme Court doctrine makes clear that an administrative subpoena statute is consistent with the Fourth Amendment when it is subject to "judicial supervision" and "surrounded by every safeguard of judicial restraint."[127]

Plaintiffs contend that § 2709 violates this Fourth Amendment process-based 496*496guarantee because it gives the FBI alone the power to issue as well as enforce its own NSLs, instead of contemplating some form of judicial review. Although Plaintiffs appear to concede that the statute does not authorize the FBI to literally enforce the terms of an NSL by, for example, unilaterally seizing documents or imposing fines, Plaintiffs contend that § 2709 has the *practical* effect of coercing compliance.

Specifically, Plaintiffs stress that the statute has no provision for judicial enforcement or review, and that theoretically any judicial review an NSL recipient sought would violate the express terms of the non-disclosure provision. For example, if an NSL recipient thought that an NSL request was unreasonable or otherwise unlawful — because, for instance, the underlying investigation was not duly "authorized," was initiated "solely on the basis of activities protected by the first amendment to the Constitution of the United States," or did not involve "international terrorism or clandestine intelligence activities,"[128] as § 2709 demands — he would have no specific statute under which to challenge the request. More fundamentally, the literal terms of the non-disclosure provision would bar the recipient from even consulting an attorney to file such a challenge. Even if he were to challenge the NSL on his own, the recipient would necessarily have to disclose the fact of the NSL's issuance to the clerk of court and to the presiding judge, again, in violation of the literal terms of the non-disclosure provision.

Rather than dispute the Plaintiffs' interpretation of the relevant constitutional doctrine, the Government's response to these arguments endeavors to heavily repair the statute, essentially by splicing together a string of judicially-sanctioned implications, glosses, or outright patchwork of the various gaps Congress left in the statute, whether inadvertently or purposefully. First, as discussed above, the Government claims that the statute implicitly affords an NSL recipient the opportunity to challenge an NSL on the same terms as would be available to any other subpoena recipient, *i.e.,* to either resist the Government's enforcement action, or to affirmatively file a motion to quash. Second,

the Government reads the statute to implicitly permit disclosure to an attorney in connection with such a challenge. Third, the Government would recognize an additional exception for disclosure to other officers, employees, or agents whose assistance may be reasonably necessary for the recipient to comply with the NSL request.

The path that, according to the Government, would lead to the above "correct" reading of § 2709 is as follows. First, concerning the judicial enforcement issue, § 2709 is conspicuously silent on how the Government's demand for records is to be enforced. Plaintiffs concede that § 2709 does not authorize the FBI to resort to "self-help" in enforcing the statute, thus leaving the possibilities that enforcement falls to either the court system, to no one at all, or, worse yet, to other forms of administrative pressures and extra-legal methods that such congressional silences and statutory lacunae may be prone to invite. Following the Government's theory, it is inconceivable that Congress intended compliance with § 2709 to be a mere courtesy in light of § 2709's mandatory phrases, such as "duty" and "shall comply."[129] The obvious purpose of the 497*497 statute — to obtain important records quickly — would be eviscerated, the argument goes, if an NSL recipient could treat the NSL as if it were a piece of junk mail to be tossed in the trash can and ignored without consequence. Furthermore, courts have long recognized the "sharp distinction between agency power to *issue* subpoenas and judicial power to*enforce* them."[130] Accordingly, the Government concludes that it would make sense that an NSL, which is in the family of administrative subpoenas, would follow that ordinary course.

Second, regarding the disclosure issue, the Government points out that the duty the statute imposes upon the NSL recipient to produce information to the FBI falls upon the designated "wire or electronic communication service provider,"[131] which in the typical case is likely to be a corporate entity, as opposed to an individual. Because "a corporation must act through agents,"[132] it is fair to assume that the various agents of a corporation, including its attorneys, would be involved in fulfilling the corporation's duty. The Government thus stresses that nothing in § 2709 suggests that the duty falls uniquely to the individual who happens to be in immediate receipt of the NSL. In this view, in parallel with this collective duty to produce information, by the very terms of the statute the prohibition upon disclosure is also apparently directed at more than one person: "No wire or electronic communication service provider, *or officer, employee, or agent thereof,* shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section."[133] The statute's reference to officers, employees and agents again suggests that those people (as opposed to merely the individual recipient) would be aware that the NSL was issued, presumably because some of those people could have involvement in fulfilling the request.

Invoking practicalities and common sense, the Government suggests that it would be unable to precisely identify the person within a company who would be capable of complying with the NSL request and thus would expect certain employees or agents, including attorneys, to play a role in gathering the information sought. To illustrate this point, assuming an executive at a telephone company is served with an NSL requesting that he produce detailed records of a particular subscriber, and that, as is likely, the executive is not familiar with the mechanics of sophisticated data retrieval, and that the statute actually barred the recipient's communication with *anyone,* the executive would be in the impossible position of being incapable of complying with what the law demanded. On this basis, the Government contends that it is doubtful Congress would have intended such a rigid reading of § 2709(c).

The Government notes that its interpretation of § 2709(c) finds at least some support in the legislative history, as well. Congress added NSL authority pertaining to credit records in 1996, and that statute 498*498 explicitly permits disclosure to persons "necessary to fulfill" the NSL request.[134] Congress considered that language as a "clarification" of (as opposed to a substantive

change from) the parallel NSL statutes because "practicalities would dictate that the provision not be interpreted to exclude such disclosure."[135]

Finally, in support of its construction of § 2709, the Government points to two cases that have interpreted wiretap laws to implicitly permit an accused unlawful wiretapper to disclose the contents of the wiretap to his attorneys for the purpose of preparing a defense.[136] Addressing this point, for example, the Sixth Circuit stated that the so-called "defense exception" was a "necessary element of wiretap law."[137] In another case, a district court observed that to construe the wiretapping laws to prevent an accused from using the intercepted communications in his own defense "would be so incompatible with basic notions of fairness in adversary proceedings that it might well raise questions regarding the statute's constitutionality."[138] Closing its argument on this point, the Government concludes that these cases recognize both that disclosures to attorneys are unique and that statutory interpretations producing absurd and unworkable results should be avoided.

The Court accepts that it should recognize a plausible interpretation of § 2709 that would salvage the statute. As the Supreme Court has instructed: "if an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is fairly possible, [courts] are obligated to construe the statute to avoid such problems."[139] Conceivably, these aspects of the Government's construction of § 2709 may be deemed "fairly possible," and thus the ordinary rule for rescuing constitutionally dubious statutes from facial invalidity may come into play at this point. Application of this doctrine here poses severe difficulties, however, because the anchoring of the Government's theory in the legislative scheme is far from clear and convincing, raising tensions with other countervailing principles of statutory interpretation and, more fundamentally, inviting risk to the proper functioning of the judiciary in the separation of powers our nation's governance constitutionally demands. As the Supreme Court has also instructed, the courts "cannot press statutory construction `to the point of disingenuous evasion' even to avoid a constitutional question."[140]

In examining the Government's construction of § 2709, the Court makes several 499*499preliminary observations as backdrop for its strong reservations to endorse it outright, even if in theory that reading were plausible. First, the suggested interpretation does not relate to a reading of particular words or provisions actually expressed in the statute. Rather, it requires listening to the law's "sounds of silence"[141] to decipher the meaning of what is unsaid; in other words, it is about specific terms not contained in § 2709 at all, though expressly provided for in other laws within the family of legislation dealing with government information-gathering in support of national security investigations and general law enforcement. This Court must base its interpretation of the statute primarily in the actual *text* of the statute, on what the statute explicitly says rather than on what it fails to say.[142] Second, to fully reach and give effect to the Government's proposal entails inserting into the law not just one, but several distinct terms the Government seeks to incorporate by implication: that the statute permits disclosure by the recipient for the purposes of seeking the assistance of counsel; that disclosure is also permitted to other officers, employees and agents; and that judicial process is available either to challenge or to enforce an NSL. Moreover, as will be discussed later, to save the statute the Court would need to go further and rule by similar means that the interpretive stretch does not embrace a vital term the Government's theory expressly rejects: that the non-disclosure ban cannot be categorical and perpetual, and that a mechanism must exist to permit judicial modification of the absolute, indefinite secrecy § 2709(c) imposes. In this respect, the Court must note that the more and the deeper the interstices in a law a judge is called upon to fill, the more what the enterprise demands is not construction of a statute but its emendation by the court, effectively an exercise of judicial legislation in order to repair and rescue the enactment by furnishing through this back channel the missing terms Congress itself did not provide.

More significantly, the Court's interpretation of § 2709, in any faithful observance of the canons of statutory construction, cannot consider that provision strictly in isolation. As made clear above in the

lengthy overview of the rules pertaining to the Government's information-gathering authority, § 2709 does not represent a discrete, stand-alone instance of legislation. Rather, it is but one point in a constellation of other laws, a part and pattern of a larger congressional design generally interrelated by the common purpose of facilitating various forms of investigations and law enforcement proceedings. As is apparent from the statutes' diverse subjects, policy aims and textual differences, however, there is no compelling evidence that Congress has intended to blend the national policy and security interests implicated in the whole body of these laws and to view them all as necessarily demanding a uniform degree of secrecy or procedural safeguards. In this sense, the methods and process Congress has authorized the FBI to undertake in administering NSLs cannot be strictly equated with those traditionally associated with the investigation or prosecution of the ordinary criminal proceeding.

In this case, therefore, the effect of inserting by judicial interpretation the substantial procedural and individual rights 500*500 protections palpably absent from § 2709 — the task the Government would have the Court assume — would be to conform the statute with the requirements of legislation belonging to the same genus, but not altogether the same species, thus essentially converting § 2709 into a mirror image of other laws Congress has enacted or contemplates in which it did see fit to explicitly include the precise terms the Government seeks to engraft onto § 2709 by judicial grace.

The course the Government urges poses several conceptual difficulties for the Court. First, it is at odds with statutory construction principle and caselaw, cited above, dealing with comparable competing interpretations deriving from different statutes.[143] If Congress took affirmative steps to legislate the provisions in question in other statutes, it may have been aware of them and of their implications when it enacted and later amended § 2709 with those standards omitted.

Second, the Government's theory may not be supported by an alternate reading of congressional intent that could reasonably be drawn from the enactment of § 2709. In light of the sensitivity and overarching national priority associated with the purposes of the NSL statutes — international terrorism and counter-intelligence investigations — as well as the gravity of the events that supplied the propelling force and context for the passage and recent amendments of § 2709, one might fairly infer that the absence of any reference to judicial review is the product of Congressional intent. Specifically, § 2709 may convey that Congress meant the statute to serve as a more stringent law enforcement tool, one affording greater investigative powers, leeway and flexibility to the FBI, providing for far more secrecy rather than less, and not necessarily to be substantively or procedurally conflated with related statutes not serving comparably heightened national security concerns. Conversely, for the same reasons and in contradistinction with other information-gathering laws not arising out of national exigencies quite as extreme, 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.

Third, for the Court to give effect to the Government's construction in the face of apparently conflicting, or at best very ambiguous legislative designs, would implicate severe concerns over the proper separation of powers. Such a complex and variable statutory scheme renders it extremely difficult for this Court to find that the absence of particular terms from § 2709 was merely inadvertent or non-substantive, or that even if Congress left holes in § 2709 that it took pains to plug in other similar laws, it falls within the legitimate domain of the Court to function as a legislative repair shop entrusted to perform Congress's labors, and fix Congress's purported errors or omissions at the Government's bidding.

No more compelling evidence exists underscoring the Court's quandary than the various remedial proposals now pending in Congress, discussed above, designed to rectify some of the shortcomings of the NSL statutes, including § 2709. Were the Court to accept the Government's

invitation 501*501 to read § 2709 as the Government proposes, the bills under consideration essentially would be rendered largely moot by the measure of this Court's ruling: NSLs would be read to be judicially enforceable, and disclosures to attorneys and other agents that would be authorized by pending bills would be read into the *existing*statute. What message would that decision convey to Congress? In effect, such a ruling would risk beating Congress to the punch through the exercise of judicial power, and would signal that Congress would not need to further consider corrective action on this score, since the legislative business and public policy ends Congress had openly contemplated would already have been dispatched by judicial decree. The very articulation of the proposition supplies its answer. It should suffice to state that this is not a task even the most intrepid court should lightly countenance.

Despite these severe reservations, in the final analysis the Court need not resolve Plaintiffs' facial challenge to § 2709 on Fourth Amendment grounds for two reasons. First, even if the Court were to accept that the FBI's authority to issue and enforce NSLs pursuant to § 2709 *means* what the Government says it means, the Court's inquiry would not end there with a ruling in favor of the Government. Investing those provisions with the reading the Government accords them does not address the Plaintiffs' distinct claim that *in practice* § 2709 in all or the vast majority of actual cases, by virtue of the statute's unwarranted application by the FBI, *operates* otherwise. The Court concludes that the operation of § 2709 renders it unconstitutional, notwithstanding that, at least in a theoretical sense, a possible reading of portions of the statute as the Government propounds, through extensive judicial tinkering with its silences, may be posited to withstand a Fourth Amendment facial challenge. In particular, deficiencies in the application of § 2709 pertain to the very core issues — access to legal advice and availability of judicial process to enforce and contest the law — upon which Plaintiffs' Fourth Amendment facial challenge is grounded. Because the Court agrees that those protections are vital to satisfy Fourth Amendment standards, it finds the manner in which § 2709 has been applied unwarranted.

The crux of the problem is that the form NSL, like the one issued in this case, which is preceded by a personal call from an FBI agent, is framed in imposing language on FBI letterhead and which, citing the authorizing statute, orders a combination of disclosure *in person* and in complete secrecy, essentially coerces the reasonable recipient into immediate compliance. Objectively viewed, it is improbable that an FBI summons invoking the authority of a certified "investigation to protect against international terrorism or clandestine intelligence activities,"[144] and phrased in tones sounding virtually as biblical commandment, would not be perceived with some apprehension by an ordinary person and therefore elicit passive obedience from a reasonable NSL recipient. The full weight of this ominous writ is especially felt when the NSL's plain language, in a measure that enhances its aura as an expression of public will, prohibits disclosing the issuance of the NSL to "any person." Reading such strictures, it is also highly unlikely that an NSL recipient reasonably would know that he may have a right to contest the NSL, and that a process to do so may exist through a judicial proceeding.

502*502 Because neither the statute, nor an NSL, nor the FBI agents dealing with the recipient say as much, all but the most mettlesome and undaunted NSL recipients would consider themselves effectively barred from consulting an attorney or anyone else who might advise them otherwise, as well as bound to absolute silence about the very existence of the NSL. Furthermore, it is doubtful that an NSL recipient, not necessarily a lawyer, would be willing to undertake any creative exercises in statutory construction to somehow reach the Government's proposed reading of § 2709, especially because that construction is not apparent from the plain language of the statute, the NSL itself, or accompanying government communications, and any penalties for non-compliance or disclosure are also unspecified in the NSL or in the statute. For the reasonable NSL recipient confronted with the NSL's mandatory language and the FBI's conduct related to the NSL, resistance is not a viable option.

The evidence in this case bears out the hypothesis that NSLs work coercively in this way. The ACLU obtained, via the Freedom of Information Act ("FOIA"), and presented to the Court in this proceeding, a document listing all the NSLs the Government issued from October 2001 through January 2003. Although the entire substance of the document is redacted, it is apparent that hundreds of NSL requests were made during that period. Because § 2709 has been available to the FBI since 1986 (and its financial records counterpart in RFPA since 1978), the Court concludes that there must have been hundreds more NSLs issued in that long time span. The evidence suggests that, until now, none of those NSLs was ever challenged in any court. First, the Department of Justice explicitly informed the House Judiciary Committee in May 2003 that there had been *no* challenges to the propriety or legality of any NSLs.[145] Second, the Government's evidence in this case conspicuously lacks any suggestion either that the Government has ever had to resort to a judicial enforcement proceeding for any NSL, or that any recipient has ever resisted an NSL request in such a proceeding or via any motion to quash.[146]

To be sure, the Court recognizes that many other reasons may exist to explain the absence of challenges to NSLs: the communications provider who receives the NSL ordinarily would have little incentive to contest the NSL on the subscriber's behalf; the standard of review for administrative subpoenas similar to NSLs is so minimal that most such NSLs would likely be upheld in court; litigating these issues is expensive; and many citizens may feel a 503*503 civic duty to help the FBI's investigation and thus may willingly comply. Nevertheless, the Court finds it striking that, in all the years during which the FBI has been serving NSLs, the evidence suggests that, until now, no single NSL recipient has ever sought to quash such a directive. The Court thus concludes that in practice NSLs are essentially unreviewable because, as explained, given the language and tone of the statute as carried into the NSL by the FBI, the recipient would consider himself, in virtually every case, obliged to comply, with no other option but to immediately obey and stay quiet.

The Government responds that Doe's arguments on this point are undermined by the very fact that Doe himself consulted an attorney and brought this challenge. The Court disagrees for several reasons. First, so far as the evidence shows, Doe's decision to challenge the NSL is a lone exception in the otherwise consistent record. The constitutional bar marking the limits the Government can permissibly reach in curtailing personal freedoms in the name of national security should not be raised to heights at which all but the most powerfully endowed would feel impelled to remain cowered or content, and none but the well-heeled could stand tall enough to take on a law enforcer's coercive order. If the Court were to take up the Government's invitation and reject Doe's as-applied challenge to the statute until one of the NSL recipients who actually felt intimidated enough by the NSL was moved to bring suit, such a day may never arrive. Moreover, in such a prospect the NSL recipient would presumably have already turned over the requested information to the FBI, further defeating the purpose of subsequent resistance.

Second, the Court finds support for its analysis in caselaw which, in testing the validity of a Government policy or law, recognizes the importance of appreciating its practical effect on a reasonable person, especially as evidenced by the methods and terms the Government employs to convey what it demands and to elicit the desired compliance. In*Bantam Books, Inc. v. Sullivan,*[147] the Rhode Island legislature created an administrative commission to determine whether publications were obscene or objectionable to minors, and where appropriate, to recommend cases to the authorities for prosecution. In accordance with its practice, the commission sent to a book distributor a notice which ordered that the distributor cease disseminating certain publications to minors and which reminded the distributor of the commission's duty to recommend prosecutions to the Attorney General. The notice thanked the distributor for his anticipated cooperation. The Supreme Court found that the commission's practice of informal censorship violated the First Amendment, as incorporated against the states by the Fourteenth Amendment.[148]

Important for purposes of this case, the Supreme Court in *Bantam Books* deemed it irrelevant that the commission did not have any actual authority to prosecute anyone.[149] The Court recognized that the distributor "was `free' to ignore the Commission's notices, in the sense that his refusal to `cooperate' would have violated no law,"[150] but the Court did not countenance that technical point in light of the realities of the situation:

504*504 People do not lightly disregard public officers' thinly veiled threats to institute criminal proceedings against them if they do not come around.... The Commission's notices, phrased virtually as orders, reasonably understood to be such by the distributor, invariably followed up by police visitations, in fact stopped the circulation of the listed publications *ex proprio vigore.* It would be naive to credit the State's assertion that these blacklists are in the nature of mere legal advice, when they plainly serve as instruments of regulation independent of the laws against obscenity.[151]

Here, the Court concludes it would be similarly naive to conclude that § 2709 NSLs, given their commandeering warrant, do anything short of coercing all but the most fearless NSL recipient into immediate compliance and secrecy.[152]

In another case along these general lines,[153] the First Circuit considered whether it was proper for the United States Attorney's Office in Puerto Rico to issue to grand jury subpoena recipients letters which stated:

You are not to disclose the existence of this subpoena or the fact of your compliance for a period of 90 days from the date of the subpoena. Any such disclosure could seriously impede the investigation being conducted and, thereby, interfere with the enforcement of the federal criminal law.[154]

The Court held that the letter violated Federal Rule of Criminal Procedure 6, which bars secrecy obligations upon subpoena recipients.[155] The First Circuit explicitly rejected the contention "that the letter did not impose any `obligation' but simply stated the United States Attorney's belief that disclosure would be harmful to the investigation":

The document at issue, after all, is from the United States Attorney's office informing its recipient that a particular course of action could "impede" a criminal investigation "and, thereby, interfere with the enforcement of the federal criminal law." Absent a clear showing to the contrary, we fail to see how a reasonable, law-abiding person who received such a letter would think anything other than that he was being told 505*505 that he was legally obligated not to engage in that course of action.[156]

The First Circuit thus invalidated what was, in practice, an obligation of secrecy, even though the letters at issue did not have the force of law.

Similarly, the Court here concludes that what is, in practice, an implicit obligation of automatic compliance with NSLs violates the Fourth Amendment right to judicial access, even if hypothetically the law were construed to imply such access. In this regard, the Court notes that even stronger grounds exist in the record before this Court to support a finding of coercive effect of the NSLs than was the case of the government agency's letters involved in both *Bantam Books* and *Grand Jury Proceedings.* In *Bantam Books,* the Rhode Island statute at issue made clear that the commission it created had no power to prosecute those who violated the "recommendations" in its letters, and in *Grand Jury Proceedings,* the Government's ability to require the secrecy sought by the letter at issue was specifically foreclosed by a Federal Rule of Criminal Procedure. By contrast, in issuing the NSL in the form employed here, the FBI's order carried out the express terms of § 2709 and, as the reference to the law reminded the recipient, directed precisely the conduct the statute mandated. An NSL recipient would be unable to learn from the text of § 2709 that the letter was not *actually* coercive.

That the form NSL and the FBI's actions were based on a plausible reading of § 2709 does not save these practices from invalidation. In *Bantam Books,* the Supreme Court nullified the commission's practices without reaching the question of whether the vague and open-ended statute creating the commission was itself constitutional,[157] and in *Grand Jury Proceedings,* the First Circuit had no occasion to reach constitutional questions because it found that the United States Attorney's Office had violated a Federal Rule of Criminal Procedure.

Recognizing from the preceding discussion the reality that § 2709 effectively keeps § 2709 NSLs out of litigation altogether, the Court concludes that supplying a judicial gloss to § 2709 but failing to address the practical effects of the unparalleled level of secrecy and coercion fostered by the FBI's implementation of the statute would be completely academic. That is the Court is reluctant to fashion a "remedy" which has no effect beyond being printed in the Federal Supplement.

The Court notes that, conceivably, the Government could endeavor to remedy the defects in § 2709 by alerting all NSL recipients as to what the Government now claims is implicit in § 2709 — that they are entitled to consult an attorney and other persons necessary to facilitate compliance, and to move to quash the NSL. However, accepting as implicit in the statute the protections the Government contends may be inferred does not remedy another deficiency that serves as independent grounds for the statute's facial invalidation: the categorical, indefinite non-disclosure provision § 2709(c), which is not amenable to a 506*506 "fairly possible"[158] construction that would save it from invalidation.

The Court explains below why categorical, indefinite, and unreviewable non-disclosure was intended by Congress and why any judicial interpretation intended to save this provision of § 2709, *e.g.,* by requiring judicial determination of the need for secrecy in each case, or by making judicial review available to challenge the categorical ban or speech at particular times, would be entirely unmoored from anything in the text, structure or legislative history of the statute, and would grossly exceed the judicial function. Such a ruling would essentially amount to judicial arrogation of legislative power, an outright statutory re-write, rather than a "fairly possible" statutory construction.[159] On this point, however, the Government's argument defends the statute as drafted, and presumably would oppose a construction that would recognize the availability of judicial review to mitigate the consequences of the permanent non-disclosure mandate. Here, then, is the nub of this case. The Government does not accept that § 2709's non-disclosure provision may be modified by judicial review — nor could it, given the plain text of the statute — and the Court, which deems such an omission from the law fatal, would be unable, for the same reason, to cure it by interpretation.

Accordingly, the Court concludes that § 2709, as applied here, must be invalidated because in all but the exceptional case it has the effect of authorizing coercive searches effectively immune from any judicial process, in violation of the Fourth Amendment. The Court next turns to other reasons that compel the more drastic conclusion that § 2709 must be invalidated on its face. First, however, the Court examines Plaintiffs' arguments that § 2709 violates communications service *subscribers'* First Amendment rights. It concludes that the absence of meaningful judicial review created by § 2709's coercive implementation may also lead to violations of subscribers' own constitutional rights.

2. *NSLs May Violate ISP Subscribers' Rights.*

Plaintiffs have focused on the possibility that § 2709 could be used to infringe subscribers' First Amendment rights of anonymous speech and association. Though it is not necessary to precisely define the scope of ISP subscribers' First Amendment rights, the Court concludes that § 2709 may, in a given case, violate a subscriber's First Amendment privacy rights, as well as other legal rights, if judicial review is not readily available to an ISP that receives an NSL. This conclusion buttresses the

Court's holding that, at least as applied, § 2709 does not permit sufficient judicial review to preserve individual subscribers' rights, where impairment of such rights may be implicated by a given NSL.[160]

The Supreme Court has recognized the First Amendment right to anonymous speech at least since *Talley v. California,*[161] which invalidated a California law 507*507 requiring that handbills distributed to the public contain certain identifying information about the source of the handbills. The Court stated that the "identification requirement would tend to restrict freedom to distribute information and thereby freedom of expression."[162] The Supreme Court has also invalidated identification requirements pertaining to persons distributing campaign literature,[163] persons circulating petitions for state ballot initiatives,[164] and persons engaging in door-to-door religious advocacy.[165]

In a related doctrine, the Supreme Court has held that "compelled disclosure of affiliation with groups engaged in advocacy" amounts to a "restraint on freedom of association" where disclosure could expose the members to "public hostility."[166] Laws mandating such disclosures will be upheld only where the Government interest is compelling.[167]

The Court concludes that such First Amendment rights may be infringed by application of § 2709 in a given case. For example, the FBI theoretically could issue to a political campaign's computer systems operator a § 2709 NSL compelling production of the names of all persons who have email addresses through the campaign's computer systems. The FBI theoretically could also issue an NSL under § 2709 to discern the identity of someone whose anonymous online web log, or "blog," is critical of the Government. Such inquiries might be beyond the permissible scope of the FBI's power under § 2709 because the targeted information might not be relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, or because the inquiry might be conducted solely on the basis of activities protected by the First Amendment. These prospects only highlight the potential danger of the FBI's self-certification process and the absence of judicial oversight.

Other rights may also be violated by the disclosure contemplated by the statute; the statute's reference to "transactional records" creates ambiguity regarding the scope of the information required to be produced by the NSL recipient. If the recipient — who in the NSL is called upon to exercise judgment in determining the extent to which complying materials constitute transactional records rather than content[168] — interprets the NSL broadly as 508*508 requiring production of all e-mail header information, including subject lines, for example, some disclosures conceivably may reveal information protected by the subscriber's attorney-client privilege, *e.g.,* a communication with an attorney where the subject line conveys privileged or possibly incriminating information. Indeed, the practical absence of judicial review may lead ISPs to disclose information that is protected from disclosure by the NSL statute itself, such as in a case where the NSL was initiated solely in retaliation for the subscriber's exercise of his First Amendment rights, as prohibited by § 2709(b)(1)-(b)(2). Only a court would be able to definitively construe the statutory and First Amendment rights at issue in the "First Amendment retaliation" provision of the statute, and to strike a proper balance among those interests.

The Government asserts that disclosure of the information sought under § 2709 could not violate a subscriber's rights (and thus demands no judicial process) because the information which a § 2709 NSL seeks has been voluntarily conveyed to the ISP who receives the NSL. According to the Government, an internet speaker relinquishes any interest in any anonymity, and any protected claim to that information, as soon as he releases his identity and other information to his ISP. In support of its position, the Government cites the Supreme Court's holding that, at least in the Fourth Amendment context involving the Government installing a pen register or obtaining bank records,

when a person voluntarily conveys information to third parties, he assumes the risk that the information will be turned over to the Government.[169]

The Court rejects the Government's reasoning. Every court that has addressed the issue has held that individual internet subscribers have a right to engage in anonymous internet speech, though anonymity may be trumped in a given case by other concerns.[170] No court has adopted the Government's argument here that anonymous internet speech or associational activity ceases to be protected because a third-party ISP is in possession of the identifying information.[171]

509*509 Moreover, the Court notes that the implications of the Government's position are profound. Anonymous internet speakers could be unmasked merely by an administrative, civil, or trial subpoena, or by any state or local disclosure regulation directed at their ISP, and the Government would not have to provide any heightened justification for revealing the speaker. The same would be true for attempts to compile membership lists by seeking the computerized records of an organization which uses a third-party electronic communications provider. Considering, as is undisputed here, the importance of the internet as a forum for speech and association, the Court rejects the invitation to permit the rights of internet anonymity and association to be placed at such grave risk.

The Court reaches this conclusion by determining that NSLs issued pursuant to § 2709 may seek information about or indirectly obtained from subscribers that may be protected from disclosure by the First Amendment or other rights-protecting constitutional provisions or statutes. Echoing the Supreme Court's observation that "differences in the characteristics of new media justify differences in the First Amendment standards applied to them,"[172] the Court concludes that even though *Smith* and *Miller* might suggest that there is no First Amendment interest at stake in compelling the disclosure by telephone companies and banks of certain transactional information derived from customer records, in deciding this case the Court must take account of the unique features of internet communications that may warrant application of different rules. The Court is persuaded that, for First Amendment purposes, internet records of the type obtained via a § 2709 NSL could differ substantially from transactional bank or phone records.

The evidence on the record now before this Court demonstrates that the information available through a § 2709 NSL served upon an ISP could easily be used to disclose vast amounts of anonymous speech and associational activity. For instance, § 2709 imposes a duty to provide "electronic communication transactional records,"[173] a phrase which, though undefined in the statute, certainly encompasses a log of email addresses with whom a subscriber has corresponded and the web pages that a subscriber visits. Those transactional records can reveal, among other things, the anonymous message boards to which a person logs on or posts, the electronic newsletters to which he subscribes, and the advocacy websites he visits. Moreover, § 2709 imposes a duty on ISPs to provide the names and addresses of subscribers,[174] thus enabling the Government to specifically identify someone who has written anonymously on the internet.[175] As discussed above, given that an 510*510 NSL recipient is directed by the FBI to turn over all information *"which you consider to be* an electronic communication transactional record,"[176] the § 2709 NSL could also reasonably be interpreted by an ISP to require, at minimum, disclosure of all e-mail header information, including subject lines.

In stark contrast to this potential to compile elaborate dossiers on internet users, the information obtainable by a pen register is far more limited. As the Supreme Court in*Smith* was careful to note:

[Pen registers] disclose only the telephone numbers that have been dialed — a means of establishing communication. Neither the purport of any communication between the caller and the

recipient of the call, their identities, nor whether the call was even completed is disclosed by pen registers.[177]

The Court doubts that the result in *Smith* would have been the same if a pen register operated as a key to the most intimate details and passions of a person's private life.

The more apt Supreme Court case for evaluating the assumption of risk argument at issue here is *Katz v. United States,*[178] the seminal decision underlying both *Smith* and*Miller. Katz* held that the Fourth Amendment's privacy protections applied where the Government wiretapped a telephone call placed from a public phone booth.[179]Especially noteworthy and pertinent to this case is the Supreme Court's remark that: "The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a `search and seizure' within the meaning of the Fourth Amendment."[180] The Supreme Court also stated that a person entering a phone booth who "shuts the door behind him" is "surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world," and held that, "[t]o read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[181]

Applying that reasoning to anonymous internet speech and associational activity is relatively straightforward. A person who signs onto an anonymous forum under a pseudonym, for example, is essentially "shut[ting] the door behind him,"[182] and is surely entitled to a reasonable expectation that his speech, whatever form the expression assumes, will not be accessible to the Government to be broadcast to the world absent appropriate legal process. To hold otherwise would ignore the role of the internet as a remarkably powerful forum for private communication and association. Even the Government concedes here that the internet is an "important vehicle for the free exchange of ideas and facilitates associations."[183]

To be sure, the Court is keenly mindful of the Government's reminder that the internet may also serve as a vehicle for crime. The Court equally recognizes that 511*511circumstances exist in which the First Amendment rights of association and anonymity must yield to a more compelling Government interest in obtaining records from internet firms. To this end, the Court re-emphasizes that it does not here purport to set forth the scope of these First Amendment rights in general, or define them in this or any other case. The Court holds only that such fundamental rights are certainly implicated in some cases in which the Government may employ § 2709 broadly to gather information, thus requiring that the process incorporate the safeguards of some judicial review to ensure that if an infringement of those rights is asserted, they are adequately protected through fair process in an independent neutral tribunal. Because the necessary procedural protections are wholly absent here, the Court finds on this ground additional cause for invalidating § 2709 as applied.

C. *CONSTITUTIONALITY OF THE NON-DISCLOSURE PROVISION*

Finally, the Court turns to the issue of whether the Government may properly enforce § 2709(c), the non-disclosure provision, against Doe or any other person who has previously received an NSL. Section 2709(c) states: "No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section."[184]

A threshold question concerning this issue is whether, as Plaintiffs contend, § 2709(c) is subject to strict scrutiny as either a prior restraint on speech or a content-based speech restriction, or whether, as the Government responds, § 2709(c) is subject to the more relaxed judicial review of intermediate scrutiny. The difference is crucial. A speech restriction which is either content-based or which imposes a prior restraint on speech is presumed invalid and may be upheld only if it is "narrowly

tailored to promote a compelling Government interest."[185] If "less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve," then the speech restriction is not narrowly tailored and may be invalidated.[186] Under intermediate scrutiny, a speech restriction may be upheld as long as "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."[187]

The Court agrees with Plaintiffs that § 2709(c) works as both a prior restraint on speech and as a content-based restriction, and hence, is subject to strict scrutiny.[188] First, axiomatically the categorical non-disclosure mandate embodied 512*512 in § 2709(c) functions as prior restraint because of the straightforward observation that it prohibits speech before the speech occurs. As the Supreme Court articulated the threshold inquiry: "The relevant question is whether the challenged regulation authorizes suppression of speech in advance of its expression...."[189] The Government nevertheless maintains that § 2709(c) does not operate as a prior restraint because it does not create a licensing system by which the Government can pick and choose among speakers to restrain. As the Government explains, somewhat cryptically, § 2709(c) "does not authorize any government official to grant a speaker permission to make any particular disclosure. Rather, the statute simply prohibits certain disclosures."[190]

In the Court's judgment, a blanket permanent prohibition on future disclosures is an even purer form of prior restraint than a licensing system in which the speaker may at least potentially obtain government approval and remain free to speak. In fact, a blanket proscription on future speech works identically to the most severe form of a licensing system — one in which *no* licenses are granted, and the speech at issue is maximally suppressed.

Second, the Court considers § 2709(c) to be a content-based speech restriction. The Court finds particular guidance on this point from *Kamasinski v. Judicial Review Council,*[191] a case which also figures prominently in addressing the question of whether § 2709(c) survives strict scrutiny. In *Kamasinski,* the plaintiff challenged certain Connecticut laws mandating that judicial ethics proceedings be kept confidential unless and until the relevant administrative authorities determined that there was probable cause to believe that judicial misconduct had occurred, after which a public hearing would be held. During the investigatory phase, the Connecticut statutes, much like § 2709(c), categorically prohibited witnesses and complainants from even disclosing that an investigation was underway. One purpose of Connecticut's non-disclosure rule (again, much like § 2709(c)) was to protect the integrity of the investigation. The Second Circuit held that the restrictions at issue were "content-based, and that strict scrutiny [was] the correct standard."[192] The Court finds *Kamasinski* controlling and thus concludes that § 2709(c) functions as a content-based restriction.

The Government nevertheless argues that § 2709(c) is content-neutral because it prohibits certain disclosures irrespective of any particular speaker's views on NSLs, terrorism, or anything else. The Government emphasizes that a "fundamental principle" underlying judicial skepticism of content-based restrictions is that the Government should not silence "less favored" or "controversial views" while permitting the "views it finds acceptable."[193] Section 2709 does not trigger that concern, the argument goes, because the Government's aim in enforcing § 2709(c) is not to "disagree[ ] with the message,"[194] or to "select which issues are worth discussing or debating 513*513 in public,"[195] but instead to apply a neutral ban on disclosures that are potentially harmful to Government investigations.

The Government's argument is unpersuasive. It fails to recognize that even a *viewpoint*-neutral restriction can be *content*-based, if the restriction pertains to an entire category of speech.[196] The Supreme Court has clearly expressed this principle: "The 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."[197] Section 2709(c) prohibits any discussion of the first-hand experiences of NSL recipients, and of their officers, employees, and agents, and thus closes off that "entire topic" from public discourse.[198] Those persons are forever barred from speaking to anyone about their knowledge and role in the underlying events pertaining to the issuance of an NSL, however substantively limited or temporally remote that role may be, even at a time when disclosure of the occurrence of the investigation may have ceased to generate legitimate national security concerns and instead may hold historical or scholarly value then bearing relatively greater interest to the general public. The restriction would also categorically bar the recipient and its agents from ever discussing their roles even if other persons may be free to do so — because, for example, the matter may have become public or the FBI itself may have revealed the information or publicly brought the investigation to closure. The absolute and permanent ban on disclosure § 2709(c) commands forecloses an objective weighing of these competing public policy interests by a neutral arbiter even as the relative merits of the respective claims may alter over time.

Moreover, the Government's argument is foreclosed by *Kamasinski*. In that case, the Connecticut non-disclosure laws were likewise neutral as to the message conveyed by the disclosure and likewise broadly prohibited the mere fact of disclosure. The Second Circuit applied strict scrutiny, as the Court will do here. As stated, § 2709(c) may survive strict scrutiny if it is "narrowly tailored to promote a compelling Government interest,"[199] and there are no "less restrictive alternatives [which] would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve."[200] The Supreme Court has instructed that, in the courts' assessment of these considerations, "[p]recision of regulation must be the touchstone" of the inquiry.[201]

In applying that test, the Court first acknowledges that the Government's interest in protecting the integrity and efficacy of international terrorism and counterintelligence investigations is a compelling one. The Supreme Court has so acknowledged: "This Court has recognized the Government's `compelling interest' in withholding national security information from unauthorized persons in the course of 514*514 executive business."[202] A suspected terrorist or foreign intelligence operative who is alerted that the Government is conducting an investigation may destroy evidence, create false leads, alert others, or otherwise take steps to avoid detection. More generally, such disclosures can reveal the Government's intelligence-gathering methods, from which foreign intelligence operatives or terrorists could learn better how to avoid detection.

Nonetheless, Plaintiffs contend that § 2709(c)'s categorical, perpetual, and automatic ban on disclosure is not a narrowly-tailored means to advance those legitimate public interests. Plaintiffs suggest that a more precisely-calibrated statute, which would equally advance the Government's compelling interests, would prohibit disclosure only on a case-by-case basis, for a limited time, and with prior judicial approval. Without detailing the degree of narrow tailoring which the First Amendment demands with respect to § 2709, the Court concludes that § 2709 is not sufficiently narrow.

The question of how narrow is narrow enough is not amenable to scientific measurement, nor can it be reduced to articulable facile tests. Rather, it depends largely on context and perspective. When focusing only upon the universe of speech to which § 2709(c) pertains, the restriction appears very narrow. A communications provider is prohibited only from disclosing "that the Federal Bureau of Investigation has sought or obtained access to information or records under [§ 2709]."[203] Anything outside this bare fact may be fair game. For example, the NSL recipient may speak freely about his objection to (or support of) the FBI and its NSL power; he may alert his subscribers to the fact that the FBI has NSL authority under § 2709; he may petition Congress to repeal § 2709 altogether; and, other privacy laws aside, he would not be barred by § 2709(c) from disclosing the substance of the information disclosed to the FBI. Furthermore, a third party unaffiliated with the provider who somehow learned from other sources about the issuance of an NSL would not be precluded from

disclosing its existence. Speech restrictions of this general nature — prohibiting the holder of information from a disclosure which could jeopardize a Government investigation — are commonplace in federal law, as discussed above in Section I.D.

Viewed from another perspective, however, the restraint imposed under § 2709(c) is as thorough as is conceivable. The statute *permanently* prohibits not only the recipient but its officers, employees or agents, from disclosing the NSL's existence to *"any* person," in*every* instance in which an NSL is issued and irrespective of the circumstances prevailing at any given point in time.[204] In this respect, § 2709(c) as well as the other NSL statutes, are uniquely extraordinary. As explained more fully earlier in Section II.D., when the Government conducts a secret investigation, it ordinarily must apply for a court order before restricting third-party participants from revealing the inquiry, and those restrictions are generally temporary.

The Court has been able to locate only three statutory provisions even arguably analogous to the automatic, categorical and permanent scope of the NSL statutes' non-disclosure rules. First, communications firms are categorically barred, *unless otherwise ordered by a court,* from ever disclosing 515*515 that a pen register or trap and trace device is in effect.[205] Second, communications firms are categorically barred, subject to a similar exception "as may otherwise be required by legal process," from ever disclosing that a wiretap or electronic surveillance is in place.[206] Third, recipients of a subpoena under FISA are categorically prohibited from ever disclosing to any person, "other than those persons necessary to produce" the records sought, that the subpoena was issued.[207]

Furthermore, these provisions are not quite as severe as those contained in the NSL statutes because, with one narrow exception for certain FISA surveillance orders,[208]they apply in contexts in which a court authorizes the investigative method in the first place.[209] Thus, even in these statutes, the silenced party, at least theoretically, would almost always have a forum in which to contest the continuing validity of the non-disclosure obligation or to seek a modified secrecy order.[210] The FISA limits the potential for abuse in yet another way 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; such protections are not present in § 2709,[211]particularly after the significant broadening of the statute's scope effectuated by the Patriot Act.[212] The NSL statutes, including § 2709(c), thus stand virtually alone in providing for blanket secrecy entirely outside the context of judicial process.

In synthesizing the broad and narrow features of § 2709(c) explained above, and 516*516 in considering how closely those features are tailored to the Government's compelling interests, the Government makes convincing points in showing that it would be consistent with the First Amendment to impose a certain amount of limited secrecy in many cases involving a § 2709 NSL. The Government also persuasively demonstrates how that secrecy, under certain circumstances, might continue for longer periods of time, consistent with the First Amendment. The Court acknowledges those arguments so far as they go, but concludes in the end that the Government cannot cast § 2709 — a blunt agent of secrecy applying in perpetuity to all persons affected in every case — as narrowly-tailored.

The Government first argues, correctly, that courts generally uphold secrecy statutes in connection with official investigations in recognition of two vital considerations: the importance of secrecy and that the secrecy is limited (as here) to facts learned only by virtue of a given person's participation in the proceedings. The Court examines this doctrine in detail to underscore both its relevance and its limits.

The evolution of this doctrine begins with *Seattle Times Co. v. Rhinehart.*[213] There, the spiritual leader of a religious group sued a newspaper which had run negative stories about him and his members. The trial court issued a protective order to prevent the newspaper from publishing articles about or otherwise disseminating private information it gained only through discovery, and the Supreme Court held that such a discovery restriction was consistent with the First Amendment. The Court reasoned that, because a litigant generally has no First Amendment right to obtain access to such discovery information in the first place, "court control over the discovered information does not raise the same specter of government censorship that such control might suggest in other situations."[214] It was also crucial to the Court's reasoning that the protective order pertained to "only that information obtained through the use of the discovery process," and thus permitted the newspaper to "disseminate the identical information covered by the protective order as long as the information [was] gained through means independent of the court's processes."[215]

The next relevant case, *Butterworth v. Smith,*[216] distinguished *Rhinehart,* but, by negative implication, sharpened the theory underlying the doctrine upon which the Government relies here. In that case, a Florida newspaper reporter, who had testified before a grand jury about alleged state corruption, sought a declaratory judgment that he could lawfully publish, after the grand jury term ended, an account of his grand jury testimony. The Supreme Court invalidated Florida's grand jury secrecy law "insofar as the Florida law prohibit[ed] a grand jury witness from disclosing his own testimony after the term of the grand jury has ended."[217] The Court explained that the reasons for grand jury secrecy (*e.g.,* keeping information from the target, preventing witness tampering, protecting an exonerated target from ridicule) were severely diminished by the end of a grand jury term.[218] 517*517 Against that weak interest, the Court explained that the impact on the reporter's free speech rights was "dramatic."[219] Whereas the reporter was previously "free to speak at will" about the topics at issue, his participation in the grand jury proceeding rendered it unlawful under Florida law for him to communicate even the "content, gist, or import" of his testimony.[220] The Court concluded that "the interests advanced by the [relevant] portion of the Florida statute ... are not sufficient to overcome [the reporter's] First Amendment right to make a truthful statement of information he acquired on his own."[221]

The Court distinguished *Rhinehart* on the ground that the issue in *Butterworth* involved "respondent's right to divulge information of which he was in possession before he testified before the grand jury, and not information which he may have obtained as a result of his participation in the proceedings of the grand jury."[222] To further mark the bounds of its holding, the Court noted that the "part of the Florida statute which prohibits the witness from disclosing the testimony of *another* witness remains enforceable under the ruling the Court of Appeals."[223]

In a lone concurrence, Justice Scalia underscored the important distinction between prohibiting the disclosure of information which a witness "kn[ows] before he enter[s] the grand jury room" (the issue then before the Court) and prohibiting "a witness' disclosure of the grand jury proceedings" (an issue not then before the Court).[224] The latter form of prohibition involves "knowledge [the witness] acquires not `on his own' but only by virtue of being made a witness," and "is in a way information of the State's own creation."[225]Justice Scalia suggested that there might be separate and compelling reasons to prohibit disclosing state-created information, but he noted that the issue was "not presented by the narrow question" of the case.[226]

The Second Circuit embraced Justice Scalia's distinction in *Kamasinski*, cited above.[227]As already stated, *Kamasinski* rejected a First Amendment challenge to Connecticut's secrecy laws surrounding judicial misconduct inquiries. The Circuit Court explained that the disclosures of a participant in such proceedings fall into three categories: (1) "the substance of an individual's complaint or testimony;" (2) "the complainant's disclosure of the *fact* that a complaint was filed or the witness' disclosure of the *fact* that testimony was given;" and (3) "information that the individual learns by interacting with" the other participants.[228] The Second Circuit, citing Justice Scalia's concurrence, held

that*Butterworth* addressed only the first category of information.[229] As for the latter two categories, the Court held that the "limited ban on disclosure" was justified in light of Connecticut's substantial interests 518*518 in the secrecy of those proceedings.[230]

In an analogous case, the Third Circuit drew the same distinction in determining the extent to which Pennsylvania's confidentiality laws for judicial ethics proceedings were constitutional.[231] The Third Circuit held that, although the First Amendment required that a witness be permitted to reveal his own testimony, Pennsylvania's secrecy requirement was constitutional "insofar as it would prevent a person," including a witness, "from disclosing proceedings taking place before" the reviewing body.[232]

Finally, in *Hoffmann Pugh v. Keenan,* the housekeeper of John and Patsy Ramsey, whose daughter JonBenet was the victim of a high-profile, unsolved murder, sought a declaration that she could publish an account of her experiences before the grand jury investigating JonBenet's murder, in spite of a Colorado law prohibiting grand jury witnesses from disclosing their testimony.[233] The Tenth Circuit upheld the secrecy requirement, noting that the Colorado statute was careful to "not prohibit disclosure of information the witness already had independently of the grand jury process."[234] The Court stated: "Reading *Butterworth* in light of *Rhinehart,* we are convinced a line should be drawn between information the witness possessed prior to becoming a witness and information the witness gained through her actual participation in the grand jury process."[235]

A basic principle emerging from these cases is that laws which prohibit persons from disclosing information they learn solely by means of participating in confidential government proceedings trigger less First Amendment concerns that laws which prohibit disclosing information a person obtains independently. Stated another way, the Government has at least some power to control information which is its "own creation,"[236] and to which there is otherwise "no First Amendment right of access."[237] The theory behind this principle is that, where an individual learns information to which he ordinarily would have no right of access, the individual takes that information subject to the statutory scheme (confidentiality rules included) which made the information available in the first place. As Judge Wilkey of the 519*519 District of Columbia Circuit expressed this concept: "The First Amendment interest of litigants in the dissemination of [materials obtained through discovery] is necessarily qualified or conditioned by the potential restrictions that are part of the system through which the materials have been obtained."[238]

The principle *Rhinehart* and its progeny represent is directly applicable to the present case in the following way. An NSL recipient or other person covered by the statute learns that an NSL has been issued only by virtue of his particular role in the underlying investigation, and, as the case law demonstrates, 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.

The relevance of this doctrine reaches its limit, however, when the Court considers that the NSL statutes, unlike other legislation cited above, 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 may no longer warrant categorical secrecy. Courts have recognized the significance of these considerations in First Amendment inquiries. In *Hoffmann Pugh,* for example, the Eighth Circuit explained that Colorado law "provides a mechanism for [the plaintiff] to free herself of the restriction on her disclosure of her grand jury testimony at such time as the investigation is truly closed and the state no longer has a legitimate interest in preserving the secrecy of that testimony."[239] Similarly, the Second Circuit noted in *Kamasinski* that secrecy rules are only consistent with the First Amendment during the investigatory phase of a judicial ethics proceeding.[240] This feature of § 2709(c) is extraordinary in that the breadth and lasting effects of its reach are uniquely exceptional, potentially compelling

secrecy even under some decidedly non-sensitive conditions or where secrecy may no longer be justifiable under articulable national security needs.

The Government's claim to perpetual secrecy surrounding the FBI's issuance of NSLs, by its theory as advanced here an authority neither restrained by the FBI's own internal discretion nor reviewable by any form of judicial process, presupposes a category of information, and thus a class of speech, that, for reasons not satisfactorily explained, must forever be kept from public view, cloaked by an official seal that will always overshadow the public's right to know. In general, as our sunshine laws and judicial doctrine attest, democracy abhors undue secrecy, in recognition that public knowledge secures freedom.[241] 520*520 Hence, an unlimited government warrant to conceal, effectively a form of secrecy *per se,* has no place in our open society. Such a claim is especially inimical to democratic values for reasons borne out by painful experience.[242]Under the mantle of secrecy, the self-preservation that ordinarily impels our government to censorship and secrecy may potentially be turned on ourselves as a weapon of self-destruction. When withholding information from disclosure is no longer justified, when it ceases to foster the proper aims that initially may have supported confidentiality, a categorical and uncritical extension of non-disclosure may 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. At that point, secrecy's protective shield may serve not as much to secure a safe country as simply to save face.

The Government does not deny that there are plausible situations in which little or no reason may remain for continuing the secrecy of the fact that an NSL was issued. To cite an example, a case may arise in which the Government's investigation has long since been completed and information about it has become public through Government sources or otherwise, in which the material obtained through an NSL revealed that there was no basis whatsoever to pursue the subject or target of the Government's investigation, or in which the disclosure may have been made by a person in the chain of information, such as an employee or agent of the NSL recipient, who was not informed in any way of the secrecy requirement. Section 2709(c) does not countenance the possibility that the FBI could permit modification of the NSL's no-disclosure order even in those or any other similar situations no longer implicating legitimate national security interests and presenting factual or legal issues that any court could reasonably adjudicate. Bluntly stated, the statute simply does not allow for that balancing of competing public interests to be made by an independent tribunal at any point. In this regard, it is conceivable that "less restrictive alternatives would be at 521*521 least as effective in achieving the legitimate purpose that the statute was enacted to serve."[243]For instance, Congress could require the FBI to make at least *some* determination concerning need before requiring secrecy, and ultimately it could provide a forum and define at least *some* circumstances in which an NSL recipient could ask the FBI or a court for a subsequent determination whether continuing secrecy was still warranted.

As mentioned above, pending legislation authorizing broad NSL powers in terrorism cases fully outlines some less restrictive alternatives along these lines.[244] Bills pending in the House and Senate would require the Attorney General to certify, before ordering secrecy, that disclosure would present a "danger to the national security," and the non-disclosure order could later be terminated by the Attorney General or a court, if the danger expires.[245] That such protective procedures were indeed incorporated in somewhat analogous statutes, and are the subject of corrective bills now pending in Congress, confirms some level of congressional recognition that § 2709(c) as now written is severely flawed, and that other means may be available to protect secrecy while still preserving First Amendment rights.[246]

The Government acknowledges that § 2709(c) was intended by Congress to impose a permanent ban on disclosure, but maintains that any less restrictive alternative, such as H.R. 3037, would not be as effective because it would put the Government to an unwelcome choice each time it considered issuing an NSL. That is, the Government would have to weigh the risk of court-ordered

disclosure against the need for the information sought. The Government argues that it should not be discouraged from seeking *all* relevant information in these highly important and sensitive investigations. This argument, as if using the edge of the hammer to hit the nail, strikes the central point only tangentially. The issue raised by the indefinite secrecy which the § 2709(c) non-disclosure provision countenances has little or nothing to do either with the Government's ability or its reach to freely gather as much information as it deems necessary, assuming the means and safeguards it employs are otherwise proper. The Court discerns no quarrel here on that score. Rather, the question is the Government's need to maintain the secrecy of discrete information, and thus a restriction on freedom of speech, long after the investigation has gathered whatever it needs and the material presumably has been put to its intended purposes. At that point, instances may arise in which the justification for concealment may have attenuated and the rights of both the NSL recipient and the public to disclosure may have correspondingly acquired greater weight and deserve heightened consideration in the balancing of pertinent public values by a neutral arbiter.

Though mindful of the Government's concerns, the Court remains skeptical of 522*522 the contention that a narrower statute could not meet the Government's needs just as effectively. As an initial matter, the Court makes clear that, where a blanket rule swearing everyone concerned to secrecy forever certainly would be the *easier* and most efficient course for the Government, that is of no moment here. Striking at speech with an all-encompassing prophylactic rule will always demand less Government effort than a more considered, case-by-case approach. Recognizing, as suggested earlier, that the most efficient course does not necessarily equate to the one which is most equitable and protective of fundamental rights, the issue here, therefore, is whether some uniquely exceptional reason in this case compels the categorical preclusive rule of § 2709 to be absolutely essential to effectuating the Government's legitimate interests in some measure of secrecy. Importantly, it is the Government's burden to make that showing.[247] As the Supreme Court has instructed: "When a plausible, less restrictive alternative is offered to a content-based speech restriction, it is the Government's obligation to prove that the alternative will be ineffective to achieve its goals."[248] The Court concludes that the Government has failed to carry its burden to show that the extraordinary scope of § 2709(c) is always necessary.[249]

In response to this standard, the Government's main contention, quite understandably, is that international terrorism and counterintelligence investigations justify more secrecy than other types of investigations. The Court agrees with that basic point so far as it goes. However, under the exacting demands of the First Amendment, the argument does not carry far enough.

The Government correctly states that international terrorism and counterintelligence investigations are generally different from investigations of past crimes in that the latter proceedings usually contemplate a logical endpoint (*i.e.,* trial or hearing) where the Government publicly presents the evidence it has gathered related to allegations of a discrete, past wrongdoing. By contrast, international terrorism and counterintelligence investigations seek to uncover and disrupt *future* activities of typically large, long-term and expansive conspiracies. So much has been acknowledged by the Supreme Court, which has aptly observed that, in contrast to investigations of" `ordinary crime,'" intelligence surveillance "is often long range and involves the interrelation of various sources and types of information," and that its emphasis "is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency."[250] Also, the Government often decides to pursue the fruits of international terrorism or counterintelligence 523*523 investigation via interdiction or diplomacy, as opposed to through formal and public criminal processes.[251] In such cases, the Government could theoretically have a much greater interest in continuing secrecy because certain elements of the investigation may remain in place for longer periods of time.[252]

The Court also agrees, insofar as relevant, with the Government's contention that it is sometimes very difficult to determine whether an isolated disclosure implicates national security. International

terrorism and counterintelligence investigations may involve continuously expanding or ever-changing players. Hence, determining whether something is sensitive in such a fluid and necessarily broad and indeterminate context may not be simple. As the Supreme Court has observed, "bits and pieces of data may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself," and thus, "what may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context."[253]

Consequently, particular institutional limitations come into play when the judiciary is asked to make such determinations. Ordinarily, judges do not have national security expertise. Nor is the institution of the judiciary well-equipped to understand the sensitivity of an isolated piece of information in the context of the entire intelligence apparatus.[254]As one Circuit Court remarked in addressing this point: "Things that d[o] not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence-gathering capabilities from what these documents revealed about sources and methods."[255] These institutional concerns explain the well-settled doctrine that courts grant substantial deference to the political branches in national security matters. The Supreme Court has recognized that in cases of "terrorism or other special circumstances" courts might afford "heightened deference to the judgments of the political branches with respect 524*524 to matters of national security."[256]

In this Court's judgment, these authorities persuasively confirm that the Government should be accorded a due measure of deference when it asserts that secrecy is necessary for national security purposes in a *particular situation* involving *particular persons* at a *particular time.* Here, however, the Government cites no authority supporting the open-ended proposition that it may universally apply these general principles to impose perpetual secrecy upon an entire category of future cases whose details are unknown and whose particular twists and turns may not justify, for all time and all places, demanding unremitting concealment and imposing a disproportionate burden on free speech.

In fact, all the cases cited above involved some judicial process pertaining to contemporary circumstances, and, for obvious reasons, the general propositions articulated in those opinions cannot always be tailored to every forthcoming or unforeseen set of facts. Thus, the central flaw in the Government's argument is that it invites the Court to "assume that [§ 2709] will *always* advance the asserted [Government] interests sufficiently to justify its abridgment of expressive activity."[257] The Court cannot uncritically embrace that proposition because there are undoubtedly circumstances in which the need for secrecy either has expired or simply no longer exists with the same compelling force that once warranted its imposition. Section 2709(c) provides no mechanism to account for or exclude any unjustifiable denial of speech in these cases. Nor has the Government persuasively shown that it cannot provide such safeguards by less burdensome means. As the Sixth Circuit commented, in rejecting the Government's attempt to impose blanket closure upon a wide class of immigration cases, 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."[258] The Court cannot, consistent with its constitutional powers, fix the shortcomings of this provision of the statute to make it more "targeted and precise."[259] That is a legislative function. Accordingly, § 2709(c) must be invalidated on its face on this ground.

The Government also makes the independent argument that § 2709(c) pertains to only one of the "few limited areas" of proscribable speech, such as obscenity and threats of violence, "which are `of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest 525*525 in order and morality.'"[260] The Government conceives of an entirely proscribable area of speech covering disclosures which would implicate national security concerns. Without deciding whether such a category should be deemed generally proscribable, the Court rejects the Government's argument as question-begging. For that argument to have any force, the Court would have to assume that § 2709(c) pertains only to disclosures which are invariably and

perpetually harmful to national security, a dubious assumption that is a highly disputed issue in this lawsuit.[261]

Because the Court concludes that § 2709(c) is facially unconstitutional, it must also determine whether the remainder of the statute can be severed from it.[262] "The inquiry into whether a statute is severable is essentially an inquiry into legislative intent."[263] Though the Court is mindful of its duty to save as much of a statute as possible when it finds a portion of it unconstitutional,[264] the Court must strike down additional provisions of a statute in the face of the unconstitutionality of particular elements of it when "it is evident that the legislature would not have enacted those provisions which are within its power, independently of that which is not."[265] The Court concludes here that Congress could not have intended §§ 2709(a) and (b), the provisions authorizing the FBI to issue NSLs seeking information from wire and electronic communication service providers, to operate absent the non-disclosure provisions contained in § 2709(c). As the Court has described above, Congress intended the statute to function as a *secret* means of gathering information from communications service providers; other, non-secret means of obtaining information are already available to law enforcement officials for procuring the same material covered by § 2709. In addition, the Court recognizes that the NSL regime cannot function in accordance with Congress's intent if the fact of an NSL's issuance could be immediately disclosed to a communications subscriber who is the target of a § 2709 NSL. Absent the secrecy provisions of the invalidated § 2709(c), however, there is no vehicle in the statute to preserve a more narrowly-tailored degree of secrecy necessary to effectuate the important purposes of the statute consistent with First Amendment values. Because "Congress could not have intended 526*526 [§ 2709(c),] a constitutionally flawed provision[,] to be severed from [§§ 2709(a) and (b)] if [§§ 2709(a) and (b) are] incapable of functioning independently,"[266] the Court concludes that §§ 2709(a) and (b) must be invalidated as non-severable from § 2709(c).

V. *STAY OF JUDGMENT*

Considering the implications of its ruling and the importance of the issues involved, the Court will stay enforcement of its judgment pending appeal, or for the Government otherwise to pursue any alternate course of action, for 90 days. The Court is aware that several material issues in this case involve uncharted legal terrain. The stay will give the Government the opportunity to move this Court, or the Court of Appeals, for whatever appropriate relief it may seek to maintain the confidentiality of any information implicated by the Court's ruling. To this end, the Court is aware that invalidating § 2709(c) on its face may carry the potential to compromise legitimately confidential information. The Court declares unequivocally that it is not its intention to cause any such information to fall into the wrong hands.

The seal governing this case thus remains in effect, with the following exception. Throughout this litigation, the Government has maintained that the Court should conceal the identity of Doe, as well the mere fact that an NSL was issued to Doe (and any other fact which would suggest as much). But, in the course of rendering this decision the Court unavoidably has revealed portions of that information. The Court cannot perceive any compelling basis for continuing to conceal narrow fact of the existence of the NSL. The disclosure amounts to only that, at some unspecified time and place, the Government issued a § 2709 NSL to some unnamed internet firm. Even if not explicitly stated, that much is readily apparent to any interested or discerning observer from the publicly available complaint and other documents on file. The revelation amounts to little more than a statement that the Government has, at some time, made use of a statutory power granted to it — as it manifestly and by its own admission has done on so many other occasions during the life of the statute. Without anything to connect the NSL in this case to the particular NSL recipient involved, and without offering any details about the NSL itself that would help link it to its recipient, the Court concludes that the extent of the additional information disclosed here is negligible, and, in any event, not conceivably harmful to compelling Government interests.[267]

VI. *CONCLUSION*

To summarize, the Court concludes that the compulsory, secret, and unreviewable production of information required by the FBI's application of 18 U.S.C. § 2709 violates the Fourth Amendment, and that the non-disclosure provision of 18 U.S.C. 527*527 § 2709(c) violates the First Amendment.[268] The Government is therefore enjoined from issuing NSLs under § 2709 or from enforcing the non-disclosure provision in this or any other case, but enforcement of the Court's judgment will be stayed pending appeal, or if no appeal is filed, for 90 days.

VII. *ORDER*

For the reasons discussed above, it is hereby:

ORDERED that the motion of John Doe, the American Civil Liberties Union, and the American Civil Liberties Union Foundation (collectively, "Plaintiffs") for summary judgment in this case is granted. Defendants John Ashcroft, in his official capacity as Attorney General of the United States, Robert Mueller, in his official capacity as Director of the Federal Bureau of Investigation, and Marion Bowman, in his official capacity as Senior Counsel to the Federal Bureau of Investigation (collectively "Defendants"), are hereby enjoined from issuing national security letters under 18 U.S.C. § 2709, or from enforcing the provisions of 18 U.S.C. § 2709(c); it is further

ORDERED that Defendants' motion to dismiss, or in the alternative, for summary judgment, is denied; it is further

ORDERED that Plaintiffs' motion to exclude Defendants' *ex parte* affidavit is denied as moot; it is further

ORDERED that the Clerk of Court shall file this Decision and Order on the public docket; and is finally

ORDERED that the Clerk of Court shall enter judgment accordingly but stay enforcement of the judgment pending any appeal, or, if no appeal is filed, for 90 days from the date of this Order.

SO ORDERED.

[1] 18 U.S.C. § 2709.

[2] *Id.* § 2709(c).

[3] By Order dated May 12, 2004, the Court granted the Government's motion to seal the record of this proceeding so as to preclude the disclosure of Doe's identity and other facts relating to Doe's role in this controversy that might identify Doe or otherwise interfere with the underlying FBI activities giving rise to this case.

[4] *See* U.S. Const. amend. IV ("The right of the *people* to be *secure* in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated....") (emphasis added).

[5] *Hamdi v. Rumsfeld,* ___ U.S. ___, ___, 124 S.Ct. 2633, 2650, 159 L.Ed.2d 578 (2004).

[6] *Home Building & Loan Ass'n v. Blaisdell,* 290 U.S. 398, 426, 54 S.Ct. 231, 78 L.Ed. 413 (1934).

[7] *See* *United States v. Harrell,* 207 F.Supp.2d 158, 162 (S.D.N.Y.2002) (Marrero, J.) ("[I]n performing their constitutional mandate, the courts will be called upon to exert particular vigilance to safeguard against excess committed in the name of expediency, to ensure that Americans do not succeed where the terrorists failed, inflicting by their own hand the deeper wrongs to the nation's essence that the September 11 external attacks upon physical structures and innocent people were unable to realize.... In short, the September 11 cases will challenge the judiciary to do September 11 justice, to rise to the moment with wisdom equal to the task, its judgments worthy of the large dimensions that define the best September 11 brought out of the rest of American society.").

[8] *Kennedy v. Mendoza-Martinez,* 372 U.S. 144, 165, 83 S.Ct. 554, 9 L.Ed.2d 644 (1963).

[9] Only a brief recitation of the most basic facts is provided here, but these details are sufficient alone to resolve the present motions.

[10] Compl. Attach. A.

[11] *Id.*

[12] *Id.* (emphasis added).

[13] *Id.* (emphasis in original). As the Court explains below, under the seal order that will remain in place, the details of any further names, times and places identified in the NSL will remain confidential.

[14] *See* 18 U.S.C. § 2709.

[15] *Id.*

[16] *See id.*

[17] *See* 12 U.S.C. § 3414 (financial records); 15 U.S.C. §§ 1681u, 1681v (credit records); 50 U.S.C. § 436 (government employee records).

[18] *See* 12 U.S.C. § 3414(a)(5)(D); 15 U.S.C. §§ 1681u(d), 1681v(c); 50 U.S.C. § 436(b).

[19] *See* Pub.L. No. 99-508, § 201, 100 Stat. 1848, 1867 (1986).

[20] S.Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

[21] Pub.L. No. 95-630, Title XI, 92 Stat. 3641, 3697 (1978).

[22] *See* H.R. Rep. 95-1383, at 28, *reprinted in* 1978 U.S.C.C.A.N. 9273, 9305.

[23] *Id.*

[24] *Id.* at 28, 1978 U.S.C.C.A.N. at 9306 (citing *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976)).

[25] *See* S.Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3558.

[26] *See* 18 U.S.C. § 2703.

[27] *See* 18 U.S.C. § 2709.

[28] 18 U.S.C. § 2709 (1988).

[29] *See* S.Rep. No. 99-307, at 18-19 (1986). This Senate Intelligence Committee report pertains to the Intelligence Authorization Act for Fiscal Year 1987 ("IAA"), not the ECPA, which originated in the Senate Judiciary Committee and which ultimately produced § 2709. However, the legislative history of the IAA is, in most respects, more detailed and instructive

regarding the meaning of the language that would eventually become enacted as § 2709. The Senate report on the ECPA directs the reader to the legislative history of the IAA for background on other aspects of the statute. *See* S.Rep. No. 99-541, at 44 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3598. Section 2709 was not enacted as part of the IAA at least partly because the conference committee recognized that it would be enacted as part of the ECPA. *See* H.R. Conf. Rep. No. 99-952, at 30 (1986), *reprinted in* 1986 U.S.C.C.A.N. 5379, 5390 ("The conferees support such legislation, but decided not to include it in the conference report since it is expected to become law as part of the Electronic Communications Privacy Act.").

[30] *See* S.Rep. No. 99-307, at 19.

[31] *See id.* at 19-20.

[32] *See id.* The version passed under the ECPA deletes the three words "or may be." *See* 18 U.S.C. § 2709 (1988). The ECPA Senate Report notes, but does not explain, the deletion. *See* S.Rep. No. 99-541, at 44 (1986),*reprinted in* 1986 U.S.C.C.A.N. 3555, 3598.

[33] *See* S.Rep. No. 99-307, at 20 (citing *Reporters Comm. for Freedom of the Press v. AT & T,* 593 F.2d 1030 (D.C.Cir.1978)).

[34] The Senate report accompanying the ECPA made particular note of this addition: while the version of § 2709 contained in the IAA merely allowed the FBI to obtain telephone subscriber and toll billing information, the version enacted as part of the ECPA added a provision authorizing use of NSLs to gather "electronic communication transactional records." *See* S.Rep. No. 99-541, at 43-44 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3597-98. The stated purpose of the addition is frankly inscrutable; the report states that the addition "ensures that the FBI has the necessary authority with regard to subscriber information and toll billing information with respect to electronic communication services other than ordinary telephone service." *Id.* at 44, 1986 U.S.C.C.A.N. at 3598.

[35] *See* 18 U.S.C. § 2709 (1994).

[36] H.R.Rep. No. 103-46, at 3 (1993), *reprinted in* 1993 U.S.C.C.A.N. 1913, 1915; *see* 18 U.S.C. § 2709 (1994). The amended statute permitted the FBI to:

(1) request the name, address, length of service, and toll billing records of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that —

(A) the name, address, length of service, and toll billing records sought are relevant to an authorized foreign counterintelligence investigation; and

(B) 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); and

(2) request the name, address, and length of service of a person or entity if the Director (or his designee in a position not lower than Deputy Assistant Director) certifies in writing to the wire or electronic communication service provider to which the request is made that —

(A) the information sought is relevant to an authorized foreign counterintelligence investigation; and

(B) there are specific and articulable facts giving reason to believe that communication facilities registered in the name of the person or entity have been used, through the services of such provider, in communication with —

(i) an individual who is engaging or has engaged in international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States; or

(ii) a foreign power or an agent of a foreign power under circumstances giving reason to believe that the communication concerned international terrorism as defined in section 101(c) of the Foreign Intelligence Surveillance Act or clandestine intelligence activities that involve or may involve a violation of the criminal statutes of the United States.

18 U.S.C. § 2709(b) (1994).

[37] H.R.Rep. No. 103-46, at 2, 1993 U.S.C.C.A.N. at 1914. In support of the change, the FBI cited to the House Judiciary Committee an occasion in which it intercepted a phone call from an unidentified former U.S. Government employee who offered to provide sensitive intelligence to a foreign nation. *See id.* According to the FBI, the original version of § 2709 did not provide it with authority to trace the employee's call (and thereby identify him) because the employee was a possible volunteer as a foreign agent, and not himself a foreign agent. *See id.*

[38] *Id.* at 2-3, 1993 U.S.C.C.A.N. at 1914-15.

[39] *See* Pub.L. 107-56, § 505, 115 Stat. 272, 365 (2001). In 1996, Congress clarified that § 2709 requests included both local and long-distance telephone records. *See* 18 U.S.C. § 2709 (2000); *see also* S.Rep. No. 104-258, at 22-23, *reprinted in* 1996 U.S.C.C.A.N. 3945, 3967-68 (explaining the change).

[40] *Compare* 18 U.S.C. § 2709 (2000) *with* 18 U.S.C. § 2709 (2000 & Supp.2003).

[41] *Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the House Comm. on the Judiciary,* 107th Cong. 57-58 (2001), *available at* http://www.house.gov/judiciary/75288.pdf (section-by-section analysis of the Anti-Terrorism Act of 2001).

[42] H.R. Rep. 107-236, at 62 (2001). The only specific objection to the § 2709 revision in the Patriot Act's legislative history came from the Center for Democracy and Technology ("CDT"), which has filed an amicus brief in this case. The CDT stated in written materials to two Senate committees that the section "would greatly increase access to the personal information of consumers or groups who are not agents of foreign powers," and also noted that "the institutions granting access to consumer information would be prohibited from disclosing that information or records had been obtained." *Protecting 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); *S. 1448, The Intelligence to Prevent Terrorism Act Of 2001 and Other Legislative Proposals in the Wake of the September 11, 2001 Attacks: Hearing Before the Senate Select Comm. On Intelligence,* 107th Cong., S. Hrg. 107-449, at 54 (2001) (same).

[43] *See* 26 U.S.C. § 7602(a).

[44] *See* 15 U.S.C. § 78u(b).

[45] *See* 7 U.S.C. § 4610a(b).

[46] *See* 16 U.S.C. § 773i(f)(2).

[47] *See* *United States v. Powell,* 379 U.S. 48, 57-58, 85 S.Ct. 248, 13 L.Ed.2d 112 (1964); *Gimbel v. Fed. Deposit Ins. Corp. (In re Gimbel),* 77 F.3d 593, 596 (2d Cir.1996).

[48] *See* *United States v. White,* 853 F.2d 107, 111 (2d Cir.1988); *see also* *Endicott Johnson Corp. v. Perkins,* 317 U.S. 501, 509, 63 S.Ct. 339, 87 L.Ed. 424 (1943) (stating that courts must enforce administrative subpoenas unless the evidence sought is "plainly ... irrelevant to any lawful purpose of the agency"); *United States v. Construction Prods. Research, Inc.,* 73 F.3d 464, 471 (2d Cir.1996).

[49] *See* *Reisman v. Caplin,* 375 U.S. 440, 449, 84 S.Ct. 508, 11 L.Ed.2d 459 (1964).

[50] *See* 12 U.S.C. § 3409(b) (providing for a court-issued non-disclosure order, in renewable 90-day increments, where an authorized Government agency subpoenas financial records); 15 U.S.C. § 78u(h)(4)(A) (providing for a court-issued non-disclosure order, in renewable 90-day increments, in SEC investigations); 18 U.S.C. § 2705(b) (providing for a court-issued non-disclosure order, "for such period as the court deems appropriate," where an authorized Government agency subpoenas stored electronic records); 18 U.S.C. § 3486(a)(6)(A) (providing for a court-issued non-disclosure order, in renewable 90-day increments, in investigations of health care fraud or crimes involving exploitation of children).

[51] 18 U.S.C. § 1505; *cf.* *United States v. Jeter,* 775 F.2d 670 (6th Cir.1985), *cert. denied,* 475 U.S. 1142, 106 S.Ct. 1796, 90 L.Ed.2d 341 (1986) (concluding that an individual could be convicted under an analogous obstruction of justice statute, 18 U.S.C. § 1503, for revealing the contents of secret grand jury transcripts to targets of the grand jury's investigation).

[52] Fed.R.Crim.P. 17(a), (c)(1) (emphasis added).

[53] *In re Grand Jury Proceedings,* 486 F.2d 85, 90 (3d Cir.1973); *see also* Fed R.Crim. P. 17(a) ("The clerk must issue a blank subpoena — signed and sealed — to the party requesting it....").

[54] Fed.R.Crim.P. 17(c)(2).

[55] *United States v. R. Enters., Inc.,* 498 U.S. 292, 299, 111 S.Ct. 722, 112 L.Ed.2d 795 (1991) (citing *United States v. Nixon,* 418 U.S. 683, 700, 94 S.Ct. 3090, 41 L.Ed.2d 1039 (1974)).

[56] *Id.* at 301, 111 S.Ct. 722.

[57] *United States v. Cleary,* 265 F.2d 459, 461 (2d Cir.1959).

[58] *See U.S. Const.* amend. VI.

[59] *See* Fed.R.Crim.P. 6(e).

[60] *See id.* at (e)(2)(A) ("No obligation of secrecy may be imposed on any person except in accordance with [Rule 6].").

[61] *See In re Subpoena to Testify Before Grand Jury,* 864 F.2d 1559, 1563-64 (11th Cir.1989); *see also In re Grand Jury Subpoena Duces Tecum,* 797 F.2d 676, 681-82 (8th Cir.1986) (permitting secrecy order pertaining to grand jury witness upon showing of compelling necessity).

[62] *See* 18 U.S.C. § 1510(b), (d).

[63] *See* 18 U.S.C. §§ 1503 (punishing "[w]hoever corruptly ... endeavors to ... impede any grand or petit juror ... [or] the due administration of justice"); 1512(b) (imposing criminal sanctions upon an person who, among other things, "corruptly persuades another person, or attempts to do so, or engages in misleading conduct toward another person, with intent to ... hinder, delay, or prevent the communication to a law enforcement officer or judge of the United States of information relating to the commission or possible commission of a Federal offense....").

[64] *See* 21 U.S.C. § 876(a).

[65] *See* 18 U.S.C. § 1968.

[66] *See* 18 U.S.C. § 3486(a)(1)(A)(i)(I).

[67] *See id.* § 3486(a)(1)(A)(i)(II).

[68] *See* 21 U.S.C. § 876(c) (providing for judicial enforcement); 18 U.S.C. § 1968(g) (same); *id.* § 3486(c) (same).

[69] Basic subscriber information includes: (1) a subscriber's name and (2) address; (3) the subscriber's local and long distance telephone connection records, or records of session times and durations; (4) the subscriber's length of service and types of service he has utilized; (5) any telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (6) the subscriber's means and source of payment for the service. *See* 18 U.S.C. § 2703(c)(2).

[70] *See* 18 U.S.C. § 2703(c)(2)-(3).

[71] *See* 18 U.S.C. § 2705.

[72] *See id.* § 2703(a)-(b). This rough description of the complex statutory terrain derives from the Justice Department's thorough analysis of the ECPA. *See* United States Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 94 (2002), *available at*http://www.cybercrime.gov/s&smanual2002.pdf. Courts are not uniform in interpreting the statute's confusing and overlapping definitions. *Compare Theofel v. Farey-Jones,* 359 F.3d 1066, 1076-77 (9th Cir.2004) (holding that copies of opened emails on ISP servers are in "electronic storage"), *with In*

re DoubleClick, Inc. Privacy Litig., 154 F.Supp.2d 497, 512 (S.D.N.Y.2001) (stating that only *un* opened email on an ISP server would be considered in "electronic storage"); *see also* *Fraser v. Nationwide Mut. Ins. Co.*, 135 F.Supp.2d 623, 633 (E.D.Pa.2001), *rev'd in part on other grounds,* 352 F.3d 107 (3d Cir.2003) ("The ECPA has been noted for its lack of clarity.").

[73] *See id.* § 2703(a).

[74] *See* Fed.R.Crim.P. 41.

[75] 18 U.S.C. § 2703(d).

[76] *Id.* § 2705(b).

[77] *See* 39 C.F.R. § 233.3.

[78] *See id.* § 233.3(e)(2).

[79] *See* *Ex parte Jackson,* 96 U.S. 727, 733, 24 L.Ed. 877 (1877).

[80] *Id.*

[81] *See* 18 U.S.C. § 3127(3)-(4).

[82] *See id.* § 3123(c).

[83] *Id.* § 3123(a).

[84] *See* 18 U.S.C. § 3123(d)(2).

[85] *See* *Katz v. United States,* 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967).

[86] *See* 18 U.S.C. §§ 2516-18.

[87] *Id.* § 2518(3).

[88] *Id.* § 2518(5).

[89] *Id.* § 2511(2)(a)(ii).

[90] *See* 50 U.S.C. § 1801 *et seq.*

[91] *Id.* § 1802(a)(1).

[92] *Id.* § 1802(a)(4)(A).

[93] *See id.* §§ 1804-1805.

[94] *See id.* § 1804.

[95] *Id.* § 1804(a)(7).

[96] *Id.* § 1805(a).

[97] *Id.* § 1805(e).

[98] *Id.* § 1805(c)(2)(B).

[99] 50 U.S.C. § 1861(a).

[100] *See id.* §§ 1861(b), (c).

[101] *See id.* § 1861(d).

[102] 50 U.S.C. § 1842(a)(1).

[103] *See id.* § 1842(c).

[104] 50 U.S.C. § 1842(d)(2)(B)(ii)(I).

[105] Fed.R.Civ.P. 56(c).

[106] *See Halverson v. Slater,* 129 F.3d 180, 186 (D.C.Cir.1997) ("legislative intent cannot fairly be inferred from different language in two sections of different enactments") (citing *Pure Oil Co. v. Suarez,* 384 U.S. 202, 206, 86 S.Ct. 1394, 16 L.Ed.2d 474 (1966)); *see also Fourco Glass Co. v. Transmirra Prods., Corp.,* 353 U.S. 222, 77 S.Ct. 787, 1 L.Ed.2d 786 (1957) (holding that the general venue provisions governing federal civil actions, even if reflecting some similarities in the actual usage of some terms, do not carry over into or supplement previously enacted venue rules controlling patent infringement actions). In addition, and as noted above, the EPCA, in which § 2709 was enacted, has previously been "noted for its lack of clarity." *Fraser v. Nationwide Mut. Ins. Co.,* 135 F.Supp.2d 623, 633 (E.D.Pa.2001), *rev'd in part on other grounds,* 352 F.3d 107 (3d Cir.2003).

[107] *Compare* 12 U.S.C. § 3414(a)(5)(D) (prohibiting disclosure to "any person") *and* 15 U.S.C. § 1681v(c) (same)*and* 18 U.S.C. § 2709(c) (same) *with* 15 U.S.C. § 1681u(d) (exempting disclosure to "those officers, employees, or agents ... necessary to fulfill the requirement to disclose information ... under this section") *and* 50 U.S.C. § 436(b) (exempting disclosure to "those officers, employees, or agents of such entity necessary to satisfy a request made under this section").

[108] *Compare, e.g.,* 18 U.S.C. § 2709 *with, e.g.,* 26 U.S.C. § 7604(b) (providing for judicial enforcement of IRS-issued administrative subpoenas) *and* 15 U.S.C. § 78u(c) (providing for judicial enforcement of SEC-issued administrative subpoenas) *and* Fed.R.Crim.P. 17(c)(2) (permitting motions to quash subpoenas in criminal cases).

[109] *Compare, e.g.,* 18 U.S.C. § 2709 *with, e.g.,* 26 U.S.C. § 7604(b) (authorizing contempt sanctions for failure to comply with IRS-issued administrative subpoenas) *and* 15 U.S.C. § 78u(c) (providing penalties of up to one year imprisonment and a $1,000 fine for failure to comply with SEC-issued administrative subpoenas).

[110] *See H.R. 3179, The "Anti-Terrorism Intelligence Tools Improvement Act of 2003": Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary,* 108th Cong. (2004) ("H.R. 3179 Hg.") (opening statement of Rep. Coble, Chairman, Subcomm. on Crime, Terrorism, and Homeland Security of the House Comm. on the Judiciary):

The current law authorizes the Federal Government to use a National Security Letter, which is basically an administrative subpoena, to make a request for transactional records, such as billing records. These requests must be related to investigations of international terrorism or clandestine intelligence activities. The current law, however, has no mechanism to enforce the requests. Furthermore, the current law provides no penalty for an individual who decides to tip off a target of a terrorism or an intelligence investigation that the Federal government has made a National Security letter request concerning the target.

[111] It should also be noted that the Department of Justice's position in this litigation is inconsistent with the position taken by the FBI in hearings on H.R. 3179. In the May 18, 2004 hearing on H.R. 3179, Thomas J. Harrington, Deputy Assistant Director of the FBI's Counterterrorism Division, told the House subcommittee examining the bill that legislation was necessary to provide the FBI with a means of seeking judicial enforcement of an NSL:

H.R. 3179 also provides for a procedure for judicial enforcement if a recipient of a National Security Letter does not comply with the mandatory request for information.... An example of where this provision would have been helpful is a case where during an investigation into international terrorist activities, analysis revealed that several subjects were using a third party internet service as a potential means of communication. NSLs served on the third party service revealed that an associate of

the subjects registered for the service using a free, web-based email service. NSLs were served on the web-based email service in order to obtain electronic transactional records. The web-based email service has not yet provided the records associated with the request. A judicial enforcement provision, such as the one included in H.R. 3179, would assist by providing a forum to quickly resolve this issue and allow the investigation to move forward more expeditiously.

Id. (statement of Thomas J. Harrington, Deputy Assistant Dir., Counterterrorism Div., FBI).

[112] *See* H.R. 3179, 108th Cong. § 2 (2003).

[113] Antiterrorism Tools Enhancement Act of 2003, H.R. 3037, 108th Cong. § 3 (2003) (proposed 18 U.S.C. § 2332g(a)).

[114] *Id.* (proposed 18 U.S.C. § 2332g(c)).

[115] *Id.* (proposed 18 U.S.C. § 2332g(a)(1)).

[116] *See* S. 2555, 108th Cong. (2004).

[117] *See id.* § 2 (proposed 18 U.S.C. § 2332g(d) clarifying the scope of the nondisclosure requirement; proposed 18 U.S.C. § 2332g(e) stating that judicial review is available to modify or set aside the summons or the nondisclosure requirement).

[118] To be clear, the Fourth Amendment rights at issue here belong to the person or entity receiving the NSL, not to the person or entity to whom the subpoenaed records pertain. Individuals possess a limited Fourth Amendment interest in records which they voluntarily convey to a third party. *See Smith,* 442 U.S. at 742-46, 99 S.Ct. 2577;*Miller,* 425 U.S. at 440-43, 96 S.Ct. 1619. Nevertheless, as discussed below, many potential NSL recipients may have particular interests in resisting an NSL, *e.g.,* because they have contractually obligated themselves to protect the anonymity of their subscribers or because their own rights are uniquely implicated by what they regard as an intrusive and secretive NSL regime. For example, since the definition of "wire or electronic communication service provider," 18 U.S.C. § 2709(a), is so vague, the statute could (and may currently) be used to seek subscriber lists or other information from an association that also provides electronic communication services (e.g., email addresses) to its members, or to seek records from libraries that many, including the *amici* appearing in this proceeding, fear will chill speech and use of these invaluable public institutions. Fear that § 2709 may be used as a tool to gain sensitive information from libraries has led both houses of Congress to introduce bills intended to exclude libraries from the ambit of § 2709. *See* S. 1709, Security and Freedom Assured ("SAFE") Act of 2003, 108th Cong. § 5 (2003) (proposing to amend § 2709(a) to state that a "library shall not be treated as a wire or electronic communication service provider for purposes of this section"); H.R. 3352, 108th Cong. § 5 (2003) (same).

[119] *See* U.S. Const. amend. IV; *United States v. Streifel,* 665 F.2d 414 (2d Cir.1981).

[120] *Streifel,* 665 F.2d at 419-20.

[121] *See United States v. Morton Salt Co.,* 338 U.S. 632, 651-52, 70 S.Ct. 357, 94 L.Ed. 401 (1950).

[122] *Id.*

[123] *Gimbel v. Federal Deposit Ins. Corp. (In re Gimbel),* 77 F.3d 593, 596 (2d Cir.1996) (internal quotation marks and citation omitted).

[124] *Morton Salt Co.,* 338 U.S. at 652, 70 S.Ct. 357; *see also Oklahoma Press Pub. Co. v. Walling,* 327 U.S. 186, 208, 66 S.Ct. 494, 90 L.Ed. 614 (1946) ("The gist of the protection is ... that the disclosure sought shall not be unreasonable.").

[125] *United States v. Bailey (In re Subpoena Duces Tecum),* 228 F.3d 341, 348 (4th Cir.2000).

[126] *See v. City of Seattle,* 387 U.S. 541, 544-45, 87 S.Ct. 1737, 18 L.Ed.2d 943 (1967); *see also Oklahoma Press,* 327 U.S. at 217, 66 S.Ct. 494

[127] *Oklahoma Press,* 327 U.S. at 217, 66 S.Ct. 494.

[128] 18 U.S.C. §§ 2709(b)(1), (b)(2).

[129] 18 U.S.C. § 2709(a). *But see* H.R. 3179 Hg. (containing statements by a senior FBI official and the Chairman of the House Subcommittee on Crime, Terrorism, and Homeland Security arguing that the current NSL statutes are merely hortatory); *supra* Part II.C (discussing other indications that Congress did not intend § 2709 to have the meaning ascribed to it by the Government in this case).

[130] *United States v. Hill,* 694 F.2d 258, 263 (D.C.Cir.1982) (emphasis in original) (collecting cases).

[131] 18 U.S.C. § 2709(a).

[132] *United States v. Doe (In re Grand Jury Proceedings),* 219 F.3d 175, 183 (2d Cir.2000).

[133] 18 U.S.C. § 2709(c) (emphasis added).

[134] *See* Pub.L. No. 104-93, 109 Stat. 961 (1996) (codified as amended at 15 U.S.C. § 1681u(d)).

[135] H.R. Conf. Rep. No. 104-427, at 39 (1995), *reprinted in* 1995 U.S.C.C.A.N. 993, 1001.

[136] *See Nix v. O'Malley,* 160 F.3d 343 (6th Cir.1998); *McQuade v. Michael Gassner Mech. & Elec. Contractors, Inc.,* 587 F.Supp. 1183 (D.Conn.1984).

[137] *Nix,* 160 F.3d at 351.

[138] *McQuade,* 587 F.Supp. at 1190.

[139] *INS v. St. Cyr.,* 533 U.S. 289, 299-300, 121 S.Ct. 2271, 150 L.Ed.2d 347 (2001) (quotation marks and citation omitted); *see also Edward J. DeBartolo Corp. v. Florida Gulf Coast Bldg. and Const. Trades Council,* 485 U.S. 568, 575, 108 S.Ct. 1392, 99 L.Ed.2d 645 (1988) (holding that "every reasonable construction must be resorted to, in order to save a statute from unconstitutionality") (quotation marks and citation omitted).

[140] *United States v. Locke,* 471 U.S. 84, 96, 105 S.Ct. 1785, 85 L.Ed.2d 64 (1985) (quoting *George Moore Ice Cream Co. v. Rose,* 289 U.S. 373, 379, 53 S.Ct. 620, 77 L.Ed. 1265 (1933) (Cardozo, J.)).

[141] Simon & Garfunkel, *Sounds of Silence* (Columbia 1966).

[142] *See, e.g., Marvel Characters, Inc. v. Simon,* 310 F.3d 280, 290 (2d Cir.2002) ("In interpreting a statute, we look first to the language of the statute itself.").

[143] *See Halverson,* 129 F.3d at 186 n. 9 ("Caution must be exercised in applying the rule that one statute will be interpreted to correspond to analogous but unrelated statutes for the reason that by way of contrast an inclusion or exclusion may show an intent or convey a meaning exactly contrary to that expressed by analogous legislation.") (quoting 2B Norman J. Singer, *Sutherland Stat. Const.* § 53.05 (5th ed.1992)).

[144] Compl. Attach. A.

[145] *See* Letter from Jamie E. Brown, Acting Assistant Attorney General, United States Dep't of Justice, to The Honorable F. James Sensebrenner, Jr., Chairman, Committee on the Judiciary, U.S. House of Representatives 4 (May 13, 2003), *available at* http:// www.lifeandliberty.gov-/subs/congress/hjcpatriotactcombinedresponses3.pdf (answering Chairman Sensebrenner's question, "Has any litigation resulted from the issuance of these [National Security] letters i.e. challenging the propriety or legality of their use? If so, please describe," as follows: "*Answer:*There has been no challenge to the propriety or legality of National Security Letters.").

[146] In fact, the evidence suggests that perhaps even the FBI does not actually believe that § 2709 contemplates judicial review. First, as discussed above, a senior FBI official testified before Congress that was no judicial enforcement provision in § 2709. *See* H.R. 3179 Hg. (statement of Thomas J. Harrington, Deputy Assistant Director, FBI). Second, Plaintiffs have obtained, via a FOIA request, two FBI memoranda concerning implementing and serving NSLs, yet neither memorandum discusses or even mentions the possibility that an NSL recipient could challenge the NSL in court.

[147] 372 U.S. 58, 83 S.Ct. 631, 9 L.Ed.2d 584 (1963).

[148] *See id.* at 71-72, 83 S.Ct. 631.

[149] *See id.* at 68-70, 83 S.Ct. 631.

[150] *Id.* at 68, 83 S.Ct. 631.

[151] *Id.* at 68-69, 83 S.Ct. 631.

[152] The Court further notes that the coercive practices invalidated in *Bantam Books* may have never even been challenged if the real parties in interest in the suit, the publishers whose books were taken off the shelves, were unable to learn of the existence of the coercive activities taking place in Rhode Island. In *Bantam Books,* the distributor who was the target of the challenged coercive letters actually complied with their "recommendations,"*see id.* at 63, 83 S.Ct. 631, but the publishers whose interests were most directly harmed by the letters learned of the letters and promptly challenged them, *see id.* at 64, 83 S.Ct. 631 (explaining that publishers gained standing to challenge the censorship letters, even though they never directly received the letters, in part because "the publisher has the greater economic stake [in resisting the letters].... Unless he is permitted to sue, infringements of freedom of the press may often go unremedied.") (citing *N.A.A.C.P. v. State of Alabama ex rel. Patterson,* 357 U.S. 449, 459, 78 S.Ct. 1163, 2 L.Ed.2d 1488 (1958)). Section 2709's secrecy provisions, along with the clear terms of the NSL form used by the FBI, affirmatively prohibit the party whose interests are most affected by the NSL — the communications service subscriber(s) whose records are targeted by the NSL — from ever learning about or gaining the ability to challenge the NSL. The secrecy surrounding NSLs thus makes them even less subject to judicial challenge than any non-secret form of coercive government activity.

[153] *See In re Grand Jury Proceedings,* 814 F.2d 61 (1st Cir.1987).

[154] *Id.* at 63-64.

[155] *See* Fed.R.Crim.P. 6(e)(2).

[156] *In re Grand Jury Proceedings,* 814 F.2d at 64, 70.

[157] *See Bantam Books,* 372 U.S. at 71, 83 S.Ct. 631 ("The *procedures of the Commission* are radically deficient.... We hold that the *system of informal censorship disclosed by this record* violates the Fourteenth Amendment"); *id.* at 74-75, 83 S.Ct. 631 (Clark, J., concurring) (emphasis added) (noting that the opinion of the Court did not invalidate the Rhode Island statute which appeared to authorize the coercive tactics undertaken by the commission).

[158] *St. Cyr,* 533 U.S. at 299-300, 121 S.Ct. 2271.

[159] *Id.*

[160] As discussed above, an ISP may be obligated by contract or other arrangement to assert its subscribers' rights, even if the subscriber herself is unaware of the existence of the NSL and is not able to personally assert her own rights. In addition, associations or other organizations that receive NSLs may have their own independent First Amendment or other interests in protecting their subscribers' information from discovery.

[161] 362 U.S. 60, 80 S.Ct. 536, 4 L.Ed.2d 559 (1960)

[162] *Id.* at 64, 80 S.Ct. 536.

[163] *See McIntyre v. Ohio Elections Comm'n,* 514 U.S. 334, 341-57, 115 S.Ct. 1511, 131 L.Ed.2d 426 (1995).

[164] *See Buckley v. American Constitutional Law Found.,* 525 U.S. 182, 199-200, 119 S.Ct. 636, 142 L.Ed.2d 599 (1999).

[165] *See Watchtower Bible & Tract Soc. of New York, Inc. v. Village of Stratton,* 536 U.S. 150, 160-69, 122 S.Ct. 2080, 153 L.Ed.2d 205 (2002).

[166] *NAACP v. State of Alabama ex rel. Patterson,* 357 U.S. 449, 462, 78 S.Ct. 1163, 2 L.Ed.2d 1488 (1958); *see also Gibson v. Florida Legislative Investigation Comm.,* 372 U.S. 539, 546-558, 83 S.Ct. 889, 9 L.Ed.2d 929 (1963) (reversing contempt sanctions against NAACP official who refused to produce membership list to state investigative

committee); *Bates v. City of Little Rock,* 361 U.S. 516, 522-26, 80 S.Ct. 412, 4 L.Ed.2d 480 (1960)(reversing convictions of NAACP officials who refused to disclose membership list to local tax officials, as required by municipal ordinance).

[167] *Gibson,* 372 U.S. at 546, 83 S.Ct. 889; *Bates,* 361 U.S. at 524, 80 S.Ct. 412.

[168] The NSL itself asks the recipient to provide the Government with "[a]ny other information *which you consider to be* an electronic communication transactional record," Compl. Attach. A (emphasis added), in addition to information that § 2709 specifically authorizes the FBI to collect, including "the name, address, and length of service of a person or entity." 18 U.S.C. § 2709(b)(2).

[169] *See Smith v. Maryland,* 442 U.S. 735, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979) (holding that installing a pen register does not violate the Fourth Amendment rights of phone customers); *United States v. Miller,* 425 U.S. 435, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (holding that a bank customer does not have any Fourth Amendment protection against the Government obtaining financial records maintained by a bank).

[170] *See, e.g., Doe v. 2TheMart.Com Inc.,* 140 F.Supp.2d 1088, 1092 (W.D.Wash.2001) ("The right to speak anonymously extends to speech via the Internet."); *Columbia Ins. Co. v. Seescandy.Com,* 185 F.R.D. 573, 578 (N.D.Cal.1999) (holding that there is a "legitimate and valuable right to participate in online forums anonymously and pseudonymously"); *see also id.* at 578-79 (establishing circumstances under which a plaintiff may compel disclosure of anonymous internet users' identities where users had allegedly committed tortious acts over the internet); *Sony Music Entm't v. Does 1-40,* 326 F.Supp.2d 556 (S.D.N.Y.2004) (holding that plaintiff could overcome anonymous internet users' First Amendment right to anonymity, asserted in anonymous users' motion to quash plaintiff's subpoena served on users' ISP, where evidence suggested that users had illegally downloaded plaintiff's music via the ISP's internet service).

[171] Courts have, however, extended the reasoning of *Smith* and *Miller* to conclude that internet users have no*Fourth Amendment* right to prohibit disclosure of information they have voluntarily turned over to ISPs. *See, e.g.,Guest v. Leis,* 255 F.3d 325, 336 (6th Cir.2001) (holding that "plaintiffs ... lack a Fourth Amendment privacy interest in their subscriber information because they communicated it to the systems operators"); *United States v. Kennedy,* 81 F.Supp.2d 1103, 1110 (D.Kan.2000) (holding that defendant could not "claim to have a Fourth Amendment privacy interest in his subscriber information" because "[w]hen defendant entered into an agreement with Road Runner for Internet service, he knowing[ly] revealed" the information to his ISP).

[172] *Red Lion Broad. Co. v. Federal Communications Comm'n,* 395 U.S. 367, 386, 89 S.Ct. 1794, 23 L.Ed.2d 371 (1969).

[173] 18 U.S.C. § 2709(a).

[174] *See id.* § 2709(b).

[175] NSLs can potentially reveal far more than constitutionally-protected associational activity or anonymous speech. By revealing the websites one visits, the Government can learn, among many other potential examples, what books the subscriber enjoys reading or where a subscriber shops. As one commentator has observed, the records compiled by ISPs can "enable the government to assemble a profile of an individual's finances, health, psychology, beliefs, politics, interests, and lifestyle." Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy,* 75 S. Cal. L.Rev. 1083, 1084 (2002).

[176] Compl. Attach. A.

[177] *Smith,* 442 U.S. at 741, 99 S.Ct. 2577 (quoting *United States v. New York Tel. Co.,* 434 U.S. 159, 167, 98 S.Ct. 364, 54 L.Ed.2d 376 (1977)).

[178] 389 U.S. 347, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967).

[179] *See id.* at 353, 88 S.Ct. 507.

[180] *Id.*

[181] *Id.* at 352, 88 S.Ct. 507.

[182] *Id.*

[183] Gov't Mem. of Law at 31.

[184] 18 U.S.C. § 2709(c).

[185] *United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 813, 120 S.Ct. 1878, 146 L.Ed.2d 865 (2000)(applying strict scrutiny to a content-based restriction); *see also* *R.A.V. v. City of St. Paul*, 505 U.S. 377, 382, 112 S.Ct. 2538, 120 L.Ed.2d 305 (1992) ("Content-based regulations are presumptively invalid,"); *Bantam Books*, 372 U.S. at 70, 83 S.Ct. 631 (holding that prior restraints on speech bear a "heavy presumption" against constitutionality).

[186] *See* *Reno v. ACLU*, 521 U.S. 844, 874, 117 S.Ct. 2329, 138 L.Ed.2d 874 (1997).

[187] *Turner Broad. Sys., Inc. v. FCC*, 520 U.S. 180, 189, 117 S.Ct. 1174, 137 L.Ed.2d 369 (1997).

[188] For this reason, the Court does not address Plaintiffs' other grounds for asserting that § 2709(c) is subject to strict scrutiny.

[189] *Ward v. Rock Against Racism*, 491 U.S. 781, 795 n. 5, 109 S.Ct. 2746, 105 L.Ed.2d 661 (1989) (emphasis omitted).

[190] Gov't Br. at 50.

[191] 44 F.3d 106 (2d Cir.1994).

[192] *Id.* at 109.

[193] *City of Renton v. Playtime Theatres, Inc.*, 475 U.S. 41, 48-49, 106 S.Ct. 925, 89 L.Ed.2d 29 (1986) (quoting*Police Dep't of Chicago v. Mosley*, 408 U.S. 92, 95-96, 92 S.Ct. 2286, 33 L.Ed.2d 212 (1972)).

[194] *Ward*, 491 U.S. at 791, 109 S.Ct. 2746.

[195] *Mosley*, 408 U.S. at 96, 92 S.Ct. 2286.

[196] *See* *Consolidated Edison Co. of New York, Inc. v. Public Serv. Comm'n*, 447 U.S. 530, 537, 100 S.Ct. 2326, 65 L.Ed.2d 319 (1980).

[197] *Id.*

[198] *Id.*

[199] *Playboy Entm't Group*, 529 U.S. at 813, 120 S.Ct. 1878.

[200] *Reno v. ACLU*, 521 U.S. at 874, 117 S.Ct. 2329.

[201] *See* *NAACP v. Button*, 371 U.S. 415, 438, 83 S.Ct. 328, 9 L.Ed.2d 405 (1963).

[202] *Department of the Navy v. Egan*, 484 U.S. 518, 527, 108 S.Ct. 818, 98 L.Ed.2d 918 (1988).

[203] *See* 18 U.S.C. § 2709(c).

[204] 18 U.S.C. § 2709(c) (emphasis added).

[205] *See* 18 U.S.C. § 3123(d)(2) (pertaining to criminal investigations); 50 U.S.C. § 1842(d)(2)(B)(ii)(I) (pertaining to international terrorism and counterintelligence investigations).

[206] *See* 18 U.S.C. § 2511(2)(a)(ii).

[207] 50 U.S.C. § 1861(d).

[208] Certain FISA electronic surveillance orders may be obtained where the Attorney General merely certifies that the proposed surveillance meets the statutory requirements. *See* 50 U.S.C. § 1802(a)(1). In such cases, the blanket secrecy rule would be triggered without any court involvement, much like § 2709(c). By way of some perhaps justifying distinction, the 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.

[209] *See* 18 U.S.C. § 2511 (wiretaps and electronic surveillance); 18 U.S.C. § 3123 (pen registers in criminal investigations); 50 U.S.C. § 1842 (pen registers in international terrorism and counterintelligence investigations); 50 U.S.C. § 1861 (FISA subpoenas).

[210] In fact, the pen register and trap and trace device statutes appear to specifically contemplate that a court could modify the secrecy requirement. *See* 18 U.S.C. § 3123(d)(2) (stating that the communications firm shall "not disclose the existence of the pen register or trap and trace device or the existence of the investigation to the listed subscriber, or to any other person, *unless or until otherwise ordered by the court*") (emphasis added); 50 U.S.C. § 1842(d)(2)(B)(ii)(I) (stating that the communications firm "shall not disclose the existence of the investigation or of the pen register or trap and trace device to any person *unless or until ordered by the court*") (emphasis added).

[211] *See supra* Part II.D.7 (discussing the FISA's requirements that any surveillance sought under the chapter be clearly connected to foreign intelligence gathering activities).

[212] *See supra* Part II.C (explaining the steady expansion of the scope of § 2709 NSL authority since the statute was passed in 1986, culminating in the removal of any required nexus between the information sought by a § 2709 NSL and a "foreign power.")

[213] 467 U.S. 20, 104 S.Ct. 2199, 81 L.Ed.2d 17 (1984).

[214] *Id.* at 32, 104 S.Ct. 2199.

[215] *Id.* at 34, 104 S.Ct. 2199.

[216] 494 U.S. 624, 110 S.Ct. 1376, 108 L.Ed.2d 572 (1990).

[217] *Id.* at 626, 110 S.Ct. 1376.

[218] *See id.* at 632-34, 110 S.Ct. 1376.

[219] *Id.* at 635, 110 S.Ct. 1376.

[220] *Id.* (quotation marks omitted).

[221] *Id.* at 636, 110 S.Ct. 1376.

[222] *Id.* at 632, 110 S.Ct. 1376.

[223] *Id.* at 633, 110 S.Ct. 1376 (emphasis in original).

[224] *Id.* at 636, 110 S.Ct. 1376 (Scalia, J., concurring).

[225] *Id.*

[226] *Id.*

[227] *See* 44 F.3d at 110-11.

[228] *Id.* at 110 (emphasis in original).

[229] *See id.* at 110-11.

[230] *Id.* at 111. The District Court had found that the secrecy rules advanced compelling state interests because they

(1) allowed the [reviewing body] to dispose of frivolous or harassing complaints without lending them credibility; (2) enhanced Connecticut's ability to attract highly qualified judges who might otherwise be deterred from service by the prospect of numerous public complaints being lodged against them; (3) ensured the independence of Connecticut's judiciary by reducing the possibility that judges would be intimidated or influenced by belligerent complainants; (4) encouraged complaints, assistance in investigations, and complete and truthful testimony; (5) allowed the [reviewing body] to informally encourage infirm or incompetent judge to retire prior to a public hearing; and (6) increased the ability of attorneys to monitor the judicial system without engendering the hostility of the judiciary.

Kamasinski, 44 F.3d at 108-09 (citing *Kamasinski v. Judicial Review Council,* 797 F.Supp. 1083, 1092-93 (D.Conn.1992)).

[231] *See First Amendment Coalition v. Judicial Inquiry & Review Bd.,* 784 F.2d 467 (3d Cir.1986) (en banc).

[232] *Id.* at 479.

[233] *See* 338 F.3d 1136 (10th Cir.2003).

[234] *Id.* at 1139.

[235] *Id.* at 1140.

[236] *Butterworth,* 494 U.S. at 636, 110 S.Ct. 1376 (Scalia, J., concurring),

[237] *Rhinehart,* 467 U.S. at 32, 104 S.Ct. 2199.

[238] *In re Halkin,* 598 F.2d 176, 206 (D.C.Cir.1979) (Wilkey, J., dissenting) *overruled by Rhinehart,* 467 U.S. at 32, 104 S.Ct. 2199 (citing *Halkin* dissent with approval).

[239] 338 F.3d at 1140.

[240] *See* 44 F.3d at 112.

[241] *See, e.g.,* Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 (establishing a presumption of public access to federal agency information subject to limited exceptions); *Environmental Protection Agency v. Mink,* 410 U.S. 73, 80, 93 S.Ct. 827, 35 L.Ed.2d 119 (1973) ("Without question, [FOIA] is broadly conceived. It seeks to permit access to official information long shielded unnecessarily from public view and attempts to create a judicially enforceable public right to secure such information from possibly unwilling official hands."); *United States v. Aguilar,*515 U.S. 593, 604 n. 3, 115 S.Ct. 2357, 132 L.Ed.2d 520 (1995) (stating that the Court would read a temporal limitation into a statute punishing disclosure of secret wiretaps in order to avoid "absurd" results); *Richmond Newspapers, Inc. v. Virginia,* 448 U.S. 555, 572, 100 S.Ct. 2814, 65 L.Ed.2d 973 (1980) ("People in an open society do not demand infallibility from their institutions, but it is difficult for them to accept what they are prohibited from observing.").

[242] FOIA itself arose, and was expanded upon, as a result of the nation's distressing experiences with excessive government secrecy. FOIA's 1974 amendments, for example, were adopted after the Watergate break-in, and the cover-up that was allowed to prevail for many months after it occurred, revealed the dangers of allowing any branch of government the unfettered ability to adopt a *per se* rule protecting information from the public eye. *See, e.g., Ray v. Turner,* 587 F.2d 1187, 1206-09 (D.C.Cir.1978) (Skelly Wright, J., concurring) (discussing the legislative history of the 1974 amendments to FOIA, and noting that the amendments, which were passed over Presidential veto, were borne out of the nation's experience with Watergate). The recognition that excessive secrecy may damage democratic values is widespread. *See, e.g., New York Times Co. v. United States,* 403 U.S. 713, 719, 91 S.Ct. 2140, 29 L.Ed.2d 822 (1971) (Black, J., concurring) ("The word `security' is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment. The guarding of military and diplomatic secrets at the expense of informed representative government provides no real security for our Republic. The Framers of the First Amendment, fully aware of both the need to defend a new nation and the abuses of the English and Colonial Governments, sought to give this new society strength and security

by providing that freedom of speech, press, religion, and assembly should not be abridged."); *Detroit Free Press v. Ashcroft,*303 F.3d 681, 683 (6th Cir.2002) ("Democracies die behind closed doors."); *National Wildlife Federation v. U.S. Forest Service,* 861 F.2d 1114, 1124 (9th Cir.1988) (Pregerson, J., concurring) ("We should all bear in mind that secret government is abhorrent to democratic values.").

[243] *Reno v. ACLU,* 521 U.S. at 874, 117 S.Ct. 2329.

[244] *See* H.R. 3037, 108th Cong. § 3 (1st Sess.2003); S. 2555 § 2 (2d Sess.2004).

[245] *See* H.R. 3037, 108th Cong. § 3 (1st Sess.2003); S. 2555 § 2 (2d Sess.2004).

[246] The Court does not intend to imply that the provisions of H.R. 3037 or S. 2555 establish any constitutional standard. Rather, the Court merely suggests that there are ways to confront the problems in § 2709(c). To echo the Supreme Court: "How or whether [the Government] is to incorporate the required procedural safeguards in the statutory scheme is, of course, for the [Government] to decide. But a model is not lacking." *Freedman v. State of Md.,* 380 U.S. 51, 60, 85 S.Ct. 734, 13 L.Ed.2d 649 (1965).

[247] *See Playboy Entm't Group,* 529 U.S. at 816, 120 S.Ct. 1878.

[248] *Id.*

[249] *Cf. Button,* 371 U.S. at 438, 83 S.Ct. 328 ("Broad prophylactic rules in the area of free expression are suspect."). The Government also argues that the rule survives strict scrutiny because individuals could mount as-applied challenges to the categorical speech ban's constitutionality, but the Court declines to view this theoretical possibility as a means of saving the statute's constitutionality when all sides agree that Congress intended a permanent, prophylactic ban on speech, and where First Amendment doctrine governing prophylactic speech bans views the bans *themselves* as suspect, regardless of their application to a theoretical case.

[250] *See United States v. U.S. Dist. Court.,* 407 U.S. 297, 322, 92 S.Ct. 2125, 32 L.Ed.2d 752 (1972).

[251] *See* H.R. Conf. Rep. 104-427, at 35-36 (1995), *reprinted in* 1995 U.S.C.C.A.N. 983, 997-98 ("Many counterintelligence investigations never reach the criminal stage but proceed for intelligence purposes or are handled in diplomatic channels.") (pertaining to NSL statute for credit records).

[252] The Court observes here that the distinction invariably between international terrorism and counterintelligence operations on one hand, and criminal investigations on the other, is not always as sharp as the Government contends. Terrorism cases, for example, are sometimes prosecuted under federal criminal laws in federal courts. In those cases, the Government's investigations must take place with all the attendant openness rules governing the criminal process. Moreover, there are undoubtedly elaborate and long-term criminal conspiracies — espionage and international drug rings, for example — which do not necessarily carry out terrorism as such. Investigating those criminal conspiracies would likely involve highly-sensitive investigative methods, and would implicate secrecy concerns similar to those characteristic of an international terrorism investigation.

[253] *CIA v. Sims,* 471 U.S. 159, 178, 105 S.Ct. 1881, 85 L.Ed.2d 173 (1985) (quotation marks, citation, and alterations omitted).

[254] *See North Jersey Media Group, Inc. v. Ashcroft,* 308 F.3d 198, 219 (3d Cir.2002) (agreeing with Government's contention that, "given judges' relative lack of expertise regarding national security and their inability to see the mosaic, [judges] should not entrust to them[selves] the decision whether an isolated fact is sensitive enough to warrant closure")

[255] *United States v. Yunis,* 867 F.2d 617, 623 (D.C.Cir.1989).

[256] *Zadvydas v. Davis,* 533 U.S. 678, 696, 121 S.Ct. 2491, 150 L.Ed.2d 653 (2001); *Egan,* 484 U.S. at 530, 108 S.Ct. 818 ("[C]ourts traditionally have been reluctant to intrude upon the authority of the Executive in military and national security affairs.") Of course, a court should not embrace these principles to the point of abdicating its constitutional duties. As the Sixth Circuit accurately observed, the Government's invocation of executive deference may have profound implications if adopted without reservation:

The Government could use its `mosaic intelligence' argument as a justification to close any public hearing completely and categorically, including criminal proceedings. The Government could operate in virtual secrecy in all matters dealing, even remotely with `national security,' resulting in a wholesale suspension of First Amendment rights.

Detroit Free Press v. Ashcroft, 303 F.3d 681, 709 (6th Cir.2002).

[257] *Members of the City Council v. Taxpayers for Vincent,* 466 U.S. 789, 803 n. 22, 104 S.Ct. 2118, 80 L.Ed.2d 772 (1984) (emphasis added).

[258] *Detroit Free Press,* 303 F.3d at 692-93.

[259] *Id.*

[260] *R.A.V.,* 505 U.S. at 382, 112 S.Ct. 2538 (quoting *Chaplinsky v. New Hampshire,* 315 U.S. 568, 572, 62 S.Ct. 766, 86 L.Ed. 1031 (1942)).

[261] Because the Court determines that § 2709(c) is invalid for the reasons discussed above, the Court declines to address Plaintiffs' additional contention that § 2709(c) is unconstitutionally vague and overbroad.

[262] *See, e.g., Denver Area Educ. Telecomm. Consortium, Inc. v. F.C.C.,* 518 U.S. 727, 767, 116 S.Ct. 2374, 135 L.Ed.2d 888 (1996) (engaging in severability analysis after concluding that a provision of a statute violated the First Amendment).

[263] *Minnesota v. Mille Lacs Band of Chippewa Indians,* 526 U.S. 172, 191, 119 S.Ct. 1187, 143 L.Ed.2d 270 (1999).

[264] "[A] court should refrain from invalidating more of the statute than is necessary.... `[W]henever an act of Congress contains unobjectionable provisions separable from those found to be unconstitutional, it is the duty of this court to so declare, and to maintain the act in so far as it is valid.'" *Alaska Airlines, Inc. v. Brock,* 480 U.S. 678, 684, 107 S.Ct. 1476, 94 L.Ed.2d 661 (1987) (quoting *Regan v. Time, Inc.,* 468 U.S. 641, 652, 104 S.Ct. 3262, 82 L.Ed.2d 487 (1984) (plurality opinion)).

[265] *Buckley v. Valeo,* 424 U.S. 1, 108, 96 S.Ct. 612, 46 L.Ed.2d 659 (1976) (quoting *Champlin Refining Co. v. Corporation Comm'n,* 286 U.S. 210, 234, 52 S.Ct. 559, 76 L.Ed. 1062 (1932)).

[266] *Alaska Airlines,* 480 U.S. at 684, 107 S.Ct. 1476.

[267] At a conference with the parties on September 10, 2004, in preparation for drafting this opinion, the Court advised the parties of the practical difficulties of maintaining the broad scope of the seal order in light of the Court's need to openly discuss all the relevant facts and its inability to elide vital information in a coherent ruling. The Government, following internal consultations, subsequently informed the Court and Plaintiffs that it would express no objection to a modification of the seal order to take account of the Court's concerns. Along related lines, Plaintiffs' motion to exclude the Government's *ex parte* affidavit, dated August 6, 2004, is rendered moot because the information presented in that affidavit has no bearing on the Court's judgment.

[268] Because the Court has granted Plaintiffs' motion for summary judgment on other grounds, the Court declines to address Plaintiffs' alternative argument that the statute violates the Fifth Amendment by failing to provide notice to persons to whom the records pertain.