

FILED

2005 AUG 29 P 2:40

UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF CONNECTICUT

U.S. DISTRICT COURT  
BRIDGEPORT, CONN.

LIBRARY CONNECTION, INC.;  
AMERICAN CIVIL LIBERTIES UNION;  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION;

Plaintiffs,

v.

ALBERTO GONZALES, 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;  
capacities; JOHN SNOW, in his official capacity  
of Secretary of the Treasury;  
MICHAEL J. WOLF, in his official capacity as  
as Special Agent in Charge, Federal Bureau of  
Investigation,

Defendants.

Civil Action No. 3:05cv1256 JCH

SEALED CASE

**DEFENDANTS' OPPOSITION TO PLAINTIFF'S  
MOTION FOR PRELIMINARY INJUNCTION**

**INTRODUCTION**

Plaintiffs Library Connection, Inc. ("Library Connection"), the American Civil Liberties Union ("ACLU"), and the American Civil Liberties Union Foundation ("ACLUF") ask the Court for mandatory, preliminary injunctive relief that would force the disclosure of confidential information from an ongoing FBI counter-terrorism investigation. Preliminary injunction is by itself an extraordinary remedy; the mandatory injunction Plaintiffs seek is more unusual still. To justify the mandatory change in the *status quo* Plaintiffs demand, which once done cannot be undone, Plaintiffs must demonstrate an imminent, irreparable harm and an exceptional likelihood

of success on the merits.

Plaintiffs have not done so. Contrary to Plaintiffs' assertion, 18 U.S.C. § 2709(c) has not prevented them from publicizing to Congress or anyone else that the National Security Letter ("NSL") power has been used to request information relating to library patrons – as the ACLU's own press release and A-Section articles on this issue in the New York Times and Washington Post attest. Plaintiffs point to no other compelling rationale for immediate and irreversible injunctive relief forcing the government to reveal the one piece of information it seeks to preserve here – the name of the particular entity served with an NSL – before the merits of this issue are considered. Indeed, the only other court to consider this issue – the Southern District of New York – has recognized that, whatever its disagreements with the specifics of the government's position on § 2709(c), the government's need to preserve the secrecy of this information in the near term is "compelling," and has stayed any enforcement of its judgment until the U.S. Court of Appeals for the Second Circuit decides this issue. See Ashcroft v. Doe, 05-0570 (2d Cir. filed Aug. 18, 2005). Whatever short-term harm to Plaintiff can be imagined from the temporary non-disclosure of its name, it is no greater here than it was there.

By contrast, the harm to the government and the public interest from disclosure of Plaintiff's name is immediate and irreparable. What Plaintiffs insincerely characterize as a minor disclosure – the "mere fact" that Library Connection is the recipient of the NSL – strikes at the heart of the non-disclosure provision (as the Doe court recognized in its stay). By publicizing Library Connection's name to the world as the recipient of the NSL, Plaintiffs will alert the target of the Federal Bureau of Investigation's ("FBI's") ongoing counter-terrorism investigation that his activities are potentially subject to scrutiny. Armed with this information, this individual can

hide, move his activities to another provider, provide misinformation to the government, or otherwise frustrate the FBI's investigation, as explained by FBI Assistant Director for Counterintelligence David Szady. It also would alert other terrorist and foreign intelligence actors to avoid this provider in the future, and provide invaluable information to hostile terrorist groups and foreign intelligence agencies on the geographic focus and methodology of the FBI's counter-terrorism investigations generally. This damage is irreversible, and could not be amended in a subsequent hearing on the merits.

Finally, when the merits of the non-disclosure provision are considered, it is clear that Plaintiffs have not demonstrated the exceptional likelihood of success they need for irreversible, mandatory injunctive relief here. The Supreme Court, the Second Circuit, and other courts of appeal have upheld non-disclosure restrictions like the one at issue here, reasoning that restrictions on information a party learns only by virtue of its participation in a confidential government investigation do not raise the same First Amendment concerns as other restrictions on speech. The Supreme Court in particular has held that such restrictions need only pass intermediate scrutiny, and the non-disclosure provision at issue here does so easily: the government's interest in preserving the effectiveness of counter-terrorism investigations is compelling, and the terms of § 2709(c) are appropriately tailored to the unique circumstances of such investigations. Even in Doe, on which Plaintiffs rely heavily, the district court followed these principles and agreed with the government that, under the First Amendment, the FBI's legitimate need for secrecy justifies non-disclosure for at least some period. Although it disagreed with the government about whether such restrictions could be *permanent*, it recognized that this issue took the court into "uncharted legal terrain," and stayed enforcement of its

judgment without allowing the irreversible disclosure Plaintiffs ask for here.

The Court should deny Plaintiff's Motion for Preliminary Injunction.

#### STATUTORY AND REGULATORY BACKGROUND

The President of the United States has given the FBI primary responsibility and authority for conducting counterintelligence and counter-terrorism investigations within the United States. See Exec. Order No. 12333 § 1.14(a), 3.4(a), 46 Fed. Reg. 59,941 (Dec. 4, 1981); see also Declaration of David Szady, Assistant Director, Counterintelligence Division, FBI ("Szady Decl.") ¶4. The President also has authorized the FBI to conduct counterintelligence activities outside the United States in coordination with the Central Intelligence Agency. See id. § 1.14(b); Szady Decl. ¶5.

#### I. 18 U.S.C. § 2709

Congress and the FBI have recognized that electronic communications play an increasingly important role in counterintelligence and counter-terrorism investigations. See S. Rep. No. 99-541, p. 44 (1986), reprinted in 1996 U.S.C.C.A.N. 3598 (concluding that information about such communications is "highly important to the successful investigation of counterintelligence cases"); Szady Decl. ¶14. To assist the FBI in obtaining information about these communications, Congress enacted 18 U.S.C. § 2709, as part of the Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (Oct. 21, 1986). Section 2709 empowers the FBI to issue administrative subpoenas, known as "National Security Letters," or "NSLs," to providers of electronic communication services as part of counterintelligence and counter-terrorism investigations. See 18 U.S.C. § 2709. Subsections (a) and (b) of Section 2709 authorize the FBI to request "subscriber information" and "toll billing information," or

“electronic communication transactional records,” from wire or electronic communication service providers. Subsection (a) directs providers to comply with such requests.

Although § 2709 authorizes the FBI to seek subscriber and transactional information, it does *not* authorize the FBI to request the contents of any communication. See 18 U.S.C. § 2709; see also S. Rep. 99-541 1, 44 (Oct. 17, 1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3598 (“It should be noted that [18 U.S.C. § 2709] applies only to transactional records, not to the content of the electronic messages of a customer or subscriber”). Furthermore, unlike other administrative subpoenas, an NSL may be issued only upon specific certifications of fact. In particular, subsection (b) provides that, in order to issue an NSL, the Director of the FBI, or a designee “not lower than Deputy Assistant Director at Bureau headquarters or a Special Agent in Charge in a Bureau Field Office” must certify that the information sought is “relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities,” and that any such investigation “is not conducted solely on the basis of activities protected by the First Amendment.” 18 U.S.C. § 2709.<sup>1/</sup>

To ensure the confidentiality and effectiveness of counterintelligence and counterterrorism investigations, § 2709(c) establishes a non-disclosure rule concerning the FBI’s request for records. Section 2709(c) provides that “[n]o wire or electronic service provider or officer, employee or agent thereof, shall disclose to any person that the Federal Bureau of Investigation

---

<sup>1/</sup> cf. 7 U.S.C. § 12 (authorizing administrative subpoenas by Commodities Futures Trading Commission without certification requirement); 15 U.S.C. § 49 (same for Federal Trade Commission); 15 U.S.C. § 772(e) (same for Administrator of Federal Energy Administration); 29 U.S.C. § 209 (same for Secretary of Labor and Administrator of Wage and Hour Division); 42 U.S.C. § 7255 (same for Secretary of Energy); also cf. Fed. R. Crim. P. 17(c) (federal rule governing issuance of grand jury subpoenas).

has sought or obtained access to information or records under this section.” In turn, subsection (d) places limits on the FBI’s dissemination of information and records obtained pursuant to NSLs. See 18 U.S.C. § 2709(d). Finally, subsection (e) provides that the FBI “shall fully inform” Congress on a “semiannual basis ... concerning all requests for information” made through such NSLs. See id. § 2709(e).<sup>2</sup>

## **II. The Need for Confidentiality in Counterintelligence and Counter-Terrorism Investigations**

Congress repeatedly has recognized the need for secrecy when conducting counterintelligence and counter-terrorism investigations, and each of the several statutes allowing issuance of NSLs includes a non-disclosure provision similar to 18 U.S.C. § 2709(c). See 12 U.S.C. § 3414(a)(1) (requests from certain government authorities for financial records); 12 U.S.C. § 3414(a)(5) (FBI requests to financial institutions for financial records of customers); 15 U.S.C. § 1681u (FBI requests to consumer reporting agencies for records seeking identification of financial institutions and other identifying information of consumers); 15 U.S.C. § 1681v (government agency requests to consumer reporting agencies for consumer reports and all other information in consumers’ files); 50 U.S.C. § 436(b) (investigative agency requests to financial institutions or consumer reporting agencies for financial information and consumer reports needed for authorized law enforcement investigation, counterintelligence inquiry, or security determination). As Congress has explained, “the FBI could not effectively monitor and counter

---

<sup>2</sup> Congress has amended section 2709 on several occasions since its enactment, most recently in the USA PATRIOT Act. See Pub. L. No. 107-56, § 505, 115 Stat. 272, 365 (2001); see also Pub. L. No. 103-142, § 1, 107 Stat. 1491, 1491 (1993); Pub. L. No. 104-293, § 601(a), 110 Stat. 3461, 3469 (1996). In general terms, these amendments have liberalized the standards for issuance of NSLs, while leaving the basic structure of the statute undisturbed.

the clandestine activities of hostile espionage agents and terrorists if they had to be notified that the FBI sought their ... records for counterintelligence investigations,” and the “effective conduct of FBI counterintelligence activities requires such non-disclosure.” H. Rep. 99-690(I) at 15, 18, reprinted in 1986 U.S.C.C.A.N. 5341, 5345 (regarding enactment of 12 U.S.C. § 3414(a)(5)); see also H. Rep. 95-1383 at 228 (July 20, 1978), reprinted in 1978 U.S.C.C.A.N. 9273, 9359 (non-disclosure requirement “assure[s] the absolute secrecy needed for the investigations covered by [the provision]”) (regarding enactment of 12 U.S.C. § 3414(a)(3)).

Congress has imposed similar non-disclosure requirements in connection with the use of other investigative techniques apart from NSLs in counterintelligence and counter-terrorism investigations. See 50 U.S.C. § 1842(d)(2)(B) (pen register or trap and trace device for foreign intelligence and counter-terrorism investigations); 50 U.S.C. § 1861(d)(2)(order for production of tangible things in connection with counterintelligence and counter-terrorism investigations); 50 U.S.C. § 1802(a)(4)(A) (electronic surveillance for purposes of intercepting foreign intelligence information); 50 U.S.C. § 1822(a)(4)(A) (physical search for foreign intelligence information). Here too, Congress has concluded that “[b]y its very nature foreign intelligence surveillance must be conducted in secret.” S. Rep. 5-604(I) at 60 (Nov. 15, 1997), reprinted in 1978 U.S.C.C.A.N. 3904, 3962

The FBI likewise has concluded that secrecy is essential to the functioning of counterintelligence and counter-terrorism investigations. As explained by Assistant Director Szady, counterintelligence and counter-terrorism investigations differ greatly from typical criminal investigations, in which investigators gather evidence of past acts with an eye toward prosecution and conviction. See Szady Decl. ¶8. Instead, counterintelligence and counter-

terrorism investigations are long-range, forward-looking and prophylactic in nature: the agency aims to anticipate and disrupt clandestine intelligence activities and terrorist attacks on the United States before they occur. See id.; see also 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). Because counterintelligence and counter-terrorism investigations are directed at groups taking efforts to keep their own activities secret, it is essential that targets not learn that they are the subject of investigation. See id. If targets learn that they are the subjects of investigation, they can be expected to take action to avoid detection or disrupt the government’s intelligence gathering efforts. See id. ¶9. Targets may flee, warn other co-conspirators, destroy damaging evidence, create false evidence or disinformation, or switch to alternate methods of communication. See id. ¶¶9-10, 20-22. Likewise, knowledge about the scope or progress of a particular investigation allows targets to determine the FBI’s degree of penetration of their activities and to alter their timing or methods. See id. ¶10. The same logic applies to knowledge about the sources and methods the FBI is using to acquire information. See id. ¶¶10, 13, 25-26.

These concerns apply in force in the case of NSLs. Disclosing the recipient of an NSL issued as part of a particular counter-terrorism investigation, or repeatedly disclosing the names of entities that receive NSLs, can alert terrorist organizations that operatives using certain electronic service providers or types of providers are potentially compromised, leading them to change operatives, change providers, or otherwise alter their activities to avoid detection. See id. ¶¶20-25. Knowledge about the recipient of an NSL or the particular information sought or

obtained also can allow terrorist organizations or intelligence agencies to deduce which of their members have decided to cooperate with the government, leading not only to a change in tactics but also to potential reprisals against family members of the suspected cooperator. See id. ¶30. Even where terrorist groups do not make use of targeted providers, knowledge about which providers the FBI seeks information from, or otherwise where the FBI is obtaining information from NSLs, can help them to avoid such providers and sources in the future. See id. ¶29. Indeed, apart from disclosing the name of the ultimate target of an investigation, disclosing the name of the recipient of an NSL is can be the most potentially harmful revelation possible in connection with an NSL. See id.

Furthermore, such disclosure need not be explicit in order to benefit terrorist groups and foreign intelligence agencies. As the FBI has determined through past and on-going counterintelligence and counter-terrorism investigations, terrorist and foreign intelligence organizations have the capability and sophistication to closely analyze publicly available information concerning the United States' intelligence-gathering activities. See id. ¶¶12-13, 28. Terrorist and foreign intelligence organizations can and do piece together various, seemingly innocuous items of publicly available information, along with private information already in their possession, to determine the scope, focus, and progress of ongoing counterintelligence and counter-terrorism investigations. See id.

Finally, the special nature of counterintelligence and counter-terrorism investigations affects the duration of secrecy necessary. In typical criminal investigations, evidence is collected concerning past acts, and any need for secrecy in connection with the gathering of this evidence disappears after it is used in a prosecution and conviction. By contrast, in

counterintelligence and counter-terrorism investigations, information used against one target may be used against additional targets in the future. See id. ¶¶8, 11, 31-33. In particular, such information may be used to identify additional co-conspirators or leaders of an organization, which is of special priority in investigations intended to prevent terrorist attacks and clandestine intelligence activities. See id. ¶¶31-33. If the source of the information is compromised, terrorist organizations and foreign intelligence agencies may adjust their tactics, and the information loses its usefulness against future targets. See id. ¶¶11, 32. By preserving the secrecy of such information, the FBI ensures its utility in future investigations. See id. Furthermore, often the usefulness of such information is not immediately known and becomes apparent only as additional information is acquired. See id. For this reason, it is important to preserve the secrecy of intelligence acquired in counter-terrorism investigations even where the importance of such information is not immediately apparent. See id. More generally, there is a long-range interest in keeping requests for information and other aspects of investigations secret in order to prevent terrorist groups and foreign intelligence organizations from discerning patterns or favored sources and methods of FBI counterintelligence and counter-terrorism investigations. See id. ¶¶12-13.

#### **BACKGROUND OF THIS ACTION**

Plaintiff Library Connection, Inc. ("Library Connection") is a consortium of 26 libraries in Connecticut. See Complaint ¶5. Library Connection administers an automated library system for its members that is used to track circulation and cataloging of library materials and to track community borrowing and library usage. See Compl. ¶45. Library Connection also provides Internet access at 19 of its member libraries. See id. ¶46. On July 13, 2005, FBI Special Agent

Aram A. Crandall of the FBI New Haven Field Office hand-delivered an NSL to George Christian, Executive Director of Library Connection. Compl. ¶27 (a copy of the NSL is attached to this memorandum as Exhibit A). The NSL directs Library Connection to provide to the FBI “any and all subscriber information, billing information, and access logs of any person or entity related to the following: IP Address: 216.47.180.118, Date 02/15/2005; Time 16:00 to 16:45 (PM) EST.” Ex. A. The NSL is signed by Michael J. Wolf, Special Agent in Charge for the New Haven Field Office who, in accordance with the requirements of 18 U.S.C. § 2709(b), certifies that “the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities,” and that the investigation “is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States.” Id. The NSL specifically identifies 18 U.S.C. § 2709 and its subsections as authority for the FBI’s issuance of the NSL. See id. The NSL goes on to state that “[y]ou are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.” Id. The NSL advises Library Connection to direct questions about the NSL to the New Haven field office of the FBI and requests that Library Connection provide the records personally to the FBI rather than by mail, telephone, or electronic communication. See id.

After consulting with counsel about its legal options, Library Connection refused to comply with the NSL. Instead, Plaintiffs filed this action on August 9, 2005, alleging that 18 U.S.C. § 2709 violates Plaintiffs’ rights under the First, Fourth and Fifth Amendments. See generally Compl. The following week, on August 11, 2005, Plaintiffs filed this motion for

preliminary injunction. By their motion, Plaintiffs ask the Court to allow Plaintiffs to publicly identify Library Connection as the recipient of the NSL at issue in this case and to enjoin the Department of Justice from enforcing the non-disclosure provision. See Pl. Mem. in Support of Prelim. Inj. (“Plaintiffs’ Brief”) at 2. Plaintiffs allege that the non-disclosure provision is an invalid prior restraint on speech in violation of the First Amendment. The FBI has not yet sought enforcement of the NSL against Library Connection.

Finally, this exact issue – the constitutionality of 18 U.S.C. § 2709(c)’s non-disclosure provision – is currently before the Second Circuit. See Ashcroft v. Doe, No. 05-0570 (2d Cir. filed May 24, 2005).

#### ARGUMENT

The purpose of preliminary injunctive relief is to “preserve the relative positions of the parties [– *i.e.*, the *status quo* – ] until a trial on the merits can be held.” University of Texas v. Camenisch, 451 U.S. 390, 395 (1981); see also Warnervision Entertainment Inc. v. Empire of Carolina, 101 F.3d Hamilton Watch Co. v. Benrus Watch Co., 206 F.2d 738, 742 (2d Cir. 1953) (purpose of preliminary injunctive relief is “to keep the parties, while the suit goes on, as far as possible in the respective positions they occupied when the suit began”). Preliminary relief is an “extraordinary and drastic remedy, one that should not be granted unless the movant, by a clear showing, carries the burden of persuasion.” Moore v. Consolidated Edison Co., 409 F.3d 506, 510 (2d Cir. 2005). To prevail, plaintiff bears the burden of demonstrating: (1) that it will suffer irreparable harm absent injunctive relief; and (2) either (a) that it is likely to succeed on the merits, or (b) “that there are sufficiently serious questions going to the merits to make them a fair ground for litigation, and that the balance of hardships tips decidedly in favor of the moving

party.” Id. (quoting No Spray Coalition, Inc. v. City of New York, 252 F.3d 148, 150 (2d Cir. 2001)).

Furthermore, in cases where a plaintiff seeks mandatory injunctive relief that alters the *status quo*, a still higher standard applies. See Beal v. Stern, 184 F.3d 117, 122-23 (2d Cir. 1999). In such cases, it is not enough for the plaintiff to demonstrate that it is likely to succeed on the merits of its claim. Rather, the plaintiff must demonstrate that its entitlement to victory is “clear.” Id. Moreover, in order to obtain a mandatory injunction, a plaintiff must establish that the injunction is necessary “both to protect against irreparable harm in a deteriorating circumstance created by the defendant *and* to preserve the court’s ability to enter ultimate relief.” In Re Microsoft Corporation Antitrust Litigation, 333 F.3d 517, 526 (4<sup>th</sup> Cir. 2003) (emphasis added).

A heightened standard also applies in cases where a plaintiff asks the court to grant it “relief [that] cannot be undone even if the defendant prevails at a trial on the merits.” Beal, 184 F.3d at 123. Under these circumstances as well, a plaintiff may prevail only if it demonstrates a “clear” likelihood of success on the merits. Id.

Both circumstances apply here. The *status quo* in this case is that Plaintiff is prohibited by statute from disclosing that it has received an NSL, and subject to enforcement if it violates the non-disclosure provision. Plaintiffs have asked the court to alter that *status quo*, before any decision on the merits of 18 U.S.C. § 2709, by allowing plaintiff to identify itself publicly as the recipient of the NSL and enjoining any enforcement of the non-disclosure provision by the government. Furthermore, it is obvious that the relief Plaintiffs request here cannot be undone, even if the government later prevails on the merits. Once the Court has forced the government to

allow disclosure of the identity of the recipient of the NSL, any harm to the government's counter-terrorism investigation from that disclosure is done, and the disclosure cannot be reversed. The "cat" cannot be put back in the bag.

In such circumstances, "it is particularly appropriate for the court to weigh the possible harm to other interested parties" apart from the plaintiff, and to consider whether the proposed injunction will "result in unnecessary damage to other parties ... perhaps as irreparable and more grave than the harm that might ensue from denial of the injunction." Punnet v. Carter, 621 F.2d 578, 587-88 (3<sup>rd</sup> Cir. 1980). In short, Plaintiffs face a very high burden to justify the preliminary injunction they seek here. As discussed below, they have not met that burden.

**I. Plaintiffs Have Not Established An Irreparable Harm Sufficient to Support a Mandatory Injunction.**

It is true that "[v]iolations of First Amendment rights are commonly considered irreparable injuries." Charette v. Town of Oyster Bay, 159 F.3d 749, 755 (2d Cir. 1998) (brackets in original) (quoting Bery v. City of New York, 97 F.3d 689, 693 (2d Cir. 1996)). "Nonetheless, 'it often will be more appropriate to determine irreparable injury by considering what adverse factual consequences the plaintiff apprehends if an injunction is not issued ...'" Id. (quoting Time Warner Cable v. Bloomberg L.P., 118 F.3d 917, 924 (2d Cir. 1997)); see also Rushia v. Town of Ashburnham, 701 F.2d 7, 10 (1<sup>st</sup> Cir. 1983) ("the fact that [the plaintiff] is asserting First Amendment rights does not automatically require a finding of irreparable injury."). Here, even a cursory examination of the specific consequences Plaintiffs allege shows that they have not suffered an irreparable harm worthy of the extraordinary injunctive relief they request.

Plaintiffs' primary assertion of irreparable harm has been that they are unable to inform

Congress and the public that the NSL power is being used to seek information about library patrons at a time when congressional action on the USA PATRIOT Act is imminent. But it is clear from the ACLU's own press release, and numerous articles in the A-Section of major newspapers last week based upon that press release, that Plaintiffs have not been prevented from communicating such information here. See Exs. B (ACLU press release) ("The American Civil Liberties Union today disclosed that the FBI has used a controversial Patriot Act power to demand records from an organization that possesses 'a wide array of sensitive information about library patrons, including information about the reading materials borrowed by library patrons and about Internet usage by library patrons.' The FBI demand was disclosed in a new lawsuit filed in Connecticut, which remains under a heavy FBI gag order ...Congress is currently undertaking efforts to reauthorize the Patriot Act, with both the House and Senate having passed different versions of legislation before adjourning for the August recess. While the ACLU has not endorsed either bill, it has said the Senate bill takes steps in the right direction."), C (Washington Post article), Defendant (New York Times article). Contrary to Plaintiffs' assertion, and as discussed above, the 2709(c)'s non-disclosure provision is not preventing the ACLU from "speaking truthfully about how the FBI is using its NSL power." Pls.' Br. at 10. The redacted complaint permits Plaintiffs to inform Congress, libraries, and anyone else that the FBI is using the NSL power to seek information related to library patrons.

## **II. Plaintiffs Have Not Demonstrated a Clear Likelihood of Success on the Merits.**

Plaintiffs contend that 18 U.S.C. § 2709(c)'s non-disclosure provision is a prior restraint on speech, that it is subject to strict scrutiny, and that the provision is facially invalid under this standard. All three contentions are without merit.

A. The Government Validly May Require Non-Disclosure of Information Gained Through Participation in an Official Investigation.

The Supreme Court, the Second Circuit, and other courts of appeal have upheld non-disclosure restrictions like the one at issue here, reasoning that restrictions on information a party learns only by virtue of its participation in a confidential government investigation do not raise the same First Amendment concerns as other restrictions on speech. See Butterworth v. Smith, 494 U.S. 624 (1990), Seattle Times Co. v. Rhinehart, 467 U.S. 20, 27 (1984); Hoffman-Pugh v. Keenan, 338 F.3d 1136, 1139-40 (10<sup>th</sup> Cir. 2003); Kamasinski v. Judicial Review Council, 44 F.3d 106, 110-12 (2d Cir. 1994); In Re Subpoena to Testify Before Grand Jury Directed to Custodian of Records, 864 F.2d 1559, 1564 (11<sup>th</sup> Cir. 1989); First Am. Coalition v. Judicial Review Bd., 784 F.2d 467, 479 (3d Cir. 1986); see also Doe v. Ashcroft, 334 F. Supp.2d 471 (S.D.N.Y. 2004).

In Rhinehart, the plaintiff, a newspaper, asserted a First Amendment right in information it obtained through civil discovery and challenged a court order precluding release of that information. 467 U.S. at 32. The Supreme Court rejected the plaintiff's claim, holding that although plaintiff had a right to express information it knew before discovery, it had "no First Amendment right of access to information made available only for purposes of trying this suit." Id. at 32. Although the Court recognized that there was substantial public interest in the information the plaintiff wished to publish, the Court reasoned that the information was obtained through an official process "that both granted [plaintiff] access to that information and placed constraints on the way in which the information might be used." Id. The Court further concluded that the restraint on disclosure "[was] not a restriction on a traditionally public source

of information,” id. at 32, and reasoned that “continued court control” over information obtained in this manner did not “raise the same specter of government censorship that such control might suggest in other situations.” Id. at 33. Accordingly, the Supreme Court held that restrictions on the disclosure of information obtained only by virtue of such processes need only satisfy intermediate scrutiny, and must be upheld if “the ‘practice in question [furthers] an important or substantial government interest unrelated to the suppression of free expression’ and whether ‘the limitation of First Amendment freedoms [is] not greater than is necessary or essential to the protection of the particular government interest involved.’” Id. at 32 (brackets in original) (quoting Procunier v. Martinez, 416 U.S. 396, 413 (1974)). The Court concluded that the restriction met this standard. See id.

In Butterworth, the Supreme Court applied this same principle to information gained by virtue of being made a witness in a grand jury investigation. See 494 U.S. at 631-32. There the Court held that a Florida statute violated the First Amendment to the extent it precluded a grand jury witness from disclosing the specific facts underlying his testimony to the grand jury. See id. at 632. In distinguishing the facts before it from Rhinehart, the Court explained that “[h]ere, by contrast, we deal only with 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.” Id. The Court went on to uphold a permanent, categorical ban on the disclosure by grand jury witnesses of the testimony of other witnesses learned as a result of participation in the grand jury. See id. at 633. Justice Scalia, in a sole concurrence, amplified further on the principle behind these holdings, writing that: “I think there is considerable doubt whether a witness can be prohibited, even while

the grand jury is sitting, from making public what he knew before he entered the grand jury room. Quite a different question is presented, however, by a witness' disclosure of the grand jury proceedings, which is knowledge he acquires not "on his own" but only by virtue of being made a witness." Id. at 636 (Scalia, J., concurring).

The Second Circuit in Kamasinski applied these same principles to an investigatory body established by statute to examine complaints against judges. See 44 F.3d at 110-11. Relying on Butterworth, the Second Circuit upheld those portions of a Connecticut statute that prohibited a complainant from disclosing "the fact that a complaint was filed" with the investigative body (a commission), the "fact that testimony was given" by the complainant to the commission, and "any information that [the] individual learn[ed] by interaction with the [commission]." Id. Although the court applied strict scrutiny, it concluded that even under this heightened review the "ban on disclosure ... [did] not run afoul of the First Amendment" and was justified by the state's interest in the integrity and efficacy of its confidential investigative process. Id. at 111.

Other Circuits consistently have upheld similar non-disclosure requirements based on this principle. See Hoffman-Pugh, 338 F.3d at 1139-40 (upholding statute prohibiting disclosure of information learned through grand jury proceedings, including information sought by prosecution, "unless and until grand jury returned indictment" and reasoning that "Butterworth does not necessarily preclude a permanent disclosure prohibition ... where that prohibition is limited to the specific content of the witness' testimony before the grand jury as opposed to the witness' knowledge of events discussed in that testimony."); In Re Subpoena, 864 F2d. at 1562 (holding that (1) university which refused to comply with subpoena could be prohibited from disclosing information that would reveal direction of grand jury investigation, including

documents sought by subpoena or names of individuals under investigation, (2) order was justified because “secrecy was essential to maintaining the effectiveness of the grand jury” investigation; and (3) narrow tailoring was not required for non-disclosure order); First Amendment Coalition, 784 F.2d at 479 (upholding state statute to extent it prohibited disclosure of proceedings of investigative board unless and until formal charges filed).

Section 2709(c) is analogous to the grand jury and other investigatory non-disclosure provisions discussed above. Indeed, 18 U.S.C. § 2709 is intended explicitly to mirror grand jury subpoena powers in many key respects. See H. Rep. 107-236(I) at 61-62 (noting that amendments to 18 U.S.C. § 2709 in USA PATRIOT Act are meant to “harmonize[] this provision with existing criminal law where an Assistant United States Attorney may issue a grand jury subpoena for all such records in a criminal case.”). In Doe v. Ashcroft, the only case so far to address the constitutionality of NSLs, the district court concluded that “[t]he principle that *Rhinehart* and its progeny represent is directly applicable” to § 2709 because “[a]n 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.” 334 F. Supp.2d at 519; see also id. at 518 (holding that the “basic principle that emerges 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 than [sic] laws which prohibit disclosing information a person obtains independently. ... the Government has at least some power to control information which is its ‘own creation’”). Because 18 U.S.C. § 2709(c) restricts information obtained only by participation in a confidential investigation, it does not “raise the same specter of censorship” as other restrictions on content, and is permissible if it

“[furthers] an important or substantial government interest unrelated to the suppression of free expression” and “[is] not greater than is necessary or essential to the protection of the particular government interest involved.” Rhinehart 467 U.S. at 32; see also Doe, 334 F. Supp.2d at 519 (because statute prohibits disclosure of information gained only by virtue of confidential investigation “it presumptively does little violence to the First Amendment values to condition the issuance of an NSL upon the recipient’s return obligation of at least some secrecy.”). Note also that, although the Second Circuit in Kamasinski purported to apply strict scrutiny in upholding the non-disclosure provision before it, see 44 F.3d at 109, ultimately this Court need not decide which test applies: section 2709 easily satisfies either standard. As discussed below, it is no more restrictive than the non-disclosure provisions upheld in the cases above, and is justified by a far more compelling purpose.

1. The Government’s Interest in Confidentiality is Compelling.

Section 2709(c)’s confidentiality provision is justified by the government’s interest in national security, and in particular its interest in conducting effective investigations to disrupt the activities of terrorist organizations and foreign intelligence agencies. The Supreme Court has recognized that “few interests can be more compelling.” See Wayte v. United States, 470 U.S. 598, 611-12 (1985) (observing also that “[u]nless a society has the capability and the will to defend itself, from the aggression of others, constitutional protections of any sort have little meaning”); Department of the Navy v. Egan, 484 U.S. 518, 527 (1988) (“This Court has recognized the Government’s ‘compelling interest’ in withholding national security information from unauthorized persons in the course of executive business.”); see also Doe v. Ashcroft, 334 F. Supp.2d at 513 (“the Government’s interest in protecting the integrity and efficacy of

international terrorism and counterintelligence investigations is a compelling one.”); accord Snepp v. United States, 444 U.S. 507, 509 n.3 (1980) (*per curiam*) (“The Government has a compelling interest in protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service.”).

Congress repeatedly has recognized that secrecy is essential to the functioning of counterintelligence and counter-terrorism investigations, and § 2709(c) represents Congress’ considered determination that disclosures of information about such investigations, and in particular which specific entity has received an NSL, are inherently harmful to the government’s efforts. See H. Rep. 99-690(I) at 15, 18, reprinted in 1986 U.S.C.C.A.N. 5341, 5345 “the FBI could not effectively monitor and counter the clandestine activities of hostile espionage agents and terrorists if they had to be notified that the FBI sought their ... records for counterintelligence investigations ... [the] effective conduct of FBI counterintelligence activities requires such non-disclosure.”); cf. In Re Subpoena, 864 F.2d at 1562 (“it takes little imagination to recognize that there are some kinds of government operations that would be totally frustrated if conducted openly.” (quoting Press Enterpr. Co. v. Superior Ct., 478 U.S. 1, 8-9 (1986))). The FBI’s own experience in conducting such investigations likewise has lead it to the conclusion that such disclosures are inherently harmful. See Szady Decl. ¶¶ 9-10. Specifically, disclosure of this type of information would identify the targets of foreign intelligence and counter-terrorism investigations, would “inform terrorists of both the substantive and geographic focus of the investigation[,] ... would inform terrorists which of their members were compromised by the investigation and which were not[,] ... could allow terrorists to better evade the ongoing

investigation and more easily formulate or revise counter-efforts, ... [and] could be of great use to al Qaeda in plotting future terrorist attacks or intimidating witnesses in the present investigation.” Center for Nat’l Sec. Studies v. United States Dep’t of Justice, 331 F.3d 918, 928-29 (D.C. Cir. 2003).

In short, the Legislature, in fashioning tools for the pursuit of counterintelligence and counter-terrorism investigations, and the Executive, in applying these tools, have recognized that secrecy is essential to the functioning of such efforts. The judgment of these two branches of government, which have the most relevant expertise in this area and are charged with ensuring the nation’s security, cannot lightly be disturbed by this Court. See CIA v. Sims, 471 U.S. 159, 180 (1985) (“It is the responsibility of the Director of Central Intelligence not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency’s intelligence-gathering process”); Center for Nat’l Sec. Studies, 331 F.3d at 928 (“[i]t is abundantly clear that the government’s top counterterrorism officials are well-suited to make [the] predictive judgment” about how disclosure of information will harm national security and that, “[c]onversely, the judiciary is in an extremely poor position to second-guess the executive’s judgment in this area of national security”); North Jersey Media Group v. Ashcroft, 308 F.3d 198, 219 (3d Cir. 2002) (“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 disclosure”); see also United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir. 1989) (“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."); Doe v. Ashcroft, 334 F. Supp.2d at 523 ("judges do not have national security experience. 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").

2. 18 U.S.C. § 2709(c) is Appropriately Tailored to the Need for Secrecy in Counterintelligence and Counter-Terrorism Investigations.

Section 2709(c) is adequately tailored to the government's compelling interest in confidentiality. As an initial matter, in accordance with Rhinehart, Kamasinski, and the other cases discussed above, § 2709(c) is narrow in scope, and limited to information gained only by virtue of participation in a confidential investigation. See Rhinehart, 467 U.S. at 32; Kamasinski, 44 F.3d at 110-11; Hoffman-Pugh, 338 F.3d at 1139-40; In Re Subpoena, 864 F.2d. at 1562; see also Doe, 334 F. Supp.2d at 519 (recognizing that § 2709(c) is consistent with limitations found in these cases). Contrary to Plaintiffs' hyperbolic assertion, see Pls.' Br. at 8-10, the non-disclosure provision does not prevent Plaintiffs from "disclos[ing] the threat that NSLs pose to intellectual freedom" or "discuss[ing] that threat with other libraries, library associations, and the public" or taking these issues "to Congress." Id. Instead, it prohibits only "*the mere fact*," Pls.' Br. At 2 (italics in original), that the FBI has sought records from Library Connection in particular – a fact Plaintiffs became aware of only through participation in a confidential investigation. As the Doe v. Ashcroft court observed: "Anything outside this bare fact may be fair game. ... 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 provided to

the FBI,” so long as he did not disclose that he had provided that information to the agency. 334 F. Supp.2d at 514.

Most importantly to Plaintiffs, as the ACLU’s own press release and A-Section articles in major newspapers demonstrate, Plaintiffs are free to communicate to Congress and the public the fact that the NSL power has been used to request information pertaining to library patrons, so long as they do not reveal the one fact critical to the FBI’s investigation – that the FBI has sought this information from Plaintiff Library Connection in particular. See Exs.B, C, D; see also Redacted Compl. (attached to this memorandum as Ex. E).

Nor is § 2709(c) over broad because it permanently prohibits disclosure of this information. See Pls.’ Br. at 14. As discussed above, counterintelligence and counter-terrorism investigations differ fundamentally from normal criminal investigations, and this difference affects the duration of secrecy necessary. See Szady Decl. ¶¶11, 31, 33; see also H.R. Conf. Rep. 104-427, at 35-36, 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.”). In criminal investigations, evidence about past acts is collected and then used for indictment and prosecution, at which point any need for secrecy in connection with the gathering of this evidence may be greatly diminished. By contrast, the goal of counterintelligence and counter-terrorism investigations is forward-looking: to unravel the members and activities of terrorist and foreign intelligence organizations, and to disrupt their activities on a continuing basis. See Szady Decl. ¶¶8-10, 32. As the Doe v. Ashcroft court explained:

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 ... Also, the Government often decides to pursue the fruits of international terrorism or counterintelligence investigation via interdiction or diplomacy, as opposed to through formal and public criminal processes. 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.

334 F. Supp.2d at 522 (emphasis in original). Information used against one target may be used against additional targets in the future, see id. ¶¶9-11, 31, 33 and in order for that intelligence to remain useful against future targets, that information, and the means by which the FBI acquired it, must remain secret. See id. ¶¶11, 33. In particular, terrorists alerted to where the FBI is obtaining its information will relocate their operatives and activities, use alternative methods of communication, spread disinformation, or take other steps to frustrate scrutiny. See id. Furthermore, often the usefulness of collected information is not immediately known, and becomes apparent only as additional information is acquired. See id.; see also Doe, 334 F. Supp.2d at 523 (“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.”). For this reason, there is a need to preserve the secrecy of intelligence acquired in counter-terrorism investigations even where the importance of such information is not immediately apparent. See id. More generally, there is a long-range interest in keeping requests for information and other aspects of

investigations secret in order to prevent terrorist groups and foreign intelligence organizations from discerning patterns or favored sources and methods of FBI counterintelligence and counter-terrorism investigations. See id. ¶¶12-13. In short, in counterintelligence and counter-terrorism investigations, there is no natural “end-point” where collected information ceases to be useful and the need for secrecy disappears.

The Supreme Court, acknowledging these realities, has recognized that counterintelligence and counter-terrorism investigations simply do not lend themselves to the same standard of narrow tailoring appropriate to criminal investigations. As the Court observed in United States v. United States District Court, 407 U.S. 297 (1972):

We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of ‘ordinary crime.’ The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government’s preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

Id. at 322. This principle likewise has guided congressional legislation providing tools for counterintelligence and counter-terrorism investigations. As Congress has observed:

Far more than in domestic security matters, foreign counterintelligence investigations are “long range” and involve “the interrelation of various sources and types of information.” Targets are often “difficult to identify,” and the emphasis is primarily “on the prevention of unlawful activity.” When foreign governments and foreign-based organizations are the source of danger, the Government clearly must prepare for a possible future crises or emergency. When clandestine intelligence and terrorist activities are planned, directed and supported from abroad, rather than within the United States, the investigative task is extraordinarily difficult. Therefore, the focus of surveillance of suspected foreign agents must “be less precise” if the United States is to maintain adequate security.

S. Rep. No. 95-604 at 16, reprinted at 1978 U.S.C.C.A.N. 3985 (quoting United States v. District Court, 407 U.S. at 322). In short, there is no appropriate basis here for the Court to overturn the considered judgment of the legislative and executive branches in this instance that the need for secrecy in connection with such information is ongoing, and to impose some finite end-date for secrecy chosen by the Court.

Plaintiffs' opposition to the duration of § 2709(c)'s non-disclosure provision, see Pls.' Br. at 14, appears to be premised entirely on the district court's holding in Doe v. Ashcroft. There, as noted above, the district court held that the government's interest in the effective functioning of counterintelligence and counter-terrorism investigations was "compelling" and agreed with the government that "Rhinehart and its progeny" were "directly applicable" to § 2709 and that the "basic principle of 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 scrutiny [than] laws which prohibit disclosing information a person learns independently." 334 F. Supp.2d at 518-19. Nevertheless, the court held § 2709(c) unconstitutional because it concluded that a permanent restriction on disclosure was not adequately tailored to the government's interest in protecting counterintelligence and counter-terrorism investigations. See id. at 519.

In reaching this holding, however, the district court demonstrated a fundamental misunderstanding of the government interests at stake, and ignored relevant Supreme Court precedent. Despite recognizing elsewhere in its opinion that counterintelligence and counter-terrorism investigations differ fundamentally from normal criminal investigations, see id. at 522, the Doe court applied a grand jury-like model to these investigations, presuming that they lead

directly to, and end in, prosecutions or some other form of discrete final action, with a resulting end to the need for secrecy. See id. at 519 (citing Kamasinski, 44 F.3d at 112, for the proposition that “secrecy rules are only consistent with the First Amendment during the investigatory phase of a judicial ethics proceeding”); 521 (“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 material presumably has been put to its intended purposes.”). This ignores the Supreme Court’s holding that counterintelligence and counter-terrorism investigations do not have convenient end-points and thus are subject to a different standard of tailoring than criminal investigations, see District Court, 407 U.S. at 322, and for this reason alone the district court’s reasoning is not persuasive.

Furthermore, the Doe court also ignored the fact that the Supreme Court itself has upheld a similar, permanent ban on disclosure even in the less compelling, criminal context of grand jury proceedings. See Butterworth, 494 U.S. at 633 (upholding permanent ban on disclosure of the testimony of other grand jury witnesses based on concern that such disclosures might lead to retribution against those witnesses); see also Hoffman-Pugh, 338 F.3d at 1139-40 (upholding ban on disclosure of information learned through grand jury proceedings “unless and until grand jury returned indictment”). It is incongruous to hold, as the Doe court did, that permanent secrecy can be had in these cases but not in the highly unusual circumstances of counterintelligence and counter-terrorism investigations, where the need for ongoing secrecy is far stronger and better supported.

In short, because § 2709(c) comports with the approach of Congress, the Executive and the Supreme Court to counterintelligence and counter-terrorism investigations, and is no more

restrictive and better justified than the permanent ban on disclosure upheld by the Supreme Court in Butterworth, it must be deemed appropriately tailored and upheld by this Court.

B. 2709(c) Is Not a Prior Restraint.

Contrary to Plaintiff's assertion, see Pls.' Br. at 11, section 2709(c) is not a prior restraint. The Supreme Court has recognized two types of prior restraint. The first takes the form of a licensing scheme for speech, where the plaintiff's right to speak is conditioned on a license or other prior approval from the government. See City of Lakewood Plain Dealer Publishing Co., 486 U.S. 750, 757 (1988). By contrast, statutes that categorically prohibit speech and impose punishments for disclosure only after the fact are not prior restraints. See id. at 764 (distinguishing between statute imposing prohibition on speech and statute conditioning speech on obtaining a license or permit from official). "The doctrine of prior restraint originated in the common law of England, where prior restraints of the press were not permitted, but punishment after publication was." Alexander v. United States, 509 U.S. 544, 553 (1993). It "has its roots in the 16th- and 17th-century system of censorship" under which "nothing could be lawfully published without the prior approval of a government or church." Id. at 554 n.2.

Here, section 2709(c) categorically prohibits recipients of NSLs from disclosing that they have received them; it does not grant the government any discretion to decide whether this information can be made public. Plaintiffs' argument that categorical restrictions on disclosures like 18 U.S.C. § 2709(c) qualify as prior restraints is wholly undermined by Landmark Comm. v. Virginia, 435 U.S. 829 (1978), on which they rely. There, a Virginia statute categorically prohibited the disclosure of information about the proceedings of judicial investigative body and imposed criminal penalties for violation. See id. at 830. The Supreme Court explained that such

a non-disclosure provision “does not constitute a prior restraint or attempt by the State to censor the news media.” *Id.* at 838 (adopting reasoning of Virginia Supreme Court on this point, *see Landmark Comm. v. Virginia*, 217 Va. 699, 704 (Va. 1977)). In short, a categorical statutory prohibition on disclosures enforceable only by a penalty action after the fact is not a prior restraint. Were that not so, countless state and federal statutes, including every anti-espionage statute that prohibits the disclosure of classified information, would be a prior restraint. *See, e.g.*, 18 U.S.C. §§ 793-794. The district court’s holding in *Doe v. Ashcroft* does not change the answer to this question. *See* 334 F. Supp.2d at 511-12 (concluding that 18 U.S.C. § 2709(c) acted as prior restraint on speech). The court in that case misapplied a single footnote, taken out of context, from an unrelated Supreme Court case on time, place and manner restrictions. *See id.* (citing *Ward v. Rock Against Racism*, 491 U.S. 781, 795 n.5 (1989)). Notably, the Supreme Court in *Ward* upheld the regulation on speech before it (allowing city to regulate the volume of amplified music) and explicitly concluded that it did not constitute a prior restraint. *See* 491 U.S. at 795 n.5. The *Doe* court did not consider *Landmark Communications* or any other case dealing with statutory prohibitions on disclosure like the one at issue here, and again its decision on this point accordingly carries little weight. *See id.*

The second category of prior restraints takes the form of court injunctions against certain speech or speakers. *See Alexander v. United States*, 509 U.S. 544, 550 (1993). Here, this Court has not imposed, and Defendants have not sought, a court order prohibiting Plaintiffs from making the disclosures prohibited by 18 U.S.C. § 2709(c). Even if Defendants had, however, the Supreme Court has recognized that court orders prohibiting information acquired only by virtue of participation in an official investigation do not raise the same concerns as other injunctions on

speech and do not represent prior restraints. See Rhinehart, 467 U.S. at 33 (court order restricting disclosure of information obtained only by virtue of participation in civil discovery was “not the kind of classic prior restraint that requires exacting First Amendment scrutiny”); In Re Subpoena, 864 F.2d at 1562 (upholding court order restricting disclosure of activities of grand jury and concluding that “[t]his is not a case of prior restraint of protected First Amendment activity”). In short, no prior restraint is presented by 18 U.S.C. § 2709(c).

C. 18 U.S.C. § 2709(c) is Valid As Applied in This Case

In addition to their facial attack on the validity of 18 U.S.C. § 2709(c), Plaintiffs cavalierly assert that, under the circumstances of this particular case, public disclosure of Library Connection as the recipient of an NSL “cannot possibly jeopardize national security or any ongoing investigation.” Pls.’ Br. at 2-3. Of course, Plaintiffs lack either the specific knowledge or the institutional competence to make such a statement, and their bare assertion that no harm will come from disclosing Library Connection as the recipient of the NSL is worthless. It is also easily refuted. By publicly disclosing that Library Connection has received an NSL, the target of the NSL – the user at IP address 216.47.180.118, who logged in at 4-4:45 PM on February 15, 2005 – will be alerted that the FBI is seeking information from his Internet provider as part of a counter-terrorism investigation. Library Connection may well have many users at the 26 libraries it serves – but only a very few are likely to be engaged in activities relevant to a counter-terrorism investigation. For these users, this information provides strong reason to believe that their particular activities may now be under investigation, and a red flag to move to another provider, begin disseminating disinformation, or take other measures to evade detection. See Szady Decl. ¶¶9-11, 29. As Assistant Director Szady makes clear, such information is more than

enough to cause serious damage to the FBI's investigation here and to its ability generally to conduct similar investigations in the future.<sup>3</sup> See *id.* ¶¶20-22, 25-26, 29.

**III. The Balance of Hardships Tips Strongly in Favor of the Government and the Public, Which will be Harmed Seriously and Irreparably by Issuance of a Mandatory, Preliminary Injunction.**

As discussed in detail above, the harm to the government from disclosing Library Connection as the recipient of the NSL is serious, immediate, and irreparable. Identifying Library Connection as the recipient of the NSL would immediately alert the target of the FBI's counter-terrorism investigation, and anyone working with him, that their actions are potentially compromised, inducing them to hide, flee, provide misinformation, or otherwise frustrate the FBI's investigation into their actions. See Szady Decl. ¶¶9-11, 20-22, 29. It would alert other terrorist and foreign intelligence actors to avoid this provider in the future. See *id.* ¶¶9-10, 20. And it would provide useful information to such groups on the geographic focus and methodology of the FBI's counter-terrorism investigations generally. See *id.* ¶¶12-13. As the *Doe* court recognized, any preliminary relief from § 2709(c) "may carry the potential to compromise legitimately confidential information," 334 F. Supp.2d at 526. Declaring

---

<sup>3</sup>Although Plaintiffs here challenge only the impact of disclosing Library Connection's name on any investigation, and not the underlying validity of the investigation itself, the government stands ready to provide the Court with the substance of the FBI's investigation. Because this material is classified, it must be presented to the Court *ex parte* and *in camera*, according to procedures set forth at 28 C.F.R. § 17.17(a); see *Jifry v. FAA*, 370 F.3d 1174, 1182 (D.C. Cir. 2004) (discussing courts' general authority to conduct *ex parte*, *in camera* review of classified materials). To date, Defendants have not presented this material because of the short briefing schedule demanded by Plaintiffs, which did not leave time to make the necessary arrangements, and because the specific issues raised by Plaintiffs did not appear to require it. In the event that the Court wishes to see it, Defendants will make the necessary arrangements.

“unequivocally” that “it is not its intention to cause any such information to fall into the wrong hands,” the court therefore stayed any enforcement of its judgment against the government until the Second Circuit had an opportunity to review its decision. Id. The government’s prediction of harm is one that this Court is obligated to treat with the utmost seriousness. See Sims, 471 U.S. at 180; Center for Nat’l Sec. Studies, 331 F.3d at 928; North Jersey Media Group, 308 F.3d at 219. Finally, because the FBI’s counter-terrorism investigation is conducted to preserve the public from harm, the injury to the FBI represents an injury to the public as well. Taken together, these harms outweigh any temporary burden on Plaintiffs from this restriction while the issue is litigated.

\* \* \*

In sum, Plaintiffs have not met their burden of proof in connection with the relief they seek. Plaintiffs have failed to establish real harms that are imminent and irreparable, as they must, and for this reason alone their motion fails. See Moore, 409 F.3d at 510 (irreparable harm is required element for preliminary injunction). Moreover, Plaintiffs have not demonstrated the “clear likelihood of success” needed to justify the extraordinary mandatory injunction they seek here. Beal, 184 F.3d at 122-23. Indeed, even if the authorities cited by the government did not already compel a decision in the government’s favor on the merits of the non-disclosure provision, it still would be inappropriate to grant a mandatory preliminary injunction here because, as the Doe court recognized, the Court is dealing in “uncharted legal terrain.” Doe, 334 F. Supp.2d at 526. As such, Plaintiffs’ entitlement to victory on the merits cannot be deemed “clear,” as it must to justify such relief, Beal, 184 F.3d at 122-23. Finally, Plaintiffs likewise are not entitled to a mandatory, preliminary injunction because the balance of hardships tips strongly

in favor of the government and the public. As demonstrated above, the irreparable harm Plaintiffs's claim does not exist: the non-disclosure provision has not prevented Plaintiffs from informing Congress that NSLs are being used to seek information about the internet usage of library patrons. By contrast, the government's harm is serious and undeniably irreparable.<sup>4</sup> See Punnet, 621 F.2d at 587-88 (where plaintiff demands mandatory injunctive relief, court must weigh harms to other parties, in particular risk of irreparable harm to parties apart from plaintiff). Plaintiffs have not alleged any special benefit from an immediate right to tell Congress and the world which particular library received an NSL, and they certainly have not provided any rationale that would override the FBI's compelling interest in preserving the confidentiality and efficacy of its counter-terrorism investigation in the short term while this issue is litigated and resolved, either by this Court or by the Second Circuit's decision in Ashcroft v. Doe.<sup>5</sup> In short, Plaintiffs have not demonstrated their entitlement to a mandatory injunction here.

#### **IV. The Court Should Stay Any Grant of Injunctive Relief.**

In the event that the Court does decide to grant Plaintiffs the mandatory injunctive relief they seek, it should stay any enforcement of that decision until the government has been given a

---

<sup>4</sup> Moreover, the purpose of a preliminary injunction is to preserve the Court's ability to provide full relief to the parties. See In Re Microsoft, 333 F.3d at 526 (holding that preliminary injunction must be denied where unnecessary to achieve this purpose). Here, the relief Plaintiffs seek is not necessary to preserve the ability of the Court to render a final judgment on the merits, and on the contrary impairs the Court's ability to grant final relief to the parties by taking away from the government something that cannot be returned.

<sup>5</sup>Indeed, by rushing unnecessarily to force an irreversible disclosure of the recipient of the NSL at issue here, this Court risks a decision on the merits of this issue inconsistent with the Second Circuit's ultimate holding.

reasonable opportunity to appeal. Such an order would be appropriate given “the implications of [such a] ruling and the importance of the issues involved.” Doe v. Ashcroft, 334 F. Supp.2d at 526 (staying enforcement of judgment finding 18 U.S.C. § 2709 unconstitutional for 90 days to allow appeal).

**CONCLUSION**

For all of the reasons above, Plaintiff’s Motion for Preliminary Injunction should be denied.

Respectfully submitted,

PETER D. KEISLER  
Assistant Attorney General

KEVIN J. O’CONNOR  
United States Attorney

LISA E. PERKINS  
Assistant United States Attorney  
450 Main Street  
Hartford, Connecticut 06103  
(860) 947-1101  
FEDERAL BAR NO. ct23164  
[lisa.perkins@usdoj.gov](mailto:lisa.perkins@usdoj.gov)

SANDRA M. SCHRAIBMAN  
Assistant Director, Federal Programs Branch



CARLTON E. GREENE  
Trial Attorney  
Civil Division, Federal Programs Branch  
United States Department of Justice  
Room 7308  
20 Massachusetts Avenue, NW  
Washington, DC 20530  
Tel. (202) 514-4938; Fax. (202) 616-8470  
FEDERAL BAR NO. va41497

August 29, 2005

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that a copy of the within and foregoing, has been sent to the following this 29th day of August, 2005:

Ann Beeson, Esq. (Via secure protected electronic mail)  
Jameel Jaffer, Esq.  
Melissa Goodman, Esq.  
American Civil Liberties Union Foundation  
125 Broad Street, 17th Floor  
New York, NY 10004

Annette M. Lamoreaux, Esq. (Via hand delivery)  
ACLU of Connecticut Foundation  
32 Grand Street  
Hartford, CT 06106



---

LISA E. PERKINS  
ASSISTANT UNITED STATES ATTORNEY