2005 WL 6237672 (C.A.2) (Appellate Brief)
United States Court of Appeals, Second Circuit.

John DOE, American Civil Liberties Union, and American Civil Liberties Union Foundation, Plaintiffs-Appellees,
v.
Alberto GONZALES, in his official capacity as Attorney General of the United States Robert S. Mueller III, in his official capacity as Director of the Federal Bureau of and John Roe, Federal Bureau of Investigation, Defendants-Appellants.

No. 05-4896-CV.
October 3, 2005.

On Appeal from the United States District Court for the District of Connecticut

Brief for the Defendants-Appellants

Kevin J. O'Connor, United States Attorney, William Collier, Lisa E. Perkins, Assistant United States Attorney, 450 Main Street, Hartford, CT 06103, 860-947-1101.

Robert D. McCallum, Jr., Acting Deputy Attorney General, Peter D. Keisler, Assistant Attorney General, Gregory G. Katsas, Deputy Assistant Attorney General, Douglas N. Letter, Scott R. McIntosh, Attorneys, Appellate Staff, Civil Division, Room 7259, Department of Justice, 950 Pennsylvania Avenue, N.W., Washington, D.C. 20530-0001, 202-514-4052.

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

PRELIMINARY STATEMENT 1

STATEMENT OF JURISDICTION 2

STATEMENT OF THE ISSUES 2

STATEMENT OF THE CASE 2

STATEMENT OF FACTS 4

I. Statutory Background 4

A. 18 U.S.C. § 2709 and National Security Letters 4

B. 18 U.S.C. § 2709(c) and the Need for Non-Disclosure of NSLs 6

II. The Present Controversy 9

SUMMARY OF ARGUMENT 14

STANDARD OF REVIEW 16

ARGUMENT 17

THE PRELIMINARY INJUNCTION AGAINST THE ENFORCEMENT OF SECTION 2709(c) IN THIS CASE SHOULD BE REVERSED 17

I. The Recipient of a National Security Letter Has No Constitutional Right To Disclose His Identity During an Ongoing Counter-Terrorism Investigation 17

A. This Court and Other Courts Have Sustained the Constitutionality of Non-Disclosure Requirements Like Section 2709(c) 17

B. The District Court's Objections to the Application of Section 2709(c) in this Case Are Without Merit 30

II. The Balance of Harms Weighs Strongly Against Allowing the Plaintiffs to Publicly Disclose the NSL Recipient's Identity 42

A. Prohibiting Disclosure of Doe's Identity Does Not Materially Impair the Plaintiffs' Asserted First Amendment Interests 42

B. Disclosure Will Irreparably Harm the Government and the Public Interest 44

CONCLUSION 50

CERTIFICATE OF COMPLIANCE

CERTIFICATE OF SERVICE

Note: Table of Contents page numbers missing in original document

TABLE OF AUTHORITIES

Cases

Afshar v. Department of State, 702 F.2d 1125 (D.C. Cir. 1981) 46

Beal v. Stern, 184 F.3d 117 (2d Cir. 1999) 17, 42, 45

Butterworth v. Smith, 494 U.S. 624 (1990) 24, 25

CIA v. Sims, 471 U.S. 159 (1985) 34

Center for National Security Studies v. Department of Justice, 331 F.3d 918 (D.C. Cir. 2003) 34

City of Lakewood v. Plain Dealer Publishing Co., 486 U.S. 750 (1988) 38, 39

Department of the Navy v. Egan, 484 U.S. 518 (1988) 25

 © 2017 Thomson Reuters. No claim to original U.S. Government Works.

Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), *appeal pending sub nom. Doe v. Gonzales,* No. 05-0570	1, 26, 35
Doe v. Gonzales, No. 05-0570 (2d Cir.)	10, 13
First Amendment Coalition v. Judicial Inquiry and Review Board, 784 F.3d 467 (3d Cir. 1986)	22, 23
Fitzgibbon v. CIA, 911 F.2d 755 (D.C. Cir.1990)	47
Freedom Holdings, Inc v. Spitzer, 408 F.3d 112 (2d Cir. 2005)	17
Frugone v. CIA, 169 F.3d 772 (D.C. Cir. 1999)	47
Halkin v. Helms, 598 F.2d 1 (D.C. Cir. 1978)	37
Halperin v. CIA, 629 F.2d 144 (D.C. Cir. 1980)	37
Harman v. City of New York, 140 F.3d 111 (2d Cr. 1998)	39
Hoffman-Pugh v. Keenan, 338 F.3d 1136 (10th Cir. 2003)	22, 23
Kamasinksi v. Judicial Review Council, 44 F.3d 106 (2d Cir. 1994)	14, 20, 21, 26, 32, 33, 41
Landmark Communications, Inc. v. Virginia, 435 U.S. 829 (1978)	39
Near v. Minnesota ex rel. Olson, 283 U.S. 697 (1931)	39
North Jersey Media Group v. Ashcroft, 308 F.3d 198 (3d Cir. 2002)	35
Public Citizen v. Department of State, 11 F.3d 198 (D.C. Cir. 1993)	46
Register.com, Inc. v. Verio, Inc., 356 F.3d 393 (2d Cir. 2004)..	16
Salisbury v. United States, 690 F.2d 966 (D.C. Cir. 1982)	47
Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984)	23, 24, 40, 41
Snepp v. United States, 444 U.S. 507 (1980)	25
In re Subpoena to Testify before Grand Jury Directed to Custodian of Records, 864 F.2d 1559 (11th Cir. 1989)	22
United States v. United States District Court, 407 U.S. 297 (1972)	27
United States v. Yunis, 867 F.2d 617 (D.C. Cir. 1989)	35

WESTLAW © 2017 Thomson Reuters. No claim to original U.S. Government Works.

Statutes

12 U.S.C. §§ 3414(a)(1) 5, 8

12 U.S.C. § 3414(a)(5) 7

12 U.S.C. § 3414(a)(1) 7

15 U.S.C. §1681u 7

15 U.S.C. §§ 1681u, 1681v 5

15 U.S.C. § 1681v 7

18 U.S.C. § 2709 .... passim

18 U.S.C. § 2709(a) 5

18 U.S.C. § 2709(b) 5

18 U.S.C. § 2709(c) .... passim

28 U.S.C. § 1292(a)(1) 2

28 U.S.C. § 1331 2

50 U.S.C. § 436 .... 5, 7

50 U.S.C. § 1802(a)(4)(A) 8

50 U.S.C. § 1822(a)(4)(A) 8

50 U.S.C. § 1842(d)(2)(B) 8

50 U.S.C. § 1861(d)(2) 8

Pub. L. No. 103-142, 107 Stat. 1491 (1993) 6

Pub. L. No. 104-293, 110 Stat. 3461 (1996) 6

Pub. L. No. 107-56, 115 Stat. 272 (2001) 6

Conn. Gen. Stat. § 51-511 20

Other Materials

Exec. Order No. 12333, 46 Fed. Reg 59941 (Dec. 4, 1981) 4

H. Rep. 99-690(I) (1986) 8

S. Rep. 5-604(I) (1997) 8

WESTLAW © 2017 Thomson Reuters. No claim to original U.S. Government Works.

S. Rep. No. 95-604 (1978) 27, 28

S. Rep. No. 99-541 (1986) 5, 6

H.R. 3199, 109th Cong., 1st Sess 6

PRELIMINARY STATEMENT

This is an appeal from a preliminary injunction issued by the District Court for the District of Connecticut (Hall, J.), on September 9, 2005. The preliminary injunction is set forth in the district court's Ruling on Plaintiffs' Motion for Preliminary Injunction, which is reported at 334 F. Supp. 2d 471.

STATEMENT OF JURISDICTION

The claims in this case arise under 18 U.S.C. § 2709 and the United States Constitution. The district court was vested with jurisdiction by 28 U.S.C. § 1331. The district court issued its preliminary injunction on September 9, 2005. The defendants-appellants filed a notice of appeal on September 16, 2005. This Court has appellate jurisdiction under 28 U.S.C. § 1292(a)(1).

STATEMENT OF ISSUES

1 18 U.S.C. § 2709(c) prohibits the recipient of a National Security Letter (NSL) sent by the Federal Bureau of Investigation as part of a counter-terrorism or counterintelligence investigation from disclosing that the government has sought or received information pursuant to Section 2709. The questions presented are:

1. Whether Section 2709(c) may constitutionally be applied to prevent the plaintiffs' public disclosure of the identity of the NSL recipient in this case.

2. Whether the injuries to the government and the public interest from an NSL recipient's disclosure of its identity during the course of an ongoing counterterrorism investigation outweigh the claimed injury to the plaintiffs' interests in being able to disclose the recipient's identity.

STATEMENT OF THE CASE

This case arises out of an ongoing counter-terrorism investigation being conducted by the Federal Bureau of Investigation. As part of that investigation, the FBI has served an electronic communication service provider with a National Security Letter (NSL) under 18 U.S.C. § 2709. The NSL directs the provider to give the FBI specific information that is within the scope of Section 2709 and that has been certified by the FBI to be relevant to its investigation.

In order to maintain the secrecy needed for effective counter-terrorism and counterintelligence investigations, Congress enacted Section 2709(c), which prohibits recipients of NSLs from disclosing that information has been sought or obtained by the FBI under Section 2709. Notwithstanding that prohibition, the provider in this case wishes to make its identity public, thereby providing public notice to the person or persons who are the targets of the NSL that the government may be conducting an investigation of their activities.

Instead of complying with the NSL, the recipient and the ACLU brought suit to challenge the constitutionality of Section 2709, including the non-disclosure requirement in Section 2709(c). On September 9, 2005, the District Court for the District of Connecticut issued a preliminary injunction enjoining the government from enforcing the non-disclosure requirement against the plaintiffs with respect to their public disclosure of the recipient's identity. The government is appealing that decision, and this Court has granted a stay pending appeal to preserve the status quo and prevent the plaintiffs from mooting

the appeal.

STATEMENT OF FACTS

I. Statutory Background

A. 18 U.S.C. § 2709 and National Security Letters

The President of the United States has charged the FBI with primary authority for conducting counterintelligence and counter-terrorism investigations in the United States. See Exec. Order No. 12333 §§ 1.14(a), 3.4(a), 46 Fed. Reg 59941 (Dec. 4, 1981). The President has also charged the FBI with conducting counterintelligence activities outside the United States in coordination with the CIA. See *id.* § 1.14(b). Today, the FBI is engaged in extensive investigations within the United States and around the world into threats, conspiracies, and attempts to perpetrate terrorist acts and foreign intelligence operations against the United States and its interests abroad. A-90-91.

The FBI's experience with counterintelligence and counter-terrorism investigations has shown that electronic communications play a vital role in advancing terrorist and foreign intelligence activities and operations. A-94. Accordingly, pursuing and disrupting terrorist plots and foreign intelligence operations often requires the FBI to seek information relating to the electronic communications of particular individuals.

The statutory provision at issue in this case, 18 U.S.C. § 2709, was enacted by Congress in 1986 to assist the FBI in obtaining such information. Section 2709 empowers the FBI to issue a type of administrative subpoena commonly referred to as a National Security Letter or "NSL." Section 2709 is one of several federal statutes that authorize the FBI or other government authorities to issue NSLs in connection with foreign counterintelligence and counter-terrorism investigations. See 12 U.S.C. §§ 3414(a)(1), 3414(a)(5); 15 U.S.C. §§ 1681u, 1681v; 50 U.S.C. § 436.

Subsections (a) and (b) of Section 2709 authorize the FBI to request "subscriber information" and "toll billing records information," or "electronic communication transactional records," from wire or electronic communication service providers. Subsection (a) directs providers to comply with such requests. While Section 2709 authorizes the FBI to seek subscriber and transactional information, it does not provide the FBI with authority to seek the *content* of any wire or electronic communication. See S. Rep. No. 99-541 at 44 (1986), *reprinted in* 1986 USCCAN 3598.

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 * * *." *Id.* § 2709(b)(1)-(2). In addition, when an NSL is issued in connection with an investigation of a "United States person," the same officials must certify that the investigation is "not conducted solely on the basis of activities protected by the first amendment * * * ." *Id.*

Section 2709 was enacted by Congress as part of Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"). Congress has amended Section 2709 on several occasions since then. See Pub. L. No. 103-142, § 1, 107 Stat. 1491, 1491 (1993); Pub. L. No. 104-293, § 601(a), 110 Stat. 3461, 3469 (1996); Pub. L.No. 107-56, § 505, 115 Stat. 272, 365 (2001). In general terms, the amendments have liberalized the standards for the issuance of NSLs, while leaving the basic structure of the statute undisturbed. Congress is presently considering additional changes to Section 2709, which may become law in the near future. See H.R. 3199, 109th Cong., 1st Sess. (passed by House of Representatives, July 21,2005); H.R. 3199, 109th Cong., 1st Sess. (passed by Senate, July 29, 2005).

B. 18 U.S.C. § 2709(c) and the Need for Non-Disclosure of NSLs

To maintain the secrecy and effectiveness of counterintelligence and counter-terrorism investigations, subsection (c) of Section 2709 subjects NSL recipients to a non-disclosure requirement. Subsection (c) provides that "[n]o 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."

Each of the other statutes allowing issuance of NSLs includes a non-disclosure provision similar to Section 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. § 1681 u (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 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 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.

II. The Present Controversy

This case grows out of an authorized FBI counter-terrorism investigation, the background of which is described in a classified ex parte declaration submitted to the district court.[1] Pursuant to that investigation, an FBI Special Agent delivered an NSL issued under Section 2709 to an electronic communication service provider that has been identified in this litigation as John Doe. A-24. Doe is a [ ] that provides [ ] with a variety of services, including [ ]. A-9, A-16-17.

The NSL directed Doe to provide the FBI with "any and all subscriber information, billing information and access logs of any person or entity" [ ]. A-24. As required by Section 2709, the FBI certified in the NSL that the information sought was relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities. *Id.* The basis for that certification is explained in the FBI's ex parte declaration. The NSL informed Doe that Section 2709(c) prohibited it and its officers, agents, and employees from "disclosing to any person that the FBI has sought or obtained access to information or records under these provisions." *Id.*

Doe did not comply with the NSL. Instead, Doe, the American Civil Liberties Union, and the American Civil Liberties Union Foundation filed suit to enjoin the government from enforcing Section 2709 in this or any other case. The plaintiffs contend that Section 2709 is facially unconstitutional under the First, Fourth, and Fifth Amendments. The plaintiffs further contend that the non-disclosure requirement in Section 2709(c) violates the First Amendment. The plaintiffs' constitutional claims are similar to those now before this Court in *Doe v. Gonzales,* No. 05-0570.

After initially filing their complaint under seal, the plaintiffs prepared a redacted version of the complaint, in consultation with the government, for public release. The redactions were intended to allow the plaintiffs to make public as much information about the litigation as possible without disclosing Doe's identity or the target of the NSL itself. Among other things, the redacted complaint discloses to the public that Doe is "a member of the American Library Association" and

 © 2017 Thomson Reuters. No claim to original U.S. Government Works.

"believes that it should not be forced to disclose" any of "its library and Internet records." A-26-35. Immediately following the release of the redacted complaint, the ACLU issued a press release reiterating that the NSL seeks information from an organization with library records. See<www.aclu.org/SafeanFeand/SafeandFree.cfm?ID=18957&c=262>. In turn, a number of media organizations, including the New York Times and the Washington Post, have published articles to the same effect. See, e.g., "FBI, Using Patriot Act, Demands Library's Records," New York Times, Aug. 26,2005, p. A12; "Library Challenges FBI Request," Washington Post, Aug. 26, 2005, p. All. Thus, the public is fully aware that an NSL has been served on an unidentified member of the American Library Association that has library records, and the government has not objected to the disclosure of that information. What remains confidential - and what Section 2709(c) prohibits from being disclosed- are the identity of the recipient of the NSL and the target of the NSL.

Notwithstanding the existence of the statutory bar on disclosure, the plaintiffs moved for a preliminary injunction to allow them to disclose the NSL recipient's identity. In support of this motion, the plaintiffs claimed that the non-disclosure provision prevents them from informing Congress, which is currently considering legislative revisions to Section 2709, about the kind of institution that has received the NSL in this case. Memorandum of Law in Support of Plaintiffs' Motion for Preliminary Injunction, p. 10 (filed Aug. 16, 2005). They also claimed that the non-disclosure provision prevents Doe from informing libraries and their patrons about the supposed "threat to intellectual freedom" posed by Section 2709. *Id.* at 8. And they similarly claimed that the non-disclosure provision prevents Doe from "discuss[ing] and develop[ing] standardized procedures and policies for responding to the receipt of future NSLs" with libraries and library associations. *Id.* at 9.

The government opposed the motion on the ground that the plaintiffs are not likely to prevail on the merits of their First Amendment claim and that the balance of harms weighs decisively against allowing the plaintiffs to make a public disclosure that would give notice to the target of the NSL that his activities may be the object of an ongoing government counter-terrorism investigation. The government pointed out that the release of the redacted complaint, and the ensuing press release and news coverage, provide the public and Congress with the very information about the application of Section 2709 that the plaintiffs claim they are currently unable to disclose. The government further pointed out that disclosing the identity of the specific recipient of the NSL would contribute nothing to the public and Congressional debate over Section 2709, but could put the target of the NSL on notice about the government's investigation and therefore could compromise the investigation itself.

On September 9, 2005, the district court issued a mandatory preliminary injunction that would allow the plaintiffs to violate Section 2709(c) by publicly disclosing that Doe is the recipient of the NSL. The injunction provide that "the defendants are hereby stayed from enforcing 18 U.S.C. § 2709(c) against the plaintiffs with regard to Doe's identity." SPA-31. Based on the record before it, the court found that "the investigation clearly relates to national security"; that "[t]he government has a legitimate interest and duty in undertaking an investigation that includes this NSL"; and that "it is clear to the court that the NSL was not issued solely on the basis of First Amendment activities." *Id.* at SPA-18. Despite these r determinations, the district court ruled that the plaintiffs are likely to establish that Section 2709(c) is unconstitutional as applied to their public disclosure of Doe's identity in this case. *Id.* at A-12-29. The court further ruled that the plaintiffs will be irreparably harmed by the inability to immediately identify Doe as the recipient of the NSL. *Id.* at SPA-10-12.[2]

The district court stayed its preliminary injunction until September 20, 2005, to permit the government to seek a stay pending appeal from this Court. On September 20, this Court granted a full stay pending appeal. At the same time, the Court ordered expedited briefing and set this appeal and *Doe v. Gonzales,* No. 05-0570, for consolided oral argument.

SUMMARY OF THE ARGUMENT

Secrecy is essential to the effective conduct of counter-terrorism and counterintelligence investigations. Public disclosure of steps taken by the government to investigate the activities of terrorist groups and foreign intelligence organizations pose a direct and immediate threat to the ability of the government to detect and prevent those activities. Alerted to the existence of an investigation, its direction, or the methods and sources being used to pursue the investigation, target groups can take steps to evade detection, destroy evidence, mislead investigators, and change their own conduct to minimize the possibility that

 © 2017 Thomson Reuters. No claim to original U.S. Government Works.

future terrorist and foreign intelligence activities will be detected.

Section 2709(c) is one of a number of statutory provisions that seek to safeguard the required secrecy of counter-terrorism and counter-intelligence investigations by preventing private parties to whom the government turns for information from destroying the confidentiality of the government's inquiry. Numerous judicial precedents, including this Court's own decision in *Kamasinksi v. Judicial Review Council,* 44 F.3d 106 (2d Cir. 1994), make clear that Congress may constitutionally prohibit disclosure of information about a secret government investigation that a private party learns only through its own participation in the investigation. Section 2709(c) readily passes constitutional muster under these precedents, for it is designed to further the compelling governmental and public interest in effectively detecting and preventing terrorism and foreign espionage, and it is carefully tailored to restrict only information that an NSL recipient has learned through its participation in the NSL inquiry itself.

Notwithstanding these precedents, the district court concluded that the plaintiffs have a First Amendment right to make public the identity of the NSL recipient in this case. That holding is fundamentally wrong. As the record below makes clear, an NSL recipient's public disclosure of its own identity places counter-terrorism and counterintelligence investigations directly in jeopardy, both because it alerts the target of the NSL that his activities may be under scrutiny by the government and because it allows terrorist groups and foreign intelligence organizations to monitor which communication service providers are being asked for information under Section 2709 and tailor their own communication activities accordingly. In demanding proof before the fact that these risks will actually come to fruition in the circumstances of this case, the district court has set the constitutional bar far higher than this Court itself did *in Kamasinski,* and has improperly substituted its own judgments about national security for the reasoned and expert judgments of the Executive Branch agencies responsible for conducting counter-terrorism and counterintelligence investigations.

In addition to misapplying governing First Amendment principles, the district court erred in concluding that the balance of harms favors immediate disclosure of the NSL recipient's identity. Contrary to the district court's belief, the plaintiffs have no need to disclose Doe's identity in order to take part in the current political debate regarding Section 2709 and library records. As shown by the redacted complaint and the subsequent press coverage, the essential facts that the plaintiffs wish to publicize regarding the potential application of Section 2709 to libraries that provide electronic communication services are already public, and Section 2709(c) does not restrain them from discussing those facts. The identity of the NSL recipient in this case adds nothing to the terms of this public discussion. In contrast, Doe's disclosure of its identity would cause present precisely the risks that Section 2709(c) legitimately seeks to forestall.

STANDARD OF REVIEW

A grant of a preliminary injunction is reviewed for abuse of discretion, "which will be found if the district court applies legal standards incorrectly or relies upon clearly erroneous findings of fact, or proceed[s] on the basis of an erroneous view of the applicable law." *Register.com, Inc. v. Verio, Inc.,* 356 F.3d 393, 398 (2d Cir. 2004) (internal quotation marks and citations omitted). When the moving party seeks a preliminary injunction of "government action taken in the public interest pursuant to a statutory or regulatory scheme, it must show (at the least) (i) irreparable harm absent the injunction and (ii) a likelihood of success on the merits." *Freedom Holdings, Inc. v. Spitzer,* 408 F.3d 112, 114 (2d Cir. 2005) (internal quotation marks omitted). Moreover, when a preliminary injunction will "alter, rather than maintain [,] the status quo, or will provide the movant with * * * relief [that] cannot be undone even if the defendant prevails at a trial on the merits," the moving party must "show a clear or substantial likelihood of success." *Beal v. Stern,* 184 F.3d 117, 122-23 (2d Cir. 1999) (internal quotation marks omitted).

ARGUMENT

THE PRELIMINARY INJUNCTION AGAINST ENFORCEMENT OF SECTION 2709(c) IN THIS CASE SHOULD BE REVERSED

I. The Recipient of a National Security Letter Has No Constitutional Right To Disclose His Identity During an Ongoing Counter-Terrorism Investigation

A. This Court and Other Courts Have Sustained the Constitutionality of Non-Disclosure Requirements Like Section 2709(c)

Counter-terrorism and counterintelligence investigations are conducted in secret because they cannot be conducted effectively any other way. Counter-terrorism and counterintelligence investigations are long-range, forward-looking, and prophylactic in nature; the government aims to anticipate and disrupt clandestine intelligence activities and terrorist attacks on the United States before they occur. A-91-92. Because these 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 an investigation. *Id.* If targets learn that their activities are being investigated, they can be expected to take action to avoid detection or disrupt the government's intelligence gathering efforts. *Id.* at A-92. Likewise, knowledge about the scope or progress of a particular investigation allows targets and to determine the FBI's degree of penetration of their activities and to alter their timing or methods. *Id.* at A-92-93. The same concern applies to knowledge about the sources and methods the FBI is using to acquire information, knowledge which can be used both by the immediate targets of an investigation and by other terrorist and foreign intelligence organizations. *Id.* at A-92-94, A-97-98.

This critical need for secrecy in counter-terrorism and counterintelligence investigations provides the explanation and justification for Section 2709(c) and the corresponding non-disclosure requirements that Congress has attached to other investigatory tools in the counter-terrorism and counterintelligence fields (see pp. 7-8 *supra).* To the extent that the government can conduct such investigations without the assistance of third parties, it can maintain the required secrecy simply by refraining from disclosing information about the investigation. But when relevant information is in the hands of third parties, requests or commands from the government for production of the information unavoidably notifies those parties of the existence of the investigation and gives them knowledge about the investigation to which they were not previously privy. In these circumstances, the only way to ensure the continued secrecy of the investigation, and thereby prevent the investigation itself from being compromised, is to obligate the private party not to disclose information about the investigation that it has learned through its own participation.

It would be both surprising and profoundly troubling if the Constitution were thought to disable the government from requiring non-disclosure in these circumstances. If that were so, the government would be left with two alternatives: either to forgo seeking the information, at least where the government lacks confidence that the private party can be relied on to maintain secrecy voluntarily, or to seek the information anyway and run the risk that the party will disclose what it has learned through its involvement in the investigation. Both alternatives compromise the government's ability to detect and prevent terrorist attacks and foreign espionage activities - the first by depriving the government of information that is relevant and perhaps critical to the investigation, the second by destroying the secrecy of the investigation itself.

In fact, however, the Constitution does not reduce the government to choosing between these two unacceptable alternatives. Numerous judicial decisions, including this Court's own decision *in Kamasinksi v. Judicial Review Council,* 44 F.3d 106 (2d Cir. 1994), make clear that the First Amendment does not entitle private parties to disclose information about a secret government investigation that the party learned only through its own participation in the investigation.

In *Kamasinski,* this Court was presented with a First Amendment challenge to a Connecticut statute that restricted disclosure of information relating to confidential investigations of judicial misconduct. The statute provided that "any individual called by the [investigating] council for the purpose of providing information shall not disclose his knowledge of such investigation to a third party prior to the decision of the council whether probable cause exists," while permitting disclosure of information "known or obtained independently of any such investigation * * * ." Conn. Gen. Stat. § 51-51*l*. A private party who had filed

a judicial misconduct complaint challenged the constitutionality of the non-disclosure requirement under the First Amendment. 44 F.3d at 109. The district court held that the statute was constitutional, and this Court affirmed that decision. *Id.* at 110-112.

In assessing the constitutional challenge, this Court identified three distinct categories of information that an individual might wish to disclose. The first category consisted of "the substance of an individual's complaint or testimony, i.e., the individual's own observations or speculations regarding judicial misconduct."*Id.* at 110. The second consisted of "the complainant's disclosure of the *fact* that a complaint was filed, or the witness's disclosure of the fact that testimony was given." *Id.* (emphasis in original). The third consisted of "information that an individual learns by interacting with" the investigating commission. *Id.*

The Court held that disclosure of the first category of information, consisting of information about judicial misconduct independently known by the complainant or witness, could not constitutionally be prohibited. *Id.* At the same time, however, the Court held that Connecticut *could* constitutionally restrict disclosure of the second and third categories of information - information about the party's participation in the investigation and information learned though that participation. *Id.* at 110-112. The Court held that "[t]he State's interest in the quality of its judiciary * * * is an interest of the highest order"; that this interest was furthered by conducting investigations of judicial misconduct on a confidential basis; and that prohibiting disclosure of information about a party's participation in the investigation and information learned though that participation was constitutionally permissible to maintain the confidentiality of the investigation. *Id.* at 110, 111-12.

Other Courts of Appeals have employed the same constitutional reasoning as *Kamasinski* in similar contexts. See *Hoffman-Pugh v. Keenan,* 338 F.3d 1136 (10th Cir. 2003); *In re Subpoena to Testify before Grand Jury Directed to Custodian of Records,* 864 F.2d 1559 (11th Cir. 1989); *First Amendment Coalition v. Judicial Inquiry and Review Board,* 784 F.3d 467 (3d Cir. 1986) (*en banc).* For example, in *Hoffman-Pugh,* the Tenth Circuit rejected a First Amendment challenge to a Colorado statute that sought to preserve the secrecy of grand jury proceedings by prohibiting witnesses from disclosing " 'what transpires or will transpire before the grand jury.' " 338 F.3d at 1139 (quoting *State v. Richard,* 761 P.2d 188, 192 (Colo. 1988)). The Tenth Circuit explained that "a [constitutional] line should be drawn between information the witness possessed prior to becoming a witness and information the witness obtained through her actual participation in the grand jury process." *Id.* at 1140. The court concluded that "drawing the line at what [the witness] knew prior to testifying before the grand jury protects her First Amendment right to speak while preserving the, state's interest in grand jury secrecy." *Id.*

In *In re Subpoena,* the Eleventh Circuit drew the same line in rejecting a First Amendment challenge to a federal grand jury closure order. The court held that, while a subpoenaed witness could not be prohibited from "disclosure of documents prepared and assembled independent of the grand jury proceedings," it could be prohibited from "revealing the direction of the grand jury investigation" and from disclosing "the names of individuals being investigated, or those who might be expected to testify before the grand jury, or any other secret aspect of the grand jury investigation." *Id.* at 1564. And in *First Amendment Coalition,* a decision that anticipated this Court's decision in *Kamasinski,* the *en bane* Third Circuit held that while Pennsylvania could not constitutionally prohibit witnesses from disclosing information about judicial misconduct "obtained from sources outside" a judicial misconduct investigation," the state could constitutionally prohibit witnesses and other persons "from disclosing proceedings taking place before the [investigating] Board." 784 F.2d at 478-79.

At a more general level, the Supreme Court itself has recognized that restrictions on a party's disclosure of information obtained through participation in confidential proceedings stand on a different and firmer constitutional footing from restrictions on the disclosure of information obtained by independent means. In *Seattle Times Co. v. Rhinehart,* 467 U.S. 20 (1984), the Supreme Court upheld the constitutionality of a judicial order that prohibited parties to a civil suit from disclosing sensitive information obtained through pretrial discovery. In rejecting a First Amendment challenge to the order, the Court noted that the parties "gained the information they wish to disseminate only by virtue of the trial court's discovery processes," which themselves were made available as a matter of legislative grace rather than constitutional right. 467 U.S. at 32. The Court reasoned that "control over [disclosure of] the discovered information does not raise the same specter of government censorship that such control might suggest in other situations." *Id.* The Court added that the order was "not the kind of classic prior restraint that requires exacting First Amendment scrutiny," because it "prevent[ed] a party from disseminating only that information obtained through the use of the discovery process" and left the party free to disseminate

 © 2017 Thomson Reuters. No claim to original U.S. Government Works.

any information "gained through means independent of the court's processes." *Id.* at 33-34.

The Supreme Court relied on this distinction again in *Butterworth v. Smith,* 494 U.S. 624 (1990). In *Butterworth,* the Court held that Florida could not constitu-tionally prohibit a grand jury witness from disclosing the substance of his testimony after the term of the grand jury had ended. In so holding, the Court distinguished *Rhinehart* on the ground that "[h]ere * * * we deal only with [the witness'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.* at 632. Enlarging on this point, Justice Scalia observed that "[q]uite a different question is presented * * * 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).

When measured against the standards established by these precedents, Section 2709(c) readily passes constitutional muster. It is designed to vindicate the government's interest in shielding its counter-terrorism and counterintelligence investigations from the eyes of terrorists and foreign intelligence organizations. That governmental interest is a manifestly compelling one. See, *e.g., 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"); *Snepp v. United States,* 444 U.S. 507, 509 n.3 (1980) (*per curiam*) ("The Government has a compelling interest in protecting * * * the secrecy of information important to our national security"). And Section 2709(c) is carefully tailored to advance that interest without unnecessarily restricting speech that does not implicate the government's legitimate interests in confidentiality.

By its terms, Section 2709(c) applies only to the NSL recipient's disclosure of the fact that the government "has sought or obtained access to information or records under this section." Its scope thus fits squarely within *Kamaniski's* second and third categories of information - the fact that information has been provided to an investigation (category 2) and "information that an individual learns by interacting with" the investigating body (category 3). 44 F.3d at 110. Section 2709(c) does not purport to prohibit an NSL recipient from disclosing information that he has learned by means other than his involvement in the NSL inquiry. And, as discussed further below, it places no restriction on the ability of NSL recipients or others to engage in general public discussions regarding the scope, operation, or desirability of Section 2709. As another district court has observed:

> Anything outside th[e] bare fact [that the FBI has sought or obtained information from the NSL recipient under Section 2709] 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.

Doe v. Ashcroft, 334 F. Supp. 2d 471, 514 (S.D.N.Y. 2004), *appeal pending sub nom. Doe v. Gonzales,* No. 05-0570.

The non-disclosure obligation imposed by Section 2709(c) differs in only one respect from the non-disclosure requirement upheld by this Court in *Kamasinski:* the obligation continues after the particular investigation that gave rise to the NSL comes to a close. As explained further below, that difference has no bearing on the plaintiffs' present as-applied challenge, because the investigation in this case is still underway. But even if the investigation were complete, the permanent character of the non-disclosure obligation is justified by the unique characteristics of counter-terrorism and counterintelligence investigations - characteristics that are amply documented in the record below and that have been recognized both by the Supreme Court and by Congress.

As explained by the Assistant Director of the FBI's Counterintelligence Division, David Szady, counter-terrorism and counterintelligence investigations differ from traditional criminal investigations because their primary objective "is not to gather evidence for prosecution of past crimes, but rather to disrupt and interdict clandestine intelligence activities and terrorist acts *before* they occur." A-92-93. Counter-terrorism and counterintelligence investigations are thus uniquely

 © 2017 Thomson Reuters. No claim to original U.S. Government Works.

forward-looking and long range. *Id.* The Supreme Court and Congress have both recognized that the forward-looking and open-ended nature of such investigations distinguish them from conventional criminal investigations. See *United States v. United States District Court,* 407 U.S. 297, 322 (1972) ("The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information," and "[o]ften, 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"); S. Rep. No. 95-604 at 16 (1978), reprinted in 1978 U.S.C.C.A.N. 3985. The need for secrecy therefore continues even after particular information has been used against a particular target. A-93.

In addition, terrorist groups and foreign intelligence organizations can use disclosures to piece together damaging information about the government's investigatory capacities and strategies even after the particular investigation in which an NSLs was issued has come to a close. The FBI has learned from experience that terrorist and foreign intelligence organizations "have the sophistication and capability to closely analyze publicly available information concerning the United States' intelligence gathering activities." A-93. They "can and do piece together publicly available information," including details that may appear innocuous in isolation, and thereby determine the scope, focus, and progress of ongoing counter-terrorism and counterintelligence investigations. *Id.* Armed with such information, they can tailor their activities to avoid detection in future investigations and exploit perceived weaknesses in this nation's intelligence gathering capabilities. *Id.* at A-93-94. Thus, information about particular uses of NSLs, even in completed investigations, can educate terrorist and foreign intelligence organizations about how to circumvent and disrupt similar intelligence gathering in the future. *Id.* at A-100-101. Nothing in *Kamasinski* suggests that a permanent non-disclosure obligation is constitutionally suspect in these circumstances.

The district court sought to distinguish this case from *Kamasinski* on other grounds, but those efforts are wholly unavailing. The district court observed that here, unlike in *Kamasinski,* "the existence of an investigation is already public." SPA-27. But that fact is irrelevant to the government's interest in preserving the continued secrecy of *other* information about the investigation, such as the identity of the NSL's recipient, that would reveal the focus of the investigation. The district court also suggested that NSL recipients "who might have information regarding investigative abuses and overreaching are preemptively prevented from sharing that information with the public and with the legislators." SPA-28. But that concern has no relevance to the plaintiffs' as-applied challenge, for here, as the district court itself acknowledged, the present investigation "clearly relates to national security," and the government "has a legitimate interest and duty in undertaking an investigation that includes this NSL." SPA-18. Moreover, even if (contrary to the district court's acknowledgment) the NSL here *were* illegitimate, an injunction that permits Doe only to disclose its identity would not advance any supposed interest in disclosing such abuse. In short, the district court's reasoning neither distinguishes *Kamasinski* nor justifies the injunction that the court entered.

B. The District Court's Objections to the Application of Section 2709(c) in this Case Are Without Merit

The district court did not take issue with the need for secrecy in counter-terrorism and counterintelligence investigations, nor did it suggest that the First Amendment vests communication service providers with a general right to disclose information they learn as a result of having been served with an NSL. Nevertheless, the court ruled that the plaintiffs are likely to establish that Section 2709(c) is unconstitutional as applied to the plaintiffs' public disclosure of the NSL recipient's identity in this case. That ruling is profoundly mistaken.

1. The record below demonstrates that the concerns animating Section 2709(c) are directly implicated by an NSL recipient's disclosure of its own identity. Persons who are engaged in (or otherwise have knowledge of) terrorist or foreign intelligence activities know which communication service providers they themselves use, and if such a person learns that the government is seeking information from his provider pursuant to an NSL issued in connection with a counter-terrorism or counterintelligence investigation, that information puts the target on notice that his activities may have attracted the government's attention. So forewarned, he can take actions to avoid detection and evade or disrupt the government's intelligence gathering activties - for example, by absconding, destroying damaging evidence, creating false evidence, or using other methods of communication. A-92, A-95-96. Even if the target of the NSL is not himself directly involved in terrorist or foreign intelligence activities, knowledge that the government may be seeking information about him could allow him to

warn others. *Id.* at A-96. In addition, a terrorist or foreign intelligence organization whose agents use the particular communication service provider may thereby learn which of its communications are potentially compromised, and could instruct its agents not to use, or to give disinformation to, such providers. A-98-99. More broadly, terrorist groups and foreign intelligence organizations can use such information to keep track of how often particular providers receive NSLs, and to avoid providers most likely to receive such inquiries, thereby screening their activities from detection. *Id.* at A-99.

The district court did not dispute that the disclosure of an NSL recipient's name can compromise the government's ability to detect and prevent terrorism and espionage in this fashion. See SPA-22. But it held that Doe nevertheless has a constitutional right to publicize its own identity because the government did not prove to the court's satisfaction that these harms will occur in this particular case. In the view of the district court, it is not enough for the government to provide uncontradicted expert testimony about the risks associated with the disclosure of NSL recipients' names. Instead, the court believed that the First Amendment requires the government to prove, conclusively and before the fact, that those risks will actually mature in the present case. See SPA-19, 21-22.

In subjecting the government to this stringent burden of proof, the district court placed itself directly at odds with this Court's decision in *Kamasinski. In Kamasinski,* this Court identified various harms that could flow from the premature disclosure of information about a confidential investigation into judicial misconduct. See 44 F.3d at 111. The Court did not find, however, that any of these harms *would* actually come to pass in the circumstances of the case before it. Nor did the Court demand that Connecticut supply such proof. Instead, it was constitutionally sufficient that the risks identified by the Court were characteristic ones that could fairly be expected to arise in the absence of any contrary showing.

For example, the Court relied on *"the fear* that * * * complainants will engage in a campaign of harassment," which *"may* result in influences that lead to the loss of judicial independence as well as an overburdening of the JRC with frivolous complaints." *Id.* (emphasis added). The Court did not require the state to show that the complainant in *Kamasinski* itself was actually engaging in such a campaign, or that allowing him to disclose that he had filed a complaint would in fact jeopardize judicial independence. Similarly, the Court relied on the fact that "a common result" of disclosure would be deterrence of other witnesses, without finding that such a I result would actually occur in the case before it. *Id.* And the Court looked to the state's "significant interest in encouraging infirm or incompetent judges to step down voluntarily," again without inquiring whether disclosure in the particular circumstances of that case would actually have such an effect. *Id.*

The kind of showing presented by the government in this case is precisely the kind relied on by this Court in *Kamasinski.* The declaration executed by the Assistant Director of the FBI's Counterintelligence Division identifies a number of real and concrete risks created by the disclosure of information regarding the FBI's use of NSLs, including information about the identity of an NSL recipient. The declaration makes clear that those risks are categorical ones characteristic to one degree or another of all cases under Section 2709. The First Amendment demanded nothing more than this in *Kamasinski;* it demands nothing more here.

In the sealed portion of its opinion, the district court noted that Doe provides [ ] service to [ ] and that the number of people who have made use of that service "would likely be [ ]." SPA-32. The court reasoned that Doe's disclosure of its identity would do little to indicate which of those [ ] users is the subject of the government's investigatory interest. But the number of people who make use of Doe's [ ] services is irrelevant to the investigative impact of the disclosure of Doe's. At most, only an extraordinarily small number of those users have reason to think that their activities are of interest to a counter-terrorism investigation. And for each of *those* users, Doe's disclosure of that it has received an NSL under Section 2709 would certainly sound an alarm bell. A user who has engaged in activity that is relevant to a counter-terrorism or counterintelligence investigation can draw no comfort from the number of other users who have not engaged in such activities.

2. At a fundamental level, the district court's opinion reflects an unwarranted reluctance to give weight to reasoned judgments of the Executive Branch regarding the risks associated with the disclosures about secret intelligence gathering activities. "[P]redictive judgment[s] [by the executive branch] of the harm that will result from the disclosure of information" in the national security context are entitled to judicial deference, for "[i]t is abundantly clear that the government's top counterterrorism officials are well-suited to make this predictive judgment," while "the judiciary is in an extremely poor position to second-guess the executive's judgment in this area of national security." *Center for National Security Studies v.*

WESTLAW © 2017 Thomson Reuters. No claim to original U.S. Government Works.

Department of Justice, 331 F.3d 918, 928 (D.C. Cir. 2003).

This principle of judicial deference has been recognized by numerous courts, including the Supreme Court itself. See, *e.g,* *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"); *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 [created by disclosures of individual facts], [judges] should not entrust to them[selves] the decision whether an isolated fact is sensitive enough to warrant disclosure"); *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,* 334 F. Supp. 2d at 523 ("judges do not have national security experience[,] [n]or 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").

The district court professed to recognize the appropriateness of judicial deference regarding these judgments, but it nevertheless dismissed the record presented by the government in this case as impermissibly "speculative." SPA-17, 19. There is nothing speculative, however, about the risks identified by the government. They are the product not of speculation, but rather hard-won experience. See, *e.g.,* A-93 ("[T]he FBI has determined *through its past and ongoing counter-terrorism and counterintelligence investigations* [that] terrorist and foreign intelligence organizations have the sophistication and capability to closely analyze publicly available information concerning the United States' intelligence gathering activities"). To dismiss the carefully considered judgments presented by the government in this case as mere "speculation," and to replace those judgments with the court's own conclusion that disclosure would not be harmful, is to make the judiciary rather than the Executive Branch the arbiter of this country's intelligence gathering needs. That is a role the judiciary is institutionally unsuited to play.

3. The district court suggested that Section 2709(c) reaches impermissibly far by mandating non-disclosure even after the completion of the investigation for which the particular NSL was issued. The district court held that, while the government has "a compelling interest in conducting its investigation in secret so that the target(s) of the investigation are not aware of it," that interest could not justify a prohibition against the disclosure of Doe's identity after the current investigation is over. SPA-23-25.

This reasoning is misconceived at two different levels. First, as shown above, the unique characteristics of counter-terrorism and counterintelligence investigations mean that public disclosures about the government's investigatory activities and methods can cause serious harm even when they occur long after a particular investigation has come to an end. See pp.26-29 *supra.* Second, even assuming that the justification for preserving the secrecy of Doe's identity could lapse *after* the current investigation is complete, that possibility hardly justifies the injunction issued by the district court, which permits the disclosure of Doe's identity *now,* while the investigation is still very much underway. In speculating about the impact of disclosures on completed investigations, the court lost sight of the ongoing investigation actually before it.

The court also suggested the Section 2709(c) is impermissibly broad because it encompasses "[a]ll details relating to the NSL * * * without any showing that each piece of information, if disclosed, would adversely affect national security." SPA-25. The court's assumption that particular "details" regarding an NSL may be harmless ignores the demonstrated capacity of terrorist and foreign intelligence agencies to assemble seemingly innocuous pieces of information into a dangerously revealing mosaic. A-93; see, *e.g.,* *Halkin v. Helms,* 598 F.2d 1, 8 (D.C. Cir. 1978); *Halperin v. CIA,* 629 F.2d 144, 150 (D.C. Cir. 1980).[3] In any event, the question before the district court concerned the effect of disclosing one piece of information in particular - the identity of the NSL recipient. As we have already shown, the plaintiffs cannot disclose *that* information without creating the risks that lie at the heart of Section 2709(c).

4. One final aspect of the district court's First Amendment analysis requires comment. The court held that Section 2709(c) is subject to strict scrutiny because, in the court's view, it constitutes a prior restraint on speech. See SPA-13-15. That holding is erroneous in two respects. First, Section 2709(c) is *not* a prior restraint. Second, even if it were, it would not constitute the

kind of prior restraint that triggers strict scrutiny under the First Amendment.

The Supreme Court's prior restraint precedents involve two types of restraint, neither of which is presented by Section 2709(c). The first is an administrative licensing scheme, under which an individual who wishes to speak must first seek a license or other prior approval from the government. See *City of Lakewood v. Plain Dealer Publishing Co.,* 486 U.S. 750, 757 (1988). Such licensing schemes present unique First Amendment concerns because they vest administrative decisionmakers with discretionary power that can be abused to suppress constitutionally protected speech; because the licensing process itself can delay speech; and because the prospect of having to undergo administrative review encourages self-censorship. *Harman v. City of New York,* 140 F.3d 111, 119-120 (2d Cir. 1998). Those risks are not created by statutes like Section 2709(c) that categorically prohibit speech, even when (unlike Section 2709(c)) they subject violators to criminal punishment. See *Landmark Communications, Inc. v. Virginia,* 435 U.S. 829, 838 (1978) (Virginia statute prohibiting disclosure of confidential information about judicial misconduct investigations and subjecting violators to criminal penalties "does not constitute a prior restraint"); *City of Lakewood,* 486 U.S. at 764 (distinguishing between statute imposing prohibition on speech and statute conditioning speech on obtaining a license or permit from official).

The second category of prior restraints consists of judicial injunctions against particular speech or speakers. See, *e.g., Near v. Minnesota ex rel. Olson,* 283 U.S. 697 (1931). In this case, the government has not sought, and the district court has not issued, any order prohibiting the plaintiffs from making the disclosures prohibited by Section 2709(c). Thus, even if such an order would constitute a prior restraint, no such restraint is involved here.

The district court acknowledged that Section 2709(c) "may not look like a typical prior restraint," but held that it nevertheless constitutes a prior restraint because it prohibits speech "in advance of it having occurred." SPA-13. But virtually any law that renders particular kinds of speech unlawful can be characterized in the same terms. For example, it is unlawful in every state to make defamatory statements. Yet no one would suggest that the common law of defamation constitutes a prior restraint simply because it makes defamatory speech unlawful. And the constitutional result would not change if a state chose to replace its common law with a statute providing that "no person shall make defamatory statements." In the absence of any requirement that a speaker submit his speech to scrutiny by an agency before making it, or any attempt to enjoin the speaker before he has spoken, the bare existence of a statutory prohibition on defamatory speech would not constitute a prior restraint. The same reasoning applies to the countless state statutes that make it unlawful to publish or disseminate obscene speech. So too here, the bare existence of Section 2709(c), without more, does not amount to a prior restraint.

In any event, even if Section 2709(c) could be classified as a prior restraint, the Supreme Court's decision in *Rhinehart* makes clear that it is not the sort of prior restraint that triggers strict scrutiny. As noted above, *Rhinehart* involved a judicial order prohibiting speech. However, the Court pointed out that the judicial order there restricted only the disclosure of information "obtained through use of the discovery process," not information "gained through means independent of the court's processes." 467 U.S. at 34. For that reason, the Court held that the order "is not the kind of classic prior restraint that requires exacting First Amendment scrutiny." *Id.* at 33. The same reasoning applies here.

Finally, even if Section 2709(c)*were* the kind of prior restraint that triggers strict scrutiny, it would readily survive that review. This Court applied strict scrutiny to the non-disclosure requirement at issue in *Kamasinski* - not because that requirement was a prior restraint, but instead because the Court regarded the requirement as content-based. See 44 F.3d at 109.[4] Yet the Court had no difficulty in holding that the statute satisfied strict scrutiny. As we have already shown above, Section 2709(c) readily passes muster *under Kamasinski.* Thus, even if strict scrutiny is otherwise appropriate, Section 2709(c) survives that scrutiny.

II. The Balance of Harms Weighs Strongly Against Allowing the Plaintiffs to Publicly Disclose the NSL Recipient's Identity

For the foregoing reasons, the plaintiffs have not established a likelihood that they will prevail on their as-applied challenge to Section 2709(c), much less the "clear or substantial" likelihood of success (*Beal,* 184 F.3d at 122-23) that is required to

support a mandatory preliminary injunction that irreversibly alters the status quo. That alone is sufficient to warrant reversal of the district court's injunction. But the injunction also must be reversed for another, equally important reason: the balance of harms does not weigh in favor of the plaintiffs, but rather tilts decisively in favor of the government.

A. Prohibiting Disclosure of Doe's Identity Does Not Materially Impair the Plaintiffs' Asserted First Amendment Interests

The plaintiffs' central rationale for demanding *immediate* disclosure of Doe's identity, as opposed to waiting for the district court to reach a final judgment on the merits of the plaintiffs' constitutional claims, is that the inability to identify Doe supposedly prevents the plaintiffs from taking part in ongoing public and Congressional debate regarding Section 2709. Thus, the plaintiffs argued below that the non-disclosure requirement prevents Doe from "lobby[ing] Congress for additional safeguards" to be added to Section 2709; from "educat[ing] and organiz[ing]" the "library community"; from "coordinat [ing] procedures for responding to NSLs"; and from alerting "patrons and the general public to the dangers posed by the Patriot Act." Reply Memorandum of Law in Support of Plaintiffs' Motion for Preliminary Injunction ("PI Reply") at 8-9.

Even a casual examination of Section 2709(c) is sufficient to dispose of these claims. By its terms, Section 2709(c) provides only that the recipient of an NSL may not disclose that the government "has sought or obtained access to information or records" from the recipient under the section. The non-disclosure provision does not prevent the recipient of an NSL, or anyone else, from taking part in public debate regarding the scope, application, and desirability of Section 2709. NSL recipients remain perfectly free to "lobby Congress for additional safeguards," to "educate and organize" the "library community" or any other sector of the public, to "coordinate procedures for responding to NSLs," and to call the attention of one and all to the supposed "dangers" presented by Section 2709 (PI Reply at 8-9). The mere inability of an NSL recipient to disclose that *it* has received an NSL places no impediment whatsoever in the way of these undertakings.

The course of this litigation itself confirms the hollowness of the plaintiffs' claims. As shown above, the plaintiffs have already publicly stated that an NSL has been served on a member of the American Library Association (ALA), and major news organizations have reported that Section 2709 is being used to seek records from a library. Thus, to the extent that the plaintiffs wish to call the attention of the public and Congress to the potential applicability of Section 2709 to libraries, they have already done precisely that - without having to identify the entity that has received the NSL in this case. The ALA itself lobbies Congress on behalf of its members (A-84-87) and is free to note that one of its members has been served with an NSL; the ability to identify *which* particular member adds nothing to that effort.

The district court expressed the view that "Doe's statements as a known recipient of a NSL would have a different impact on the public debate than the same statements by a speaker who is not identified as a recipient." SPA-12. But there is no reason whatsoever to expect that to be so. Doe has no "tale to tell" about the details of the NSL in this case; the injunction allows Doe only to identify itself as the recipient of the NSL, not to disclose any other information about the NSL or the circumstances surrounding it. There is no reason to think that Congress will find Doe's general views about the wisdom of Section 2709 more persuasive simply because of the bare fact that Doe has been served with an undescribed NSL.

B. Disclosure Will Irreparably Harm the Government and the Public Interest

The injuries to the government and the public interest that would be presented by Doe's public disclosure of its own identity have been discussed at length above, and we need not repeat that discussion in detail here. See pp. ___ *supra.* What bears emphasis is that these injuries are not only serious, but irreversible as well. Once Doe has been allowed to disclose its identity, the target of the NSL will be on notice that his actions are potentially compromised, offering him the opportunity to hide, flee, provide misinformation, or otherwise frustrate the investigation. A-92-93, A-95-96, A-98-99. At the same time, the disclosure will alert terrorist and foreign intelligence organizations to avoid this recipient in the future and will provide such groups with useful information about the geographic focus and methodology of the FBI's counter-terrorism and/or

WESTLAW © 2017 Thomson Reuters. No claim to original U.S. Government Works.

counterintelligence investigations generally. A-93-94. None of these consequences can be undone after Doe makes its identity public.

As a practical matter, therefore, the "preliminary" injunction in this case is tantamount to a final injunction with respect to the disclosure of Doe's identity. It is for that reason that this Court's precedents require the plaintiffs to demonstrate a "clear or substantial likelihood of success." *Beal,* 184 F.3d at 123. And that the plaintiffs have manifestly failed to do.

The plaintiffs can be expected to argue that the government's interests in non-disclosure [ ] But as the plaintiffs themselves acknowledge, [ ] but this Court granted a stay nevertheless - and rightly so. As other courts have repeatedly recognized [ ] So too here, [ ]

In their motion to vacate the Court's stay pending appeal, the plaintiffs suggested that [ ] The plaintiffs argued that [ ] [ ] That argument is misconceived both legally and factually.

Note: footnote reference missing in original document

5. See [ ]

As a legal matter, the interests of the Executive Branch in avoiding disclosure of information relating to national security are [ ]. See, *e.g.,* [ ] Indeed, [ ] the D.C. Circuit has held that [ ]

The plaintiffs sought to distinguish these cases in their stay vacatur motion on the ground that [ ] But the logic of these cases does not depend on [ ]. Instead, it rests on the recognition that [ ] The same logic applies where, as here,

As a factual matter, moreover, [ ]. See Even assuming that [ ] [ ]

For these reasons, this not a case in which [ ].

CONCLUSION

For the foregoing reasons, the preliminary injunction should be reversed.

Footnotes

1 The district court reviewed the classified declaration on an in camera basis. See SPA-6-8. If this Court wishes to see the classified declaration, the government will make appropriate security arrangements to make the declaration available to the Court. We strongly encourage the Court to review the declaration, as the district court did, to understand the origins of the current investigation and the nature of the interests involved.

2 The district court divided its opinion into three parts: an unsealed portion, a sealed portion, and a classified portion. The unsealed and sealed portions of the opinion are reproduced in the sealed appendix. The government will make appropriate security arrangements to make the classified portion of the opinion available to the Court.

3 The district court reasoned that cases like *Halkin and Halperin* are inapposite because the plaintiffs here are asserting a right to disclose information in their own possession, rather than a right to obtain information in the government's possession. SPA-21-22. That response misses the point. The risks identified in *Halkin* and *Halperin* turn on the nature of the information and the investigations at issue, not the nature of the legal claim being pressed by the plaintiffs, and the same risks are present here.

4 In our view, statutes like Section 2709(c) that seek to preserve the secrecy of confidential governmental investigations without prohibiting the disclosure of independently obtained information do not present the kind of First Amendment risks that warrant strict scrutiny. *Cf. Rhinehart,* 467 U.S. at 30-32 (applying intermediate rather than strict scrutiny to order prohibiting disclosure of

 © 2017 Thomson Reuters. No claim to original U.S. Government Works.

information obtained through discovery). To the extent that *Kamasinski* is inconsistent with that view, we respectfully submit that it is incorrect. We recognize that, absent *en banc* consideration, this Court is bound to adhere to *Kamasinski's* holding regarding the appropriate standard of constitutional review. By the same token, of course, the manner in which *Kamasinski* applied that standard is equally binding, and application of the standard in the same manner here confirms the constitutionality of Section 2709(c).

End of Document

© 2017 Thomson Reuters. No claim to original U.S. Government Works.