

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

NICHOLAS MERRILL,

Plaintiff,

v.

14 CIV. 9763 (VM)

ERIC HOLDER, Jr., in his official capacity as  
Attorney General of the United States, and  
JAMES B. COMEY, in his official capacity  
as Director of the Federal Bureau of  
Investigation,

Defendants.

REPLY MEMORANDUM OF LAW IN SUPPORT OF  
NICHOLAS MERRILL'S MOTION FOR SUMMARY JUDGMENT  
AND IN OPPOSITION TO THE GOVERNMENT'S MOTION TO DISMISS  
OR FOR SUMMARY JUDGMENT

Jonathan Manes, supervising attorney  
David A. Schulz, supervising attorney  
Benjamin Graham, law student intern  
Matthew Halgren, law student intern  
Nicholas Handler, law student intern  
Amanda Lynch, law student intern  
MEDIA FREEDOM AND INFORMATION  
ACCESS CLINIC  
YALE LAW SCHOOL  
P.O. Box. 208215  
New Haven, CT 06520  
Tel: (203) 432-9387  
Fax: (203) 432-3034  
jonathan.manes@yale.edu

*Attorneys for Plaintiff Nicholas Merrill*

**TABLE OF CONTENTS**

PRELIMINARY STATEMENT ..... 1

ARGUMENT ..... 2

I. THE FIRST AMENDMENT DOES NOT ALLOW THE FBI TO INDEFINITELY SUPPRESS SPEECH ABOUT THE SCOPE OF ITS STATUTORY AUTHORITY. .... 2

    A. The Gag Order Suppresses Discussion of the Government’s Interpretation of Its Statutory Authority, not Law Enforcement Techniques and Procedures. .... 3

        1. The Attachment Reveals the Scope of the Government’s Claimed Authority, Not “Techniques and Procedures.” .....3

        2. The Breadth of the Gag Order Can Be Explained Only by a Concern With Maintaining a Secret Interpretation of the NSL Statute.....6

    B. The Gag Order Unconstitutionally Suppresses Discussion of the Legal Interpretation of a Statute that Directly Affects the Rights of Citizens. .... 7

        1. The First Amendment Does Not Permit Gag Orders Whose Purpose or Effect Is to Maintain Secret Interpretations of Law.....7

        2. The Gag Order Has the Effect of Impeding Democratic Oversight of the Scope and Lawfulness of the Government’s Claimed Authority. ....9

    C. The First Amendment Has Never Been Interpreted to Permit Restraints on Speech About Government “Techniques and Procedures.” ..... 13

    D. The Gag Order is Permanent, and Therefore Unconstitutional, Because Its Duration Now Depends Solely on the Preferences of the Government..... 15

    E. The First Amendment Does Not Permit Gag Orders on Private Citizens With Respect to Information That Is in the Public Domain. .... 17

    F. The “Good Reason” Standard of *John Doe, Inc. v. Mukasey* Is Not Appropriate in the Circumstances of This As-Applied Challenge..... 18

II. THE GOVERNMENT FAILS TO ESTABLISH THAT ALLOWING PLAINTIFF TO SPEAK WOULD RESULT IN ANY HARMS..... 20

III. THE NSL STATUTE DOES NOT AUTHORIZE THE PRESENT GAG ORDER. .... 22

IV. IF THE COURT UPHOLDS THE GAG ORDER, IT SHOULD DO SO ONLY FOR A LIMITED PERIOD OF TIME..... 25

CONCLUSION..... 26

## TABLE OF AUTHORITIES

## CASES

<i>ACLU v. Clapper</i> , __ F.3d __, 2015 WL 2097814 (2d Cir. May 7, 2015).....	12
<i>Amazon.com LLC v. Lay</i> , 758 F. Supp. 2d 1154 (W.D. Wash. 2010).....	11
<i>Bank Julius Baer &amp; Co. Ltd v. Wikileaks</i> , 535 F. Supp. 2d 980 (N.D. Cal. 2008).....	17
<i>Black v. Sheraton Corp.</i> , 564 F.2d 531 (D.C. Cir. 1977).....	4
<i>Borchers v. Commercial Union Assur. Co.</i> , 874 F. Supp. 78 (S.D.N.Y. 1995).....	4
<i>Brennan Ctr. for Justice v. DOJ</i> , 697 F.3d 184 (2d Cir. 2012).....	9
<i>Brooklyn Legal Servs. Corp. v. Legal Servs. Corp.</i> , 462 F.3d 219 (2d Cir. 2006).....	19
<i>Butterworth v. Smith</i> , 494 U.S. 624 (1990).....	15
<i>Caplan v. ATF</i> , 587 F.2d 544 (2d Cir. 1978).....	9
<i>Cox Broad. Corp. v. Cohn</i> , 420 U.S. 469 (1975).....	17
<i>Crooker v. ATF</i> , 670 F.2d 1051 (D.C. Cir. 1981).....	9
<i>Doe v. Ashcroft</i> , 334 F. Supp. 2d 471 (S.D.N.Y. 2004).....	11
<i>Doe v. Gonzales</i> , 449 F.3d 415 (2d Cir. 2006).....	15
<i>Doe v. Holder</i> , 703 F. Supp. 2d 313 (S.D.N.Y. 2010).....	14, 16, 17, 23
<i>First Am. Coal. v. Judicial Inquiry &amp; Review Bd.</i> , 784 F.2d 467 (3d Cir. 1986).....	4, 8, 13

*Floyd v. City of New York*,  
739 F. Supp. 2d 376 (S.D.N.Y. 2010) ..... 14

*Frankel v. SEC*,  
460 F.2d 813 (2d Cir. 1972) ..... 4

*Hoffman-Pugh v. Keenan*,  
338 F.3d 1136 (10th Cir. 2003) ..... 4

*In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*,  
396 F. Supp. 2d 747 (S.D. Tex. 2005) ..... 8

*In re Application of N.Y. Times Co. for Access to Certain Sealed Court Records*,  
585 F. Supp. 2d 83 (D.D.C. 2008) ..... 8

*In re Application of United States*,  
396 F. Supp. 2d 45 (D. Mass. 2005) ..... 10, 22

*In re Charlotte Observer*,  
921 F.2d 47 (4th Cir. 1990) ..... 17

*In re City of New York*,  
607 F.3d 923 (2d Cir. 2010) ..... 4

*In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*,  
706 F. Supp. 2d 11 (D.D.C. 2009) ..... 11

*In re Grand Jury Subpoena to Amazon.com*,  
246 F.R.D. 570 (W.D. Wis. 2007) ..... 11

*In re Orders of this Court Interpreting Section 215 of the Patriot Act*,  
No. Misc. 13-02, 2014 WL 5442058 (For. Intel. Surv. Ct. Aug. 7, 2014) ..... 7, 8

*In re Pharmatrak, Inc. Privacy Litigation*,  
329 F.3d 9 (1st Cir. 2003) ..... 10

*Jewel v. Nat'l Sec. Agency*,  
673 F.3d 902 (9th Cir. 2011) ..... 8

*John Doe, Inc. v. Mukasey*,  
549 F.3d 861 (2008) ..... 19, 22, 24, 25

*Kamasinski v. Judicial Review Council*,  
44 F.3d 106 (2d Cir. 1994) ..... 4, 13, 15

*Lowenschuss v. W. Pub. Co.*,  
542 F.2d 180 (3d Cir. 1976) ..... 8

*McGehee v. Casey*,  
718 F.2d 1137 (D.C. Cir. 1983) ..... 14

*Milner v. Dep't of the Navy*,  
562 U.S. 562 (2011)..... 9

*N.Y. Times v. DOJ*,  
756 F.3d 100 (2d Cir. 2014) ..... 7

*Nat'l Cong. for P.R. Rights ex rel. Perez v. City of N.Y.*,  
194 F.R.D. 88 (S.D.N.Y. 2000) ..... 4

*Neb. Press Ass'n v. Stuart*,  
427 U.S. 539 (1976)..... 17, 22

*NLRB v. Sears*,  
421 U.S. 132 (1975)..... 9

*Papachristou v. Jacksonville*,  
405 U.S. 156 (1972)..... 9

*Scheiner v. Wallace*,  
No. 93-cv-0062, 1996 WL 633226 (S.D.N.Y. Oct. 31, 1996)..... 8

*United States v. Aguilar*,  
515 U.S. 593 (1995)..... 18

*United States v. Amodeo*,  
71 F.3d 1044 (2d Cir. 1995) ..... 8

*United States v. Antar*,  
38 F.3d 1348 (3d Cir. 1994) ..... 25

*United States v. Cooper*,  
No. 13-cr-693, 2015 WL 881578 (N.D. Cal. Mar. 2, 2015)..... 11, 22

*United States v. Davis*,  
785 F.3d 498 (11th Cir. 2015) ..... 6, 11, 22

*United States v. Duggan*,  
743 F.2d 59 (2d Cir. 1984) ..... 8

*United States v. U.S. Dist. Court for the E. Dist. of Mich.*,  
407 U.S. 297 (1972)..... 8

*Weisberg v. DOJ*,  
489 F.2d 1195 (D.C. Cir. 1973)..... 4

*Wilson v. CIA*,  
586 F.3d 171 (2d Cir. 2009) ..... 18

*Wright v. F.B.I.*,  
613 F. Supp. 2d 13 (D.D.C. 2009) ..... 14

**STATUTES**

18 U.S.C. § 2703 ..... 21

18 U.S.C. § 2709 ..... 22, 23

18 U.S.C. § 3511 ..... 23

USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101, 129 Stat. 268, 269-270 ..... 12

USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 103, 129 Stat. 268, 272 ..... 12

USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 107, 129 Stat. 268, 273-74 ..... 12

USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 501, 129 Stat. 268, 282 ..... 12

USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 502, 129 Stat. 268, 283-89 ..... 23, 24, 25

USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 503, 129 Stat. 268, 289-91 ..... 24

**OTHER AUTHORITIES**

Benjamin N. Cardozo, *The Nature of the Judicial Process* (1963) ..... 8

S. 2685, 113th Cong. (2014) ..... 24

PRELIMINARY STATEMENT

As plaintiff has demonstrated, Pl. Mem. in Supp. S.J., at 1-5, 15-16 (“Pl. Br.”), ECF No. 17, the Attachment to the National Security Letter (“NSL”) issued in 2004 identifies the types of materials the FBI considers to fall within its statutory authority to secretly collect “electronic communications transactional records” (“ECTR”). The Attachment thus reveals key information about the FBI’s claimed authority to gather data about citizens’ digital lives without individual suspicion, without prior judicial review, and with scant prospect of subsequent review. By forbidding plaintiff from describing the Attachment, the FBI suppresses debate over the accuracy of its interpretation of the NSL statute and the propriety of the broad authority it now exercises.

Citizens today cannot help but leave detailed digital traces that paint intimate portraits of their lives. Whether and how easily the government should be able to inspect these digital biographies is a matter of significant policy, legislative, and constitutional debate. But for that debate to be meaningful, it is essential to understand the NSL authority that the government currently believes to exist and routinely exercises in secret. Indeed, Congress just amended the NSL statute by enacting the USA FREEDOM Act, even while the public remained in the dark as to what the FBI believes the statute already authorizes. Because of the gag order, plaintiff could not inform the public about the FBI’s interpretation, which goes well beyond what a reasonable person would anticipate based on the statute’s text and the government’s public assurances.

In opposition, the government concedes that it is not barring plaintiff from discussing the Attachment to protect the investigation underlying the 2004 NSL, *or any other specific ongoing investigation*. Instead, it contends that disclosure would reveal law enforcement “techniques and procedures.” But the Attachment does not reveal “techniques and procedures” (*i.e., how* the FBI uses its lawful authority); it reveals *what* authority the FBI believes the statute grants. This is a

vitality important distinction. The First Amendment does not allow the government to suppress a citizen's speech in order conceal its interpretation of the authority granted by statute—especially where that interpretation defines the government's power to intrude upon the privacy of citizens.

The government's basic argument for continuing without end the extraordinary injunction on plaintiff's speech is that disclosing the Attachment could permit circumvention of future NSLs, but it is no secret that the government can and does obtain the kinds of records demanded in the Attachment using *other* authorities. Disclosing that the FBI considers such records to be available through the use of NSLs cannot reasonably be expected to compromise the FBI's ability to conduct investigations. Anyone truly seeking to conceal certain digital traces is already fully aware that it must do so to evade FBI detection. On the other hand, the law-abiding public remains in the dark about how broadly the FBI may peer into their digital lives by issuing secret NSLs—tens of thousands of which are issued every year. Manes Decl. Ex. F-H, ECF No. 20.

Defendants' opposition also confirms that they will sustain the gag order permanently or, to be more precise, for exactly as long as the FBI wishes to prolong it. Defendants point to no circumstances that might ever render the current gag order obsolete under its rationale for imposing it. For First Amendment purposes, the gag order is indeed "permanent" and, for this reason as well, plainly impermissible. After eleven years, this Court should set aside this prohibition on important speech about a matter of great public concern.

### ARGUMENT

#### **I. THE FIRST AMENDMENT DOES NOT ALLOW THE FBI TO INDEFINITELY SUPPRESS SPEECH ABOUT THE SCOPE OF ITS STATUTORY AUTHORITY.**

The government seeks to justify the gag order as necessary to prevent circumvention of law enforcement techniques, but the impact of the gag order, more accurately, is to suppress discussion about the scope of the government's authority. The First Amendment does not permit



restraints on speech that have this purpose or effect, nor does it permit gag orders that are *de facto* permanent. The First Amendment is equally explicit in prohibiting the government from maintaining the gag order with respect to information that is already in the public domain.

**A. The Gag Order Suppresses Discussion of the Government's Interpretation of Its Statutory Authority, not Law Enforcement Techniques and Procedures.**

As shown, the gag order forbids speech about the government's legal interpretation of the NSL statute, Pl. Br. 1-5, 15-16. Defendants acknowledge that the Attachment reveals "the types of information the FBI can obtain through the NSL mechanism concerning the user of an e-mail account." Gov't Br. 16, ECF No. 25. But to avoid the implication that the gag serves to maintain secret law, they seek to recast the Attachment as describing "techniques and procedures" whose "disclosure would compromise their usefulness" *Id.* 17. This effort fails.

1. *The Attachment Reveals the Scope of the Government's Claimed Authority, Not "Techniques and Procedures."*

The gag order prevents Mr. Merrill from speaking about *what* the government believes it can lawfully do—not whether, how, when, or why the government may choose to deploy such authority. Indeed, plaintiff has no insight into how the government uses NSLs to conduct investigations *in general*. Plaintiff only seeks to disclose what he knows: that the FBI has interpreted the NSL statute to allow it to obtain the kinds of records listed in the Attachment.

The government has no effective responses to the straightforward observation that the gag suppresses disclosure of its interpretation of law. It contends that plaintiff's position "proves too much" because any disclosure about "what the government does can be described as information about what the government believes it can do." *Id.* 12. The government is incorrect. The current case presents concerns about secret law that simply do not arise in other cases involving "techniques and procedures." Here, unlike the typical case, the public is unaware that the government even has the authority to engage in the specific activity the Attachment reveals—

the scope of the government's NSL authority is secret, not merely the manner in which it exercises that authority. Moreover, whether the NSL statute actually permits the kinds of data collection revealed in the Attachment is not obvious on the face of the statute and is a matter of significant legal doubt. See Pl. Br. 4 & n.1; *infra* 9-11 (discussing legal infirmities of the government's interpretation). The gag order thus serves to perpetuate public ignorance as to the meaning of a statute. Contrary to the government's assertion, it is not the case that all secrets about "what the government does" raise this concern about "what the government can do."

Indeed, in all of the gag order cases the government cites, which relate to grand jury and other confidential investigatory proceedings, there was no doubt that the government had the *legal authority* to do that which was gagged, and so the gags implicated no concerns about secret legal interpretations. See Gov't Br. 12 (citing cases).<sup>1</sup> In fact, the cases the government relies on regarding protection of "techniques and procedures" illustrate the distinction that plaintiffs draw here, between concealing *how* the government exercises its lawful authority to conduct investigations and concealing *that* the government claims certain authority in the first place. None of the cases cited by the government protects the secrecy of the latter. Gov't Br. 18-19.<sup>2</sup>

If anything, it is not the plaintiff's position that "proves too much," but the government's. If the Attachment can be withheld on the grounds that its disclosure would reduce the

---

<sup>1</sup> *Kamasinski v. Judicial Review Council*, 44 F.3d 106, 111 (2d Cir. 1994) (investigation of judicial misconduct); *First Am. Coal. v. Judicial Inquiry & Review Bd.*, 784 F.2d 467, 479 (3d Cir. 1986) (en banc) (same); *Hoffmann-Pugh v. Keenan*, 338 F.3d 1136, 1140 (10th Cir. 2003) (grand jury proceedings).

<sup>2</sup> *Frankel v. SEC*, 460 F.2d 813, 817 (2d Cir. 1972) (files would reveal how SEC conducted its investigations); *Weisberg v. DOJ*, 489 F.2d 1195, 1199 (D.C. Cir. 1973) (withholding results and analysis from use of a forensic technique that itself was not secret); *In re City of New York*, 607 F.3d 923, 944 (2d Cir. 2010) (withholding "field reports" that "contain[ed] detailed information about undercover operations of the NYPD"); *Nat'l Cong. for P.R. Rights ex rel. Perez v. City of N.Y.*, 194 F.R.D. 88, 95 (S.D.N.Y. 2000) (documents describing "plans for deployment" and other details of how deployed stops-and-frisks); *Borchers v. Commercial Union Assur. Co.*, 874 F. Supp. 78, 80 (S.D.N.Y. 1995) (files privileged because they revealed "the scope of the criminal investigation, as well as the identity and substantive testimony of various witnesses interviewed"); *Black v. Sheraton Corp.*, 564 F.2d 531, 546 (D.C. Cir. 1977) (disclosing surveillance technique and fruits thereof, but withholding unrelated investigatory files).

effectiveness of investigations by disclosing that the FBI has the authority to engage in certain kinds of surveillance, then the government would be equally justified in concealing much of the law of search and seizure. After all, disclosing to criminals that the government is able to obtain access to, say, cell-site location data using any given statutory authority may well “reveal[] to current and future subjects of investigations . . . the ways in which the FBI uses” the particular statutory authority “and the types of information the FBI can obtain” using such authority; such disclosure could also “expose what information the FBI deems important” in a particular kind of investigation. Gov’t Br. 16 (quoting government’s reasons for suppressing NSL Attachment). But in this country members of the public who learn of law enforcement activities are free to publicize them and, in the appropriate case, to challenge them. *See, e.g., infra* 7-8 & nn.5-6 (describing public disclosures and decisions adjudicating lawfulness of surveillance techniques).

In any event, it is not the case that the Attachment reveals how the FBI conducts its investigations *in general*, or discloses what its investigatory tactics are *in general*, which is the harm that the FBI must establish given that the 2004 investigation underlying the NSL is closed. *See* Defs’ Rule 56.1(b) Stmt. ¶ 25. Indeed, the Attachment does not reveal why the FBI decided to use an NSL in the underlying investigation, or why it sought to obtain the particular categories of records listed in the Attachment, or what it planned to do with that information.<sup>3</sup> Moreover, the FBI acknowledges that it has since changed the form of the NSLs it uses, Perdue Decl. ¶ 72, and nowhere does the FBI contend that it uses NSLs in precisely the same circumstances as it did in 2004, *id.* In fact, [REDACTED]

[REDACTED] the NSL statute as

<sup>3</sup> *See* Manes Decl., Ex. E, at 6 (“The NSL is an unclassified document because it does not detail the specific relevance of the request record to an authorized FBI investigation.”). The details of the underlying investigation that gave rise to the 2004 NSL are not public. The portions of the Perdue Declaration describing the investigation were filed under seal. *See* ECF No. 30.

was revealed in the 2004 Attachment. *Id.* Disclosing the Attachment would therefore reveal little or nothing about *how* the government uses NSLs today to conduct particular investigations. It would instead reveal only *what* the government believes the statute authorizes. There is no compelling or constitutionally legitimate interest in suppressing the latter. *See infra* 7-14.

2. *The Breadth of the Gag Order Can Be Explained Only by a Concern With Maintaining a Secret Interpretation of the NSL Statute.*

The scope of the gag order the government defends is not consistent with an interest in protecting the effectiveness of “techniques,” but can be explained only as a means to keep the public in the dark about the scope of its claimed authority to conduct ECTR surveillance using NSLs. In particular, the FBI continues to gag Mr. Merrill with respect to a category of records—  
[REDACTED]—that it concedes it is not currently gathering using NSLs, but which it claims the law authorizes it to collect.

Category Two in the Attachment requests information from [REDACTED] and the Perdue Declaration confirms [REDACTED]  
[REDACTED]  
[REDACTED] The government explains that “as matter of policy” the FBI no longer seeks such information, but that it still interprets the NSL statute to allow it. Perdue Decl. ¶ 59(a).

The government contends that the gag on this disused—but not abandoned—legal authority is justified because disclosure “may provide individuals foreknowledge” about a method that “the Attorney General might someday . . . allow the FBI” to resume using. *Id.* This supposed harm is utterly speculative; the public’s right to know the extent of the claimed authority is not. The government provides no reason to believe that it [REDACTED] in the foreseeable future, and it concedes that no current, planned, or foreseen investigations would be

affected by disclosure. Moreover, it is no secret that the FBI [REDACTED] in other ways. *See infra* 21-22 & n.15. Continuing the gag on this portion of the Attachment serves only to hide that the Government interprets ECTR [REDACTED]. In short, the gag order is tailored to conceal a legal interpretation, not to protect an FBI “technique.”

**B. The Gag Order Unconstitutionally Suppresses Discussion of the Legal Interpretation of a Statute that Directly Affects the Rights of Citizens.**

Even if the Court accepts the government’s claim that the gag order serves an interest in protecting a law enforcement method, it is undeniably true that the gag order *also* serves to maintain a secret interpretation of law, *supra* 3-6. As plaintiff has already demonstrated, Pl. Br. 15-17, the First Amendment forbids gag orders whose purpose or effect is to maintain secret law.

1. *The First Amendment Does Not Permit Gag Orders Whose Purpose or Effect Is to Maintain Secret Interpretations of Law.*

The gag order at issue presents a particularly acute secret law problem. It is aberrational that an interpretation of law affecting the rights of citizens would be kept secret from the public in the first place. Previous examples of such secret law have all pertained to highly classified national security programs. *See, e.g., N.Y. Times v. DOJ*, 756 F.3d 100 (2d Cir. 2014) (disclosing legal basis for targeted killing of citizen); *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, 2014 WL 5442058 (For. Intel. Surv. Ct. Aug. 7, 2014) (declassifying opinions regarding bulk collection under Section 215). It is rarer still—perhaps unprecedented—that the government seeks to maintain a secret interpretation of law not by enforcing information controls among government employees and contractors who have signed nondisclosure agreements and consented to the classification system, but by enforcing gag orders on private citizens who have not agreed to keep the government’s secrets and who did not even set out to learn them. Moreover, the government is insisting on secrecy in this case for

reasons that do not relate to a specific investigation, but in order to maintain the secrecy of the program *in general*. The First Amendment does not allow such prohibitions on speech.

In every analogous situation to the present circumstance, courts have affirmed the hostility of the First Amendment and other sources of law to secret rules governing citizens. For instance, the public's ability to access judicial decisions that interpret and elaborate the law lies at the very core of the First Amendment and common law rights of access to courts.<sup>4</sup> Indeed, courts have routinely published opinions construing the government's authority to gather information about U.S. citizens under various surveillance laws.<sup>5</sup> This is true even with respect to intelligence collection for national security purposes.<sup>6</sup>

Where, as here, access to secret law is not premised upon the qualified First Amendment right of access, but rather the core right to speak, it is even clearer that any government interest in maintaining secret interpretations of law must yield to the First Amendment. *See First Am. Coal.*, 784 F.2d at 477 ("The claim . . . is based on the broader right of free speech, not simply access. Consequently, we must be less deferential to state interests.").

<sup>4</sup> *See, e.g., Lowenschuss v. W. Pub. Co.*, 542 F.2d 180, 185 (3d Cir. 1976) ("Even that part of the law which consists of codified statutes is incomplete without the accompanying body of judicial decisions construing the statutes. Accordingly, under our system of jurisprudence the judiciary has the duty of publishing and disseminating its decisions.") (quoting Benjamin N. Cardozo, *The Nature of the Judicial Process*, 20, 21-22 (1963)); *Scheiner v. Wallace*, No. 93-cv-0062, 1996 WL 633226, at \*1 (S.D.N.Y. Oct. 31, 1996) ("The public interest in an accountable judiciary generally demands that the reasons for a judgment be exposed to public scrutiny." (citing *United States v. Amodeo*, 71 F.3d 1044, 1048-49 (2d Cir. 1995))).

<sup>5</sup> *See, e.g., In re Application of N.Y. Times Co. for Access to Certain Sealed Court Records*, 585 F. Supp. 2d 83, 88 (D.D.C. 2008).

<sup>6</sup> *See, e.g., In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, 2014 WL 5442058 (Foreign Intel. Surv. Ct. Aug. 7, 2014) (ordering government to declassify opinions of the FISC interpreting Section 215 of the Patriot Act); *United States v. U.S. Dist. Court for the E. Dist. of Mich.*, 407 U.S. 297 (1972) (considering constitutionality of warrantless-wiretapping program conducted by the government to "protect the national security"); *United States v. Duggan*, 743 F.2d 59, 72-74, 77 (2d Cir. 1984) (analyzing FISA's original "purpose" requirement, and holding that "FISA does not violate the probable cause requirement of the Fourth Amendment"); *Jewel v. Nat'l Sec. Agency*, 673 F.3d 902, 905 (9th Cir. 2011) (reversing dismissal of lawsuit challenging "widespread warrantless eavesdropping in the United States"); *In re Application for Pen Register & Trap/Trace Device with Cell Site Location Auth.*, 396 F. Supp. 2d 747, 748-49 (S.D. Tex. 2005) (refusing government request to seal opinion "because it concerns a matter of statutory interpretation" and the issue explored "has serious implications for the balance between privacy and law enforcement, and is a matter of first impression").



The law's hostility to secret rules is also manifest in other provisions of the Constitution, and in the courts' interpretation of relevant statutory law. For instance, it is a bedrock principle of Due Process that individuals must have notice of what the law is before being subjected to deprivations of life, liberty or property. *See, e.g., Papachristou v. Jacksonville*, 405 U.S. 156, 162 (1972) ("Living under a rule of law entails various suppositions, one of which is that all persons are entitled to be informed as to what the State commands or forbids.") (internal quotation and alteration omitted). In the statutory FOIA context, the Second Circuit has recognized that "secret law is an abomination." *Caplan v. ATF*, 587 F.2d 544, 548 (2d Cir. 1978) (quotation omitted). The Supreme Court and lower courts have interpreted FOIA to prevent the government from withholding authoritative interpretations of law. *See, e.g., NLRB v. Sears*, 421 U.S. 132, 153-54 (1975) (secret law cannot be withheld under Exemption 5); *Brennan Ctr. for Justice v. DOJ*, 697 F.3d 184 (2d Cir. 2012) (same); *Crooker v. ATF*, 670 F.2d 1051, 1073 (D.C. Cir. 1981) (government can withhold law enforcement techniques only if the material does not constitute "'secret law' of the agency," and instead is "used for predominantly internal purposes"), *abrogated on other grounds, Milner v. Dep't of the Navy*, 562 U.S. 562 (2011).

2. *The Gag Order Has the Effect of Impeding Democratic Oversight of the Scope and Lawfulness of the Government's Claimed Authority.*

The government's effort to suppress the Attachment illustrates many of the particular evils of secret law. By preserving the secrecy of the FBI's interpretation, the gag order deprives citizens of their democratic prerogative to know what the law empowers their government to do. It prevents citizens from determining whether the law, as interpreted, should be modified. And it makes it impossible to advocate for effective changes to the law. In this case the situation is particularly troubling because the public has arguably been misled about how the NSL statute has been interpreted by the FBI. Because of the gag order, the accuracy of the government's

public pronouncements cannot be challenged. Moreover, serious questions about the very lawfulness and constitutionality of the FBI's interpretation cannot be aired publicly and debated.

The government's public statements regarding its interpretation of the NSL statute's ECTR provision are arguably misleading in at least two ways. First, as plaintiff has previously noted, Pl. Br. 4 n.1, a formal opinion issued by the Department of Justice states that the FBI's authority to collect ECTR using NSLs "reaches only those categories of information parallel to subscriber information and toll billing records for ordinary telephone service." Manes Decl. Ex. I, at 3 n.3. But it is very difficult to understand how various categories of records revealed in the Attachment are "parallel to subscriber information or toll billing records." For instance, [REDACTED]

[REDACTED] does not appear to be "parallel to" telephone toll billing records. Yet that type information can be collected using an NSL, as revealed in the Attachment. See Perdue Decl. ¶ 65. It is equally unclear how [REDACTED]

[REDACTED] are analogous to familiar toll billing records. See Perdue Decl. ¶¶ 59, 69.

Second, despite the FBI's public assurances that NSLs cannot be used to obtain the "content" of communications, *see, e.g.*, Perdue Decl. ¶ 11, the Attachment reveals that the FBI has interpreted the ECTR provision to permit collection of records that can and often do contain "content." For example, [REDACTED]

[REDACTED] But the Attachment reveals that [REDACTED]

[REDACTED]  
[REDACTED] Second Declaration of Jonathan Manes, [REDACTED]  
("Second Manes Decl.").



[REDACTED]

[REDACTED] See *Perdue Decl.* ¶ 69.

The gag order prevents plaintiff from correcting the public record on both of these points. As a result, the public has a distorted picture of what the NSL statute actually permits. The gag order also serves to suppress public discussion about the constitutionality of certain aspects of the interpretation that the FBI has adopted. For instance, courts have consistently held that the First Amendment requires the government to meet a much more stringent test than mere “relevance” where it seeks to obtain purchase records regarding books, or other expressive materials.<sup>8</sup> But the Attachment reveals that [REDACTED]

[REDACTED] See *id.* ¶¶ 64-65. There is also considerable doubt whether the First Amendment permits the identity of an anonymous online speaker to be obtained upon a showing of mere “relevance.” See Pl. Br. 5; *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 508-09 (S.D.N.Y. 2004); *cf.* *Perdue Decl.* ¶ 67 ([REDACTED]). It is also doubtful that the Fourth Amendment permits the government to obtain [REDACTED] upon a bare showing of “relevance.”<sup>9</sup> *Cf.* *Perdue Decl.* ¶ 59.

Because of the gag order, these and other specific concerns about how Section 215 has been interpreted could not be raised during the very recent legislative debate regarding the USA

<sup>8</sup> See, e.g., *Amazon.com LLC v. Lay*, 758 F. Supp. 2d 1154, 1167-69 (W.D. Wash. 2010) (“The First Amendment protects a buyer from having the expressive content of her purchase of books, music, and audiovisual material disclosed to the government.”); *In re Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461 et seq.*, 706 F. Supp. 2d 11, 18 (D.D.C. 2009) (“United States may only obtain the records [of purchases of expressive material] if it demonstrates a compelling need for them and a sufficient nexus between the records and the grand jury’s investigation”); *In re Grand Jury Subpoena to Amazon.com*, 246 F.R.D. 570, 572-73 (W.D. Wis. 2007) (same). *Accord Doe v. Ashcroft*, 334 F. Supp. 2d 471, 506-511 (S.D.N.Y. 2004).

<sup>9</sup> Some courts have held that [REDACTED] requires a showing of probable cause. See, e.g., [REDACTED]. Others have upheld [REDACTED] using orders under 18 U.S.C. § 2703(d), which require a court order issued upon a finding of “specific and articulable facts” showing that the information is both “relevant and material.” See, e.g., [REDACTED]. Plaintiff is aware of no court endorsing [REDACTED] upon the issuance of an administrative (rather than judicial) subpoena premised upon mere relevance, as is the case with NSLs.

FREEDOM Act. There is good reason to believe that a more informed public discussion would have led to consideration of additional limits on the scope of NSL authority. *Cf. ACLU v. Clapper*, \_\_\_ F.3d \_\_\_, 2015 WL 2097814, at \*27 (2d Cir. May 7, 2015) (observing that when Congress reenacted Section 215 of the PATRIOT Act in 2011, “there was certainly no opportunity for broad discussion in the Congress or among the public of whether the [secret] interpretation of § 215 was correct,” in contrast with the “widespread controversy that developed, in and out of Congress, upon [its] public disclosure.”).

In enacting the USA FREEDOM Act, Congress recognized the strong parallel between Section 215 of the PATRIOT Act—the principal subject of the Act—and the NSL statute, amending both to limit “bulk collection” by requiring the government to identify a specific person, entity, or other identifier as the target of a request. *See* Pub. L. No. 114-23, §§ 101(a)(3), 103(a)-(b), 501(a), 129 Stat. 268. The Act also amended [REDACTED]

[REDACTED]

[REDACTED] was included in the amendments [REDACTED]

[REDACTED] Had the public known that the FBI believes [REDACTED]

[REDACTED] the issue might have been addressed in both contexts. More broadly, given that NSLs can be issued much more easily than Section 215 orders, which require judicial approval, it seems likely that the FBI’s aggressive interpretation of “ECTR” would have been the subject of significant controversy and debate if it had been public. Because of the gag order, no such controversy was possible.

The gag order serves to conceal an interpretation of the NSL statute that provides the government with broader authority to intrude upon citizens’ digital lives than DOJ’s public statements would suggest, and whose very legality is reasonably disputed. The gag order

prevented this interpretation from being debated even while Congress set about amending the statute. The First Amendment simply cannot tolerate a gag order that has these effects.

**C. The First Amendment Has Never Been Interpreted to Permit Restraints on Speech About Government “Techniques and Procedures.”**

Even if the Attachment could be characterized as revealing “techniques and procedures,” as the government urges, there is no authority in First Amendment law for the proposition that the government can forcibly silence private citizens from speaking about “techniques and procedures” of which they have become aware. The government cannot cite even a single case in which an interest in protecting “techniques and procedures” was sufficient to overcome the First Amendment’s protection of free speech. *See* Gov’t Br. 12, 18-19. Instead, all of the gag orders cited by the government are aimed at maintaining the secrecy of grand jury or similar investigatory proceedings in order to protect the integrity of those proceedings. Gov’t Br. 12.<sup>10</sup>

In the absence of support in First Amendment law, the government resorts to a grab-bag of cases interpreting FOIA exemptions and the evidentiary privilege for law enforcement techniques. Gov’t Br. 18-19. But, as noted, these cases in fact illustrate the distinction that plaintiffs draw here between concealing *how* the government exercises its lawful authority and concealing *that* the government claims certain authority in the first place. *See supra* 4 & n.2.

While the government concedes that FOIA and the law enforcement privilege are not directly applicable in this context, it nonetheless urges that “their principles . . . still pertain.” Gov’t Br 19. To the contrary, those principles are inapposite. FOIA cases, which concern the scope of the government’s right to *withhold* information from citizens in the face of a request to

---

<sup>10</sup> Citing *Kamasinski*, 44 F.3d at 111 (permitting restraint forbidding complainant or witnesses from discussing investigation while it was ongoing); *First Am. Coal.*, 784 F.2d at 479 (permitting restraint forbidding disclosure of other witnesses’ testimony in investigatory proceeding akin to a grand jury); *Hoffmann-Pugh*, 338 F.3d at 1140 (permitting restraint forbidding disclosure of what transpired at grand jury until investigation is “truly closed”).

disclose it, have no bearing on the situation where a citizen possesses information and the government seeks to suppress it. *See, e.g., Wright v. F.B.I.*, 613 F. Supp. 2d 13, 24 (D.D.C. 2009) (“[T]he Government has cited to no case holding that FOIA is coterminous with the First Amendment.”). Even in cases where the First Amendment rights at stake were much weaker than those here, courts have declined to conflate FOIA and the First Amendment. *Id.* at 24 (rejecting weaker FOIA standards in First Amendment lawsuit challenging redactions of book written by former government employee who had consented to prepublication review by government censors); *McGehee v. Casey*, 718 F.2d 1137, 1148-49 (D.C. Cir. 1983) (same).

Similarly, the law of privilege is of no relevance because the question here is not whether the government can *resist disclosure* sought by a private citizen for purposes of litigating a civil suit, but whether the government can *suppress discussion* of information that it has voluntarily provided to a private citizen. The latitude afforded the government will obviously be broader in the former context, which is not inflected with First Amendment concerns. But even in the discovery context, the law enforcement privilege is “qualified” and can be overcome where “a lawsuit involves a matter of public concern such as civil rights—a factor that will usually support disclosure.” *Floyd v. City of New York*, 739 F. Supp. 2d 376, 381 (S.D.N.Y. 2010).

Simply put, a government interest in maintaining the secrecy of “techniques and procedures” is insufficient to justify a prior restraint barring a private citizen from discussing matters of public concern when he has not voluntarily assumed a duty of confidentiality.<sup>11</sup>

---

<sup>11</sup> The government points to this Court’s 2010 decision upholding a gag order on the Attachment as precedent for the proposition that law enforcement techniques may be suppressed. Gov’t Br. 19-20. But at that time there were multiple reasons for maintaining the gag order on the Attachment, including protecting the integrity of the underlying investigation which remained ongoing. *Doe v. Holder*, 703 F. Supp. 2d 313, 316-17 (S.D.N.Y. 2010). Moreover, the Court applied the more lenient standard of review set forth in by the Second Circuit in *John Doe, Inc v. Mukasey*. *See id.* In the context of the present as-applied challenge, more stringent scrutiny is required. *See infra* Part I.F.

**D. The Gag Order is Permanent, and Therefore Unconstitutional, Because Its Duration Now Depends Solely on the Preferences of the Government.**

Plaintiff contends that permanent bans on speech are unconstitutional. Pl. Br. 13-14. The government does not contest that legal proposition but instead argues that the gag on Mr. Merrill is not “permanent” in the constitutionally relevant sense, for two reasons: first, because Mr. Merrill is permitted to annually challenge the gag in court and, second, because of “the FBI’s repeated willingness to reassess and reduce the scope of the nondisclosure requirement in light of changing needs and circumstances.” Gov’t Br. 22-24. These arguments miss the mark.

The cases forbidding permanent gag orders do not merely insist that an individual have the procedural right to periodically return to court. They look to whether the gag order will *in fact* remain in place indefinitely. *See, e.g., Butterworth v. Smith*, 494 U.S. 624, 635 (1990) (gag unconstitutional because “[t]he ban extends . . . into the indefinite future”); *Kamasinski*, 44 F.3d at 112 (after investigation is closed “even [the state’s] most compelling interests cannot justify a ban on public disclosure”); *Doe v. Gonzales*, 449 F.3d 415, 421-23 (2d Cir. 2006) (Cardamone, J., concurring). Whether a gag is permanent thus depends on whether it is tied to circumstances in the world that might change, rendering the gag order obsolete. The only circumstances that the government points to here are the FBI’s preferences, but a gag that lasts precisely as long as the government wishes is just the sort of permanent gag order that the First Amendment forbids.

The government seeks to avoid this conclusion by pointing to the FBI’s “willingness” to progressively lift the gag on Mr. Merrill, but the FBI has hardly been “willing” to reduce the gag, particularly with respect to the Attachment. The scope of the gag on the Attachment was first limited, against the Government’s vigorous protest, by this Court’s 2010 order to unredact portions of in the Attachment that were described verbatim in the NSL statute or that had otherwise been made public by the government. *Doe v. Holder*, 703 F. Supp. 2d 313, 316

(S.D.N.Y. 2010). The parties reached a settlement prior to appeal permitting plaintiff to identify himself, but the gag on the Attachment remained intact for five years with no apparent effort by DOJ to determine whether it could be narrowed.

The government did not change its position until Mr. Merrill undertook the burden of bringing new litigation and filed his motion for summary judgment, pointing out that the government had already disclosed several other categories of records listed in the Attachment years earlier. Pl. Br. 18. In response, the government agreed to lift the gag with respect to some, but not all, of these publicly disclosed categories, and to lift the gag with respect to the phrase “Internet Service Provider (ISP).” Gov’t Br. 14. Far from demonstrating a “willingness to reassess” the gag “in light of changing needs and circumstances,” the government’s new position shows that the duration of the gag order does not depend on “changing circumstances” and is likely to remain in place permanently.

Three aspects of the government’s current position demonstrate that the duration of the gag order is now untethered from any changing circumstances. First, the government contends it can maintain the gag order with respect to categories of records that were described in an official letter from DOJ to Congress that was published in the congressional record. Gov’t Br. 14. The government defends this position on the grounds that the decision to publish the letter was made by Congress, rather than the FBI. *Id.* In other words, even though an official document revealing precisely the information found in the Attachment is now in the public domain, the gag order will remain in place for precisely as long as *the FBI* chooses not to publicly disclose it.

Second, the government has maintained the gag order with respect to categories of records it no longer seeks. *See supra* 6-7. This again demonstrates that the gag is untethered authority from “changing circumstances” and depends simply on the caprice of the FBI.

Finally, in this entire eleven-year saga, the government has voluntarily unredacted a single phrase in the Attachment. Gov't Br. 14; Perdue Decl. ¶ 57.<sup>12</sup> But in so doing the government pointed to no "changing circumstances" that justified its change of heart. Indeed, the FBI offered no reason at all why it changed its position, or why it did so only now. *Id.*; Perdue Decl. ¶ 57. Lifting the gag, in the FBI's view, was simply an exercise of executive grace. But a gag that will remain in place indefinitely, subject only to the government's whim, is the very essence of a permanent restraint forbidden by the First Amendment.

**E. The First Amendment Does Not Permit Gag Orders on Private Citizens With Respect to Information That Is in the Public Domain.**

The government refuses to allow Mr. Merrill to speak about categories in the Attachment that are already in the public domain. It prohibits Mr. Merrill from discussing Category Eleven

[REDACTED] even though a DOJ report discloses that NSLs are used to obtain "billing records and methods of payment." Gov't Br. 14; Manes Decl. Ex. K, at 10. It insists Mr. Merrill not discuss Category Ten— [REDACTED]

[REDACTED] in a DOJ letter to Congress describing the use of NSLs. Gov't Br. 14; Manes Decl. Ex. J. The First Amendment does not allow gag orders that in this way suppress speech about matters that are already in the public domain. *See, e.g., Neb. Press Ass'n v. Stuart*, 427 U.S. 539, 596-98 (1976); *Cox Broad. Corp. v. Cohn*, 420 U.S. 469, 491 (1975); *In re Charlotte Observer*, 921 F.2d 47, 50 (4th Cir. 1990) (gag order unjustified once "the cat is out of the bag"); *Bank Julius Baer & Co. Ltd v. Wikileaks*, 535 F. Supp. 2d 980, 985 (N.D. Cal. 2008).

<sup>12</sup> The Perdue Declaration also claims to "concede" that the phrase "account number" can now be disclosed. But this Court ordered the FBI to disclose that phrase in 2010, and it has been public ever since. *See Doe v. Holder*, 703 F. Supp. 2d at 316; Merrill Decl. Ex. C. Defendants do not explain the apparent error. Gov't Br. 14.



Attempting nevertheless to justify a gag on public domain information, the government invokes the test for “official disclosure” of classified information, developed in FOIA cases. Gov’t Br. 14. That test determines when the government has forfeited its power to keep information classified. *See Wilson v. CIA*, 586 F.3d 171, 186 (2d Cir. 2009). Of course, the Attachment is not classified. But, more importantly, the test has no bearing on the free speech rights of private citizens. The principal case upon which the government relies, *Wilson v. CIA*, concerned the right of a former government employee to publish classified information even though she had signed away her right to do so in a nondisclosure agreement. *Id.* at 183, 192-93. *Wilson* explicitly distinguished cases like this one, observing that “when a government employee ‘voluntarily assume[s] a duty of confidentiality, governmental restrictions on disclosure are not subject to the same stringent standards that would apply to efforts to impose restrictions on unwilling members of the public.’” *Id.* (quoting *United States v. Aguilar*, 515 U.S. 593, 606 (1995)). Plaintiff has not voluntarily assumed any duty of confidentiality, and he cannot be prohibited from discussing the contents of the Attachment that are now in the public domain.<sup>13</sup>

**F. The “Good Reason” Standard of *John Doe, Inc. v. Mukasey* Is Not Appropriate in the Circumstances of This As-Applied Challenge.**

In the context of this as-applied challenge, the First Amendment requires the Court either to invalidate the remaining gag order outright (because it conceals secret law and is a permanent ban on speech) or, at a minimum, to apply strict scrutiny. But the government contends that it need only meet the “good reason” standard of *John Doe Inc.*, arguing that plaintiff

---

<sup>13</sup> While the official disclosure doctrine does not apply here, plaintiff notes that the Second Circuit recently clarified the test, holding that “the ‘matching’ aspect of the *Wilson* test” does not require “absolute identity.” *New York Times Co. v. U.S. Dep’t of Justice*, 756 F.3d 100, 120 & n.19 (2d Cir. 2014). Nevertheless, the government insists on just this kind of precise match, arguing that the Attachment’s reference to [redacted] billing [redacted] is not officially disclosed despite an official DOJ report stating that NSLs are used to obtain “billing records and all methods of payment.” Gov’t Br 14. The FBI also identifies no harm that would result if plaintiff were able to speak about the portions of the Attachment that were described in the DOJ letter printed in the Congressional Record.



misunderstands the distinction between facial and as-applied challenges, and that the same legal standard must apply in both contexts. Gov't Br. 21 (citing *Brooklyn Legal Servs. Corp. v. Legal Servs. Corp.*, 462 F.3d 219 (2d Cir. 2006)). It is the government that misunderstands the distinction. In the context of the facial challenge decided by *John Doe, Inc.*, the Second Circuit held only that the NSL gag order provisions could, at least in *some* circumstances, be applied constitutionally if the statute were interpreted to require the government to demonstrate a "good reason." *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 876 (2008). As a facial challenge, *John Doe, Inc.* could not have held that *every* application of the gag provision would be constitutional upon a showing of "good reason," and in the present case, the Constitution is more demanding.

As the Second Circuit explained in *Brooklyn Legal Services*, even after a facial challenge is decided, a plaintiff remains free to bring an as-applied challenge to show that a statute "will, in the case of some recipients, prove unduly burdensome and inadequately justified." 462 F.3d at 29 (quotation omitted). Because the as-applied challenge in *Brooklyn Legal Services* was "in all relevant respects, on all fours with its facial counterpart," the legal rule developed in a prior facial challenge applied without modification. *Id.* at 228. The circumstances of the gag order today are not "on all fours" with those considered in *John Doe Inc.* Unlike in 2008, the gag order now serves *only* to protect a secret interpretation of law—or, according to the government, "techniques and procedures"—and does not protect any particular ongoing investigation.

Moreover, the duration of the gag is now untethered from any investigation and depends solely on the government's whims. *See* Pl. Br. 13-14. Contrary to the government's assertion, Gov't Br. 20-22, 25, the Second Circuit did not incorporate these considerations when it crafted the "good reason" standard; none of these circumstances existed at that time, and so the court

had no need to address them. On the current facts, the First Amendment requires that the gag be set aside, or at least that the government bear the burden of justifying it under strict scrutiny.

**II. THE GOVERNMENT FAILS TO ESTABLISH THAT ALLOWING PLAINTIFF TO SPEAK WOULD RESULT IN ANY HARMS.**

The government's posited justification for suppressing the Attachment is speculative, conclusory, and ultimately implausible. It cannot satisfy strict scrutiny or even the attenuated *John Doe, Inc.* standard. While the government's brief invokes a vague but ominous specter of harm to "national security," Gov't Br. 11, the precise harm the FBI articulates in its declaration is more concrete: "Individuals may not be aware law enforcement officials can obtain [the suppressed categories of] information during the course of an authorized investigation," so "[d]isclosure of the language in the NSL attachment" could allow individuals to "avoid law enforcement detection when planning or committing criminal, counterintelligence or terrorism activities." Perdue Decl. ¶ 58. The government repeats this justification, often verbatim, with respect to every suppressed category of the Attachment. *Id.* ¶¶ 55, 56, 59-70.<sup>14</sup>

This justification fails because its premise is false: individuals in fact *are* aware that law enforcement can obtain the categories of information described in the Attachment. The FBI's specific interest in the categories of records described in the Attachment is public and easily ascertained. As a result, individuals seeking to evade detection by the FBI already know to avoid creating such records. In truth, the only thing the government is keeping secret is that it can and does obtain this kind of information *using an NSL*, as opposed to other authorities. But that

---

<sup>14</sup> The FBI's declaration recites the same rationale when justifying the gag order on Category Seventeen—*i.e.* "Any other information which you consider to be an electronic communications transaction record." Perdue Decl. ¶ 70. But that portion of the Attachment is not currently redacted, and has been public since 2009. *See* Merrill Decl. Ex. C; Exhibit A to Mem. in Supp. of Pltfs' Mot. for Partial Reconsid'n, *John Doe, Inc. v. Holder*, No. 04-cv-2614 (S.D.N.Y. filed Nov. 3, 2009) (Attachment as it was then required to be redacted). That the FBI's declaration asserts this justification, under oath, in circumstances where it clearly does not apply suggests a lack of careful consideration and invites some skepticism when the government asserts the same boilerplate rationale with respect to the still-gagged portions of the Attachment. *See also supra* 17 n.12.

information is irrelevant to a person seeking to evade the FBI, who does not care what tool the FBI uses to obtain certain kinds of records, but only whether it does so.

Potential targets of FBI investigations already know, if they care to learn, that the Government has a particular interest in the categories of records described in the Attachment. For example, DOJ guidance regarding the Stored Communications Act (“SCA”) makes clear that the government routinely requires disclosure of (1) “subscriber names, user names, screen names, or other identities;” (2) “addresses,” including mailing, residential, business, and email, and “other contact information;” (3) “length of service (including start date) and types of service utilized;” (4) “telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address;” (5) “means and source of payment for such service (including any credit card or bank account number);” (5) “billing records;” (6) “records of user activity for any connections made to or from the account;” (7) “Internet Protocol addresses;” (8) “cell site and sector information;” (9) “non-content information associated with the contents of any communication or file stored by or for the account;” and (10) “correspondence and notes of records related to the account.” Manes Decl. Ex L, at 222-23; 18 U.S.C. § 2703(c)(2). [REDACTED]

[REDACTED]

[REDACTED] See Perdue Decl. [REDACTED]

Other examples abound. The FBI suppresses the fact that it can obtain Category 2 [REDACTED] [REDACTED] using an NSL, even while it publicizes its interest in obtaining this information under other authorities. We know this because, among other things, DOJ has said so in a training manual, and because individuals have challenged the constitutionality of obtaining this

information.<sup>15</sup> We know that the FBI has an interest in obtaining Category 16 [REDACTED] for the same reasons.<sup>16</sup> *See also supra* 17 (pointing out that DOJ correspondence published in the Congressional Record directly reveals Category 10 [REDACTED]).

Individuals seeking to evade detection thus already know that the categories of records described in the Attachment can be obtained by—and are of interest to—the FBI. Such individuals therefore can already devise and take measures to avoid detection using these methods, if they are so inclined. Disclosing the remainder of the Attachment will not provide additional insight permitting additional circumvention. The gag order therefore does not advance the interest the government claims to be serving: protecting the effectiveness of an investigatory tool. *See* Gov't Br. 16. For this reason, it fails strict scrutiny. *See, e.g., Neb. Press Ass'n*, 427 U.S. 539, 569 (1976) (government must demonstrate, to a high degree of certainty, that “restraining order actually entered would serve its intended purpose.”). Indeed, it fails even the less stringent standard set forth in *John Doe, Inc.* 549 F.3d at 875 (government must demonstrate “reasonable likelihood” that an enumerated harm will result).

### III. THE NSL STATUTE DOES NOT AUTHORIZE THE PRESENT GAG ORDER.

The best reading of the NSL statute does not allow permanent gag orders or suppression of legal interpretations. Pl. Br. 21-24. Gag orders may only be issued against the recipient of an NSL request, and such requests can only be issued to obtain information “relevant to an authorized investigation.” 18 U.S.C. § 2709(b)(1). The gag order provision forbids disclosure of the fact that “the [FBI] has sought or obtained access to information or records under this section,” and enumerates four harms that can justify a gag order, which are recited again in the

<sup>15</sup> *See, e.g.,* Second Manes Decl., [REDACTED] 159-61; [REDACTED]

<sup>16</sup> *See* Second Manes Decl. [REDACTED]

judicial review provision, §§ 2709(c)(1), 3511(b)(3). Read together, these provisions are best understood to require that the enumerated harms must have a nexus with the particular “authorized investigation” that prompted the NSL. *See* Pl. Br. 21-24.<sup>17</sup>

The government disagrees, arguing that harm to *any* investigation—or danger to “national security” writ large—suffices to sustain a gag beyond the end of the particular investigation. Gov’t Br. 17-18. In support, the government relies heavily on this Court’s 2010 decision upholding part of the gag on the Attachment. *Id.* 19 (citing *Doe*, 703 F. Supp. 2d 313). The government is mistaken. While this Court found that disclosure could plausibly result in a statutorily enumerated harm, it was careful to limit its holding to situations where the underlying investigation was ongoing. “For instance,” the Court wrote, “disclosure of the Attachment could risk providing information useful to the Government’s targets of *the* pending investigation that could prompt changes in their behavior to prevent detection, or signal that *particular* targets remain under active surveillance.” 703 F. Supp. 2d at 317 (emphasis added). While the Court did note the government’s concern that disclosure could “potentially [inform] future targets,” that was not the basis for the Court’s decision sustaining the nondisclosure order. *Id.* at 316.<sup>18</sup>

Had Congress wanted to authorize permanent gag orders regarding the FBI’s interpretation of the scope of its authority under the statute, it would have spoken far more clearly when it amended the nondisclosure provisions earlier this month. Instead, three pieces of

---

<sup>17</sup> The USA FREEDOM Act amended § 2709 and § 3511 in a number of respects, but did not change the enumerated harms specified in §§ 2709(c)(1) and 3511(b)(3), now codified at §§ 2709(c)(2) and 3511(b)(3), nor did it change their relationship with the substantive authority to issue NSLs in connection with an “authorized investigation.” Pub. L. No. 114-23, § 502(a), (g). To avoid confusion, citations to the U.S. Code refer to the unamended text. Recent amendments are cited to the enrolled bill, Pub. L. No. 114-23.

<sup>18</sup> The best reading of the statute requires harm to *the* particular investigation that gave rise to the gag order itself, but at the very least, the government must show a harm to *a* particular investigation. The government fails to meet even that lower bar, arguing instead that it may, for example, continue to prevent disclosure that it once sought [redacted] on the basis that it may, hypothetically, seek such information in the future. *See supra* 6-7.

evidence strongly suggest that Congress intended to reject the notion that gag orders can continue indefinitely to suppress the information revealed by the Attachment. First, Congress imposed upon the government an affirmative obligation to periodically review gag orders to “assess whether the facts supporting nondisclosure continue to exist.” Pub. L. No. 114-23 § 503(f)(1)(A). This strongly suggests that Congress believes that the “facts” can indeed change so as to obviate the need for the gag. *Cf. supra* § I.D (arguing that gag has become untethered from any facts save for government preferences). Second, an earlier version of the bill contained a provision that would have relieved the government of its obligation to periodically review the need for a gag order if, following the close of an investigation, a court upheld the gag order. S. 2685 sec. 502(a), § 2709(c)(3)(B), 113th Cong. (2014). That provision would have condoned precisely the kind of permanent gag order that the government seeks here. But Congress rejected that provision, opting instead to require periodic governmental review of gag orders, without regard to whether the investigation remains pending. Pub. L. No. 114-23 § 503(f). Finally, the USA FREEDOM Act amends the judicial review provision to adopt procedures that clearly contemplate that gag orders will end. As amended, § 3511 requires the government to come to court to justify the imposition of a nondisclosure order and any “extension thereof” whenever the NSL recipient “notif[ies] the Government” that he “wishes to have a court review a nondisclosure requirement.” Pub. L. No. 114-23 § 502(g) (to be codified at 18 U.S.C. § 3511(b)(1)(A)-(B)). The amendment thus contemplates that nondisclosure orders will be time limited, subject to re-review by the Court on applications for “extensions.” This goes well beyond the holding in *John Doe, Inc.*, which required the government to initiate judicial review only once immediately following receipt of the NSL, and arguably allowed gag orders to remain in place indefinitely thereafter, unless challenged again by the NSL recipient. 549 F.3d at 883-

84. In adopting this provision, Congress registered its disagreement with the Second Circuit's supposition that "once the need for secrecy—avoiding risk of harm related to international terrorism—has been shown, that need is not likely to dissipate soon." *Id.* at 884 n.16.

Indeed, the best way to understand Congress' recent action is to construe the statute to forbid gag orders that indefinitely suppress discussion of the FBI's use of NSLs. By adopting an interpretation that requires a nexus with the particular underlying investigation (or otherwise disallows indefinite suppression of the FBI's interpretation of the law), this Court can effectuate Congress' intent and also avoid adjudicating the grave constitutional infirmities that plague the nondisclosure order here. *See supra*; Pl. Br. 25. If Congress means to empower the FBI to press the limits of the First Amendment as far as it does today, it should speak more clearly than it has.

**IV. IF THE COURT UPHOLDS THE GAG ORDER, IT SHOULD DO SO ONLY FOR A LIMITED PERIOD OF TIME.**

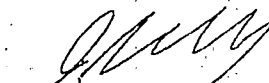
Should the Court decide not to lift the entire gag order, it should specify a date certain on which the gag will expire unless the government reinitiates proceedings to further extend the order. *See* Compl. ¶ 43. While plaintiff recognizes that the Second Circuit wrote, in *dicta*, that the government "would not be obligated to [re]initiate judicial review," 549 F.3d at 884, that statement was ill-considered in light of the First Amendment prohibition on restraints that extend longer than necessary, *e.g.*, *United States v. Antar*, 38 F.3d 1348, 1362 (3d Cir. 1994) ("Under the First Amendment, once an overriding interest initially necessitating closure has passed, the restrictions must be lifted.") (citations omitted). In any case, the recent amendments to § 3511 require the government to periodically review the continuing need for a nondisclosure order, Pub. L. No. 114-23, § 502(f), and to apply to a court when necessary to obtain an "extension thereof," § 502(g); *supra* 24. Thus, even if the Court were to find that the gag remains justified today, it should give effect to the recent amendments by setting an expiration date.



**CONCLUSION**

For these reasons, the Court should lift the nondisclosure order on plaintiff in its entirety.

Respectfully submitted,



---

Jonathan Manes, supervising attorney  
David A. Schulz, supervising attorney  
Benjamin Graham, law student intern  
Matthew Halgren, law student intern  
Nicholas Handler, law student intern  
Amanda Lynch, law student intern  
MEDIA FREEDOM AND INFORMATION  
ACCESS CLINIC  
YALE LAW SCHOOL\*  
P.O. Box. 208215  
New Haven, CT 06520  
Tel: (203) 432-9387  
Fax: (203) 432-3034  
jonathan.manes@yale.edu

*Attorneys for Plaintiff Nicholas Merrill*

Dated: June 11, 2015  
New Haven, CT

---

\* The Media Freedom and Information Access Clinic is a program of the Abrams Institute for Freedom of Expression and the Information Society Project at Yale Law School. This memorandum does not purport to present the school's institutional views, if any.



UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

NICHOLAS MERRILL,

Plaintiff,

v.

14 CIV. 09763 (VM)

ERIC HOLDER, Jr., in his official capacity as  
Attorney General of the United States, and  
JAMES B. COMEY, in his official capacity as  
Director of the Federal Bureau of Investigation,

Defendants.

**STATEMENT PURSUANT TO LOCAL CIVIL RULE 56.1(b)**

Pursuant to Local Civil Rule 56.1(b), plaintiff in the above-named action submits this response to the In Camera, Ex Parte Declaration of Gary Douglas Perdue, Federal Bureau of Investigation ("Perdue Declaration" or "Declaration"), which defendants submitted in lieu of the statement of material facts ordinarily required on a motion for summary judgment pursuant to Local Civil Rule 56.1(a). See Memorandum of Law in Support of the Government's Motion to Dismiss or for Summary Judgment, at 2 n.1, ECF No. 25. To the extent possible, plaintiff responds to each paragraph of the Perdue Declaration as if it were a statement pursuant to Local Civil Rule 56.1(a).

Certain paragraphs of the Perdue Declaration were classified as national security information by the government and were not shared with plaintiff or plaintiff's counsel. As a result, this statement cannot respond to those paragraphs. If the Court regards any of the classified portions of the Perdue Declaration to be relevant or material to the pending cross-motions, the Court should, after conducting an *in camera* review, order the government to disclose those portions to the plaintiff to the greatest extent possible and to furnish plaintiff with an unclassified summary of any material that remains redacted. See *Doe v. Holder*, 640 F. Supp. 2d 517 (S.D.N.Y. 2009).

*Paragraphs 1-4:*

These paragraphs describe the position and authority of the declarant, and the purpose and basis of his subsequent statements. These paragraphs therefore do not state material facts to which a response is required under Local Civil Rule 56.1(b). To the extent that these paragraphs state material facts, admit for the purpose of these cross-motions.

*Paragraph 5:*

Deny to the extent that this paragraph suggests that the declaration is classified in full and deny to the extent it suggests that plaintiff's counsel is not entitled to disclosure of the classified portions of the declaration in any form. Otherwise admit for the purpose of these cross-motions.

*Paragraph 6:*

This paragraph describes the purpose of the Perdue Declaration and does not state material facts to which a response is required under Local Civil Rule 56.1(b). To the extent that it states material facts, admit for the purpose of these cross-motions.

*Paragraph 7:*

Deny that disclosure of information contained in the Attachment to the NSL in question would reveal sensitive FBI national security methods and techniques. *See* responses to paragraphs 55-72 below. Otherwise admit for the purpose of these cross-motions.

To the extent that this paragraph asserts that disclosure would result in harm sufficient to justify a nondisclosure order under the NSL statute and/or the First Amendment, it states a legal conclusion to which no response is required under Local Civil Rule 56.1(b). To the extent a response is required, it is provided in plaintiff's Memorandum of Law in Support of Summary Judgment and in plaintiff's Reply Memorandum of Law in further Support of Summary Judgment and in Opposition to the Government's Motion to Dismiss or for Summary Judgment.

*Paragraph 8:*

This paragraph summarizes the contents of the Perdue Declaration and does not state material facts to which a response is required under Local Civil Rule 56.1(b).

*Paragraphs 9-10:*

Admit for the purpose of these cross-motions.

*Paragraph 11:*

Admit first sentence. Deny that NSLs are not used to obtain the content of electronic communications. *See* Merrill Decl. ¶ 51; Second Manes Decl. Exs. A-B; Reply Mem. of Law in further Supp. of Pl.'s Mot. for S.J. and in Opp. to the Govt's Mot. to Dismiss or for S.J., at 10-11 (filed June 12, 2015) ("Pl. Reply and Opp. Br."). The third sentence characterizes the legal requirements of 18 U.S.C. § 2709(b), and plaintiff does not join in that characterization. For instance, § 2709(b) does not include the term "high-ranking official" as stated in the Declaration, but instead specifies that each NSL requires a certification by an FBI official of rank not lower than a Special Agent in Charge in a Bureau field office or Deputy Assistant Director at Bureau headquarters.

*Paragraphs 12-13:*

Deny to the extent these paragraphs suggest that revealing the specific categories of records listed in the Attachment could be expected to compromise FBI investigations. *See* Merrill Decl. ¶¶ 37-49; Manes Decl. ¶¶ 17-19, Exs. J, K (at p. 10), L (at pp. 217-18, 222-23), R (at pp. 4-5); Second Manes Decl., Exs. A-B. Otherwise admit for purposes of these cross-motions.

*Paragraphs 14-18:*

These paragraphs are marked classified and were redacted from the version of the Declaration shared with plaintiff. The section heading, however, suggests that the redacted material pertains to the "underlying FBI national security investigation." Object to all information pertaining to the target of the NSL or the underlying investigation as irrelevant, immaterial, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraph 19:*

Object as irrelevant, immaterial, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed); ECF No. 26.

*Paragraph 20 and the unnumbered paragraph that follows:*

These paragraphs are marked classified and were redacted from the version of the Declaration shared with plaintiff. The section heading, however, suggests that the redacted material pertains to the "underlying FBI national security investigation." Object to all information pertaining to the target of the NSL or the underlying investigation as irrelevant, immaterial, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraph 21:*

Admit for the purpose of these cross-motions.

*Paragraph 22:*

This paragraph is marked classified and was redacted from the version of the Declaration shared with plaintiff. The section heading, however, suggests that the redacted material pertains to the "underlying FBI national security investigation." Object to all information pertaining to the target of the NSL or the underlying investigation as irrelevant, immaterial, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraphs 23-24:*

Object as irrelevant, immaterial, unfairly prejudicial, hearsay, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraphs 25-28:*

These paragraphs are marked classified and were redacted from the version of the Declaration shared with plaintiff. The section heading, however, suggests that the redacted material pertains to the target of the NSL that was served upon plaintiff. Object to all information pertaining to the target of the NSL or the underlying investigation as irrelevant,

immaterial, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraph 29:*

Object as irrelevant, immaterial, hearsay, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraph 30:*

Admit for the purpose of these cross-motions.

*Paragraph 31:*

This paragraph is marked classified and was redacted from the version of the Declaration shared with plaintiff. The section heading, however, suggests that the redacted material pertains to the target of the NSL that was served upon plaintiff. Object to all information pertaining to the target of the NSL or the underlying investigation as irrelevant, immaterial, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraph 32:*

Admit for the purpose of these cross-motions.

*Paragraph 33:*

Object as irrelevant, immaterial, hearsay, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraph 34:*

Admit that Merrill engaged in communications with [REDACTED] as described in the Declaration of Nicholas Merrill executed on May 15, 2004. Otherwise object as irrelevant, immaterial, hearsay, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraphs 35-37:*

Object as irrelevant, immaterial, hearsay, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraph 38:*

This paragraph is marked classified and was redacted from the version of the Declaration shared with plaintiff. The section heading, however, suggests that the redacted material pertains

to the target of the NSL that was served upon plaintiff. Object to all information pertaining to the target of the NSL or the underlying investigation as irrelevant, immaterial, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraphs 39-44:*

Object as irrelevant, immaterial, hearsay, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraph 45:*

This paragraph is marked classified and was redacted from the version of the Declaration shared with plaintiff. The section heading, however, suggests that the redacted material pertains to the target of the NSL that was served upon plaintiff. Object to all information pertaining to the target of the NSL or the underlying investigation as irrelevant, immaterial, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraphs 46-54:*

Object as irrelevant, immaterial, hearsay, unfairly prejudicial, confusing the issues, and otherwise unsupported by admissible evidence. *See* Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

*Paragraph 55:*

Deny the first sentence in full, and deny all subsequent sentences of this paragraph to the extent they suggest that revealing the specific categories of records listed in the Attachment could be expected to compromise future investigations. *See* Merrill Decl. ¶¶ 37-49; Manes Decl. ¶¶ 17-19, Exs. J, K (at p. 10), L (at pp. 217-18, 222-23), R (at pp. 4-5); Second Manes Decl., Exs. A-B.

To the extent that this paragraph suggests that disclosure would result in harm sufficient to justify a nondisclosure order under the NSL statute and/or the First Amendment, it states a legal conclusion to which no response is required under Local Civil Rule 56.1(b). To the extent a response is required, it is provided in plaintiff's Memorandum of Law in Support of Summary Judgment and in plaintiff's Reply Memorandum of Law in further Support of Summary Judgment and in Opposition to the Government's Motion to Dismiss or for Summary Judgment.

For the purpose of these cross-motions, admit the second sentence to the extent that it states that the NSL Attachment specifically outlined the information sought from plaintiff. Otherwise deny the second sentence, including to deny that the NSL Attachment indicates why the FBI was seeking the information specified in the Attachment (i.e. "to help identify the account holder and/or his/her computer [REDACTED]"). *See* Merrill. Decl. Ex. B; Manes Decl. Ex E, at 6.



Deny the third sentence to the extent it asserts that information concerning items listed in the Attachment would provide "essential facts" to the investigation, or would "further the FBI investigation and analysis." *See* Merrill Decl. ¶ 14; Defendants' Local Civil Rule 56.1(b) Statement, response to para. 25 (admitting that the underlying investigation is now closed), ECF No. 26.

Deny the fourth sentence to the extent that it states that collection of such information assists the FBI in "every investigation." *See* Merrill Decl. ¶ 14; Manes Decl. Ex. R, at 7.

*Paragraph 56:*

Admit that releasing the NSL Attachment would disclose what kinds of records the FBI can obtain with an NSL. Otherwise deny in full. *See* Merrill Decl. ¶¶ 37-49; Manes Decl. ¶¶ 17-19, Exs. J, K (at p. 10), L (at pp. 217-18, 222-23); R (at pp. 4-5); Second Manes Decl., Exs. A-B.

To the extent that this paragraph suggests that disclosure would result in harm sufficient to justify a nondisclosure order under the NSL statute and/or the First Amendment, it states a legal conclusion to which no response is required under Local Civil Rule 56.1(b). To the extent a response is required, it is provided in plaintiff's Memorandum of Law in Support of Summary Judgment and in plaintiff's Reply Memorandum of Law in further Support of Summary Judgment and in Opposition to the Government's Motion to Dismiss or for Summary Judgment.

*Paragraph 57:*

Admit the first three sentences for the purpose of these cross-motions. Admit the fourth sentence for the purpose of these cross-motions, except note that the phrase "account number" has not been subject to a nondisclosure requirement since 2010. *See Doe v. Holder*, 703 F. Supp. 2d 313, 316 (S.D.N.Y. 2010). The fifth sentence characterizes the subsequent paragraphs of the Declaration and so does not state material facts to which a response is required under Local Civil Rule 56.1(b). To the extent a response is required, deny on the same grounds provided in response to the subsequent paragraphs.

*Paragraphs 58-69:*

Admit that the category of information identified in each paragraph is contained in the Attachment. Admit that releasing the NSL Attachment would disclose that the FBI can obtain each of the categories of information listed in the Attachment by issuing an NSL. Otherwise object to the remainder of these paragraphs as unsupported by admissible evidence, and deny the remainder of these paragraphs in full, including to deny that disclosure would harm current and future FBI investigations or allow individuals to avoid law enforcement detection. *See* Merrill Decl. ¶¶ 37-49; Manes Decl. ¶¶ 17-19, Exs. J, K (at p. 10), L (at pp. 217-18, 222-23), R (at pp. 4-5); Second Manes Decl., Exs. A-B.

To the extent that these paragraphs assert that disclosure would result in harm sufficient to justify a nondisclosure order under the NSL statute and/or the First Amendment, they state legal conclusions to which no response is required under Local Civil Rule 56.1(b). To the extent a response is required, it is provided in plaintiff's Memorandum of Law in Support of Summary Judgment and in plaintiff's Reply Memorandum of Law in further Support of Summary Judgment and in Opposition to the Government's Motion to Dismiss or for Summary Judgment.

*Paragraph 70:*

Admit the first two sentences of subparagraph (a) for the purpose of these cross-motions. The third sentence states a legal conclusion to which no response is required under Local Civil Rule 56.1(b). To the extent a response is required, the third sentence is denied for the reasons provided at Pl. Reply and Opp. Br. 9-12. The fourth sentence is denied because this category of records is not redacted from the public version of the NSL Attachment and appears to have been public since 2009. *See* Merrill Decl. Ex. C; Exhibit A to Mem. in Supp. of Pltfs' Mot. for Partial Reconsid'n, *Doe v. Holder*, No. 04-cv-2614, 703 F. Supp. 2d 313 (S.D.N.Y. filed Nov. 3, 2009).

*Paragraph 71:*

Deny. *See* Merrill Decl. ¶¶ 37-49, Ex. C; Manes Decl. ¶¶ 17-19, Exs. J, K (at p. 10), L (at pp. 217-18, 222-23), R (at pp. 4-5); Second Manes Decl., Exs. A-B.

To the extent that this paragraph asserts that disclosure would result in harm sufficient to justify a nondisclosure order under the NSL statute and/or the First Amendment, it states a legal conclusion to which no response is required under Local Civil Rule 56.1(b). To the extent a response is required, it is provided in plaintiff's Memorandum of Law in Support of Summary Judgment and in plaintiff's Reply Memorandum of Law in further Support of Summary Judgment and in Opposition to the Government's Motion to Dismiss or for Summary Judgment.

*Paragraph 72:*

Admit the first three sentences for the purpose of these cross-motions. Deny the remainder of the paragraph. *See* Merrill Decl. ¶¶ 37-49, Ex. C; Manes Decl. ¶¶ 17-19, Exs. J, K (at p. 10), L (at pp. 217-18, 222-23), R (at pp. 4-5); Second Manes Decl., Exs. A-B.

To the extent that this paragraph asserts that disclosure would result in harm sufficient to justify a nondisclosure order under the NSL statute and/or the First Amendment, it states a legal conclusion to which no response is required under Local Civil Rule 56.1(b). To the extent a response is required, it is provided in plaintiff's Memorandum of Law in Support of Summary Judgment and in plaintiff's Reply Memorandum of Law in further Support of Summary Judgment and in Opposition to the Government's Motion to Dismiss or for Summary Judgment.

*Paragraph 73:*

Admit.

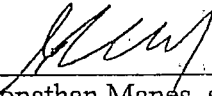
*Paragraph 74:*

Admit for the purpose of these cross-motions. With respect to the second sentence, plaintiff notes that section 502 of the USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268, 288, requires the Attorney General to adopt procedures with respect to the review and termination of nondisclosure requirements issued pursuant to 18 U.S.C. § 2709. Nothing in the statute excludes from that requirement nondisclosure orders that were in place prior to the enactment of the law, nor does it exclude nondisclosure orders where the underlying investigation was closed prior to the enactment of the law.

*Paragraph 75:*

This paragraph declares that the Perdue Declaration was made under penalty of perjury. No response is required.

Respectfully submitted,

  
Jonathan Manes, supervising attorney  
David A. Schulz, supervising attorney  
Benjamin Graham, law student intern  
Matthew Halgren, law student intern  
Nicholas Handler, law student intern  
Amanda Lynch, law student intern  
MEDIA FREEDOM AND INFORMATION  
ACCESS CLINIC  
YALE LAW SCHOOL  
P.O. Box 208215  
New Haven, CT 06520  
Tel: (203) 432-9387  
Fax: (203) 432-3034  
jonathan.manes@yale.edu

*Counsel for the Plaintiff*

Dated: New Haven, CT  
June 11, 2015



UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

NICHOLAS MERRILL,

Plaintiff,

v.

14 CIV. 9763 (VM)

ERIC HOLDER, Jr., in his official capacity as ~~SEALED~~  
Attorney General of the United States, and  
JAMES B. COMEY, in his official capacity  
as Director of the Federal Bureau of  
Investigation,

Defendants.

**SECOND DECLARATION OF JONATHAN MANES**

I, Jonathan Manes, hereby declare:

1. I am a supervising attorney and clinical lecturer in the Media Freedom and Information Access Clinic at Yale Law School, which represents Nicholas Merrill in the above-captioned litigation. I submit this supplemental declaration in order to introduce two additional exhibits that are relevant to plaintiff's opposition to the defendants' Motion to Dismiss or for Summary Judgment, and to plaintiff's Motion for Summary Judgment.

2. Attached hereto as Exhibit A are true and correct excerpts from H. Marshall Jarrett & Michael W. Bailie, Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009). An additional excerpt from this source was attached as Exhibit L to the first Declaration of Jonathan Manes. ECF No. 20-12.

3. Attached hereto as Exhibit B is a true and correct copy of the U.S. Department of Justice's United States Attorneys' Manual § 9-7.500, as published online at the following address: <http://www.justice.gov/usam/usam-9-7000-electronic-surveillance#9-7.500>.

I declare under penalty of perjury that the foregoing is true and correct. Executed on June 11, 2015, at New Haven, CT.

  
\_\_\_\_\_  
Jonathan Manes

**EXHIBIT A**

**SEARCHING AND  
SEIZING COMPUTERS  
AND OBTAINING  
ELECTRONIC EVIDENCE  
IN CRIMINAL  
INVESTIGATIONS**

**Computer Crime and  
Intellectual Property Section  
Criminal Division**



**Published by  
Office of Legal Education  
Executive Office for  
United States Attorneys**

**H. Marshall Jarrett  
Director, EOUSA**

**Michael W. Bailie  
Director, OLE**

**OLE  
Litigation  
Series**

**Ed Hagen  
Assistant Director,  
OLE**

**Nathan Judish  
Computer Crime  
and Intellectual  
Property Section**

The Office of Legal Education intends that this book be used by Federal prosecutors for training and law enforcement purposes.

The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. See *United States v. Caceres*, 440 U.S. 741 (1979).


[ pages ii – 114 omitted]

# Chapter 3

## The Stored Communications Act

---

### A. Introduction

 The SCA regulates how the government can obtain stored account information from network service providers such as ISPs. Whenever agents or prosecutors seek stored email, account records, or subscriber information from a network service provider, they must comply with the SCA. The SCA's classifications are summarized in the chart that appears in Section F of this chapter.

The Stored Communications Act, 18 U.S.C. §§ 2701-2712 (“SCA”), sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers.<sup>1</sup> There are three main substantive components to this system, which serves to protect and regulate the privacy interests of network users with respect to government, network service providers, and the world at large. First, § 2703 creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications from network service providers. Second, § 2702 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-government entities. Third, § 2701 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties.

The structure of the SCA reflects a series of classifications that indicate the drafters’ judgments about what kinds of information implicate greater or lesser privacy interests. For example, the drafters saw greater privacy interests in the

---

<sup>1</sup> The SCA is sometimes referred to as the Electronic Communications Privacy Act. The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 (“ECPA”), but ECPA itself also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute addressed in Chapter 4. *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986). Although 18 U.S.C. § 2701-2712 is referred to as the “Stored Communications Act” here and elsewhere, the phrase “Stored Communications Act” appears nowhere in the language of the statute.

content of stored emails than in subscriber account information. Similarly, the drafters believed that computing services available “to the public” required more strict regulation than services not available to the public. (Perhaps this judgment reflects the view that providers available to the public are not likely to have close relationships with their customers, and therefore might have less incentive to protect their customers’ privacy.) To protect the array of privacy interests identified by its drafters, the SCA offers varying degrees of legal protection depending on the perceived importance of the privacy interest involved. Some information can be obtained from providers with a subpoena; other information requires a special court order; and still other information requires a search warrant. In addition, some types of legal process require notice to the subscriber, while other types do not.

Agents and prosecutors must apply the various classifications devised by the SCA’s drafters to the facts of each case to figure out the proper procedure for obtaining the information sought. First, they must classify the network service provider (*e.g.*, does the provider provide “electronic communication service,” “remote computing service,” or neither). Next, they must classify the information sought (*e.g.*, is the information content “in electronic storage,” content held by a remote computing service, a non-content record pertaining to a subscriber, or other information enumerated by the SCA). Third, they must consider whether they are seeking to compel disclosure or seeking to accept information disclosed voluntarily by the provider. If they seek compelled disclosure, they need to determine whether they need a search warrant, a 2703(d) court order, or a subpoena to compel the disclosure. If they are seeking to accept information voluntarily disclosed, they must determine whether the statute permits the disclosure. The chart contained in Section F of this chapter provides a useful way to apply these distinctions in practice.

The organization of this chapter will follow the SCA’s various classifications. Section B explains the SCA’s classification structure, which distinguishes between providers of “electronic communication service” and providers of “remote computing service.” Section C explains the different kinds of information that providers can divulge, such as content “in electronic storage” and “records . . . pertaining to a subscriber.” Section D explains the legal process that agents and prosecutors must follow to compel a provider to disclose information. Section E looks at the flip side of this problem and explains when providers may voluntarily disclose account information. A summary chart appears in Section F. Section G discusses important issues that may arise when agents



obtain records from network providers: steps to preserve evidence, steps to prevent disclosure to subjects, Cable Act issues, and reimbursement to providers. Section H discusses the Fourth Amendment’s application to stored electronic communications. Finally, Section I discusses the remedies that courts may impose following violations of the SCA.

## B. Providers of Electronic Communication Service vs. Remote Computing Service

The SCA protects communications held by two defined classes of network service providers: providers of “electronic communication service,” *see* 18 U.S.C. § 2510(15), and providers of “remote computing service,” *see* 18 U.S.C. § 2711(2). Careful examination of the definitions of these two terms is necessary to understand how to apply the SCA.

### 1. Electronic Communication Service

An electronic communication service (“ECS”) is “any service which provides to users thereof the ability to send or receive wire or electronic communications.” 18 U.S.C. § 2510(15). (For a discussion of the definitions of wire and electronic communications, see Chapter 4.D.2.) For example, “telephone companies and electronic mail companies” generally act as ECS providers. *See* S. Rep. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3568; *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 900-03 (9th Cir. 2008) (text messaging service provider is an ECS); *In re Application of United States*, 509 F. Supp. 2d 76, 79 (D. Mass. 2007) (cell phone service provider is an ECS); *Kaufman v. Nest Seekers, LLC*, 2006 WL 2807177, at \*5 (S.D.N.Y. Sept. 26, 2006) (host of electronic bulletin board is ECS); *Freedman v. America Online, Inc.*, 325 F. Supp. 2d 638, 643 n.4 (E.D. Va. 2004) (AOL is an ECS).

Any company or government entity that provides others with the means to communicate electronically can be a “provider of electronic communication service” relating to the communications it provides, regardless of the entity’s primary business or function. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114-15 (3d Cir. 2004) (insurance company that provided email service to employees is an ECS); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (city providing pager service to its police officers was a provider of ECS); *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (airline that provides travel agents with computerized travel reservation system

[ pages 118 – 119 omitted]

Verizon is a provider to the public: anyone can obtain a Verizon account. (It may seem odd at first that a service can charge a fee but still be considered available “to the public,” but this approach mirrors commercial relationships in the physical world. For example, movie theaters are open “to the public” because anyone can buy a ticket and see a show, even though tickets are not free.) In contrast, providers whose services are available only to those with a special relationship with the provider do not provide service to the public. For example, an employer that provides email accounts to its employees will not be an RCS with respect to those employees, because such email accounts are not available to the public. See *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (interpreting the “to the public” clause in § 2702(a) to exclude an internal email system that was made available to a hired contractor but was not available to “any member of the community at large”).

In *Quon v. Arch Wireless Operating Co.*, the Ninth Circuit held that a text messaging service provider was an ECS and therefore not an RCS. See *Quon*, 529 F.3d at 902-03. However, this “either/or” approach to ECS and RCS is contrary to the language of the statute and its legislative history. The definitions of ECS and RCS are independent of each other, and therefore nothing prevents a service provider from providing both forms of service to a single customer. In addition, an email service provider is certainly an ECS, but the House report on the SCA also stated that an email stored after transmission would be protected by a provision of the SCA that protects contents of communications stored by an RCS. See H.R. Rep. No. 99-647, at 65 (1986). One subsequent court has rejected the Ninth Circuit’s analysis in *Quon* and stated that a provider “may be deemed to provide both an ECS and an RCS to the same customer.” *Flagg v. City of Detroit*, 252 F.R.D. 346, 362 (E.D. Mich. 2008). The key to determining whether the provider is an ECS or RCS is to ask what role the provider has played and is playing with respect to the communication in question.

### C. Classifying Types of Information Held by Service Providers

Network service providers can store different kinds of information relating to an individual customer or subscriber. Consider the range of information that an ISP may typically store regarding one of its customers. It may have the customer’s subscriber information, such as name, address, and credit card

number. It may have logs revealing when the customer logged on and off the service, the IP addresses assigned to the customer, and other more detailed logs pertaining to what the customer did while online. The ISP may also have the customer's opened, unopened, draft, and sent emails.

When agents and prosecutors wish to obtain such records, they must be able to classify these types of information using the language of the SCA. The SCA breaks the information down into three categories: (1) contents; (2) non-content records and other information pertaining to a subscriber or customer; and (3) basic subscriber and session information, which is a subset of non-content records and is specifically enumerated in 18 U.S.C. § 2703(c)(2). *See* 18 U.S.C. §§ 2510(8), 2703. In addition, as described below, the SCA creates substantially different protections for contents in “electronic storage” in an ECS and contents stored by a provider of RCS.

### **1. Basic Subscriber and Session Information Listed in 18 U.S.C. § 2703(c)(2)**

Section 2703(c)(2) lists the categories of basic subscriber and session information:

(A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)[.]

In general, the items in this list relate to the identity of a subscriber, his relationship with his service provider, and his basic session connection records. In the Internet context, “any temporarily assigned network address” includes the IP address used by a customer for a particular session. For example, for a webmail service, the IP address used by a customer accessing her email account constitutes a “temporarily assigned network address.” This list does not include other, more extensive transaction-related records, such as logging information revealing the email addresses of persons with whom a customer corresponded.

## 2. Records or Other Information Pertaining to a Customer or Subscriber

Section 2703(c)(1) covers a second type of information: “a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications).” This is a catch-all category that includes all records that are not contents, including basic subscriber and session information described in the previous section. As one court explained, “a record means something stored or archived. The term information is synonymous with data.” *In re United States*, 509 F. Supp. 2d 76, 80 (D. Mass. 2007).

Common examples of “record[s] . . . pertaining to a subscriber” include transactional records, such as account logs that record account usage; cell-site data for cellular telephone calls; and email addresses of other individuals with whom the account holder has corresponded. *See* H.R. Rep. No. 103-827, at 10, 17, 31 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3490, 3497, 3511. *See also In re Application of United States*, 509 F. Supp. 76, 80 (D. Mass. 2007) (historical cell-site information fall within scope of § 2703(c)(1)); *United States v. Allen*, 53 M.J. 402, 409 (C.A.A.F. 2000) (concluding that “a log identifying the date, time, user, and detailed internet address of sites accessed” by a user constituted “a record or other information pertaining to a subscriber or customer of such service” under the SCA); *Hill v. MCI WorldCom Commc’ns, Inc.*, 120 F. Supp. 2d 1194, 1195-96 (S.D. Iowa 2000) (concluding that the “names, addresses, and phone numbers of parties . . . called” constituted “a record or other information pertaining to a subscriber or customer of such service,” not contents, for a telephone account); *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (holding that a customer’s identification information is a “record or other information pertaining to a subscriber” rather than contents). According to the legislative history of the 1994 amendments to § 2703(c), the purpose of separating the basic subscriber and session information from other non-content records was to distinguish basic subscriber and session information from more revealing transactional information that could contain a “person’s entire on-line profile.” H.R. Rep. No. 103-827, at 17, 31-32 (1994), *reprinted in* 1994 U.S.C.C.A.N. 3489, 3497, 3511-12.

## 3. Contents and “Electronic Storage”

The contents of a network account are the actual files (including email) stored in the account. *See* 18 U.S.C. § 2510(8) (“‘contents,’ when used with

[ pages 123 – 150 omitted]

# Chapter 4

## Electronic Surveillance in Communications Networks

---

### A. Introduction

Criminal investigations often involve real-time electronic surveillance. In computer crime cases, agents may want to monitor a hacker as he breaks into a victim computer system or set up a “cloned” email account to monitor a suspect sending or receiving child pornography. In cases involving cellular telephones, agents may wish to obtain “cell-site” location information for a suspect’s cellular telephone to determine the suspect’s approximate location at the time of a call. Agents may wish to wiretap a suspect’s telephone or learn whom the suspect has called. This chapter explains how the electronic surveillance statutes apply to criminal investigations involving computers and also discusses how to obtain cell-site location information for cellular phones.

Real-time electronic surveillance in federal criminal investigations is governed primarily by two statutes. The first is the federal Wiretap Act, 18 U.S.C. §§ 2510-2522, first passed as Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (and generally known as “Title III”). The second statute is the Pen Registers and Trap and Trace Devices chapter of Title 18 (“the Pen/Trap statute”), 18 U.S.C. §§ 3121-3127, first passed as part of the Electronic Communications Privacy Act of 1986. Failure to comply with these statutes may result in civil and criminal liability, and in the case of Title III, may also result in suppression of evidence.

### B. Content vs. Addressing Information



In general, the Pen/Trap statute regulates the collection of addressing and other non-content information for wire and electronic communications. Title III regulates the collection of actual content of wire and electronic communications.



Title III and the Pen/Trap statute regulate access to different types of information. Title III permits the government to obtain the contents of wire and electronic communications in transmission. In contrast, the Pen/Trap statute concerns the real-time collection of addressing and other non-content information relating to those communications. *See* 18 U.S.C. § 2511(2)(h)(i) (stating that it is not a violation of Title III to use a pen register or trap and trace device); *United States Telecom Ass'n v. FCC*, 227 F.3d 450, 453-54 (D.C. Cir. 2000) (contrasting pen registers and Title III intercept devices); *Brown v. Waddell*, 50 F.3d 285, 289-94 (4th Cir. 1995) (same).

The difference between addressing information and content is clear for telephone calls. The addressing information is the phone numbers of the originating and receiving telephones. The content of the communication is the actual conversation between the parties to the call.

The distinction between addressing information and content also applies to Internet communications. For example, when computers on the Internet communicate with each other, they break down messages into discrete chunks known as packets and then send each packet out to its intended destination. Every packet contains addressing information in the header of the packet (much like the “to” and “from” addresses on an envelope), followed by the payload of the packet, which contains the contents (much like a letter inside an envelope). The Pen/Trap statute permits law enforcement to obtain the addressing information of Internet communications much as it would addressing information for traditional phone calls. However, collecting the entire packet ordinarily implicates Title III. The primary difference between an Internet pen/trap device and an Internet Title III intercept device is that the former is designed to capture and retain only addressing information, while the latter is designed to capture and retain the entire packet.

The same distinction applies to Internet email. Every Internet email message consists of a set of headers that contain addressing and routing information generated by the mail program, followed by the actual contents of the message authored by the sender. The addressing and routing information includes the email address of the sender and recipient, as well as information about when and where the message was sent on its way (roughly analogous to the postmark on a letter). *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (email to/from addresses and IP addresses constitute addressing information). The Pen/Trap statute permits law enforcement to obtain the header information of Internet emails (except for the subject line, which can

contain content) using a court order, just like it permits law enforcement to obtain addressing information for phone calls and individual Internet packets using a court order. Conversely, the interception of email contents, including the subject line, requires compliance with the strict dictates of Title III.

In some circumstances, questions may arise regarding whether particular components of network communications contain content. *See In re Application of United States*, 396 F. Supp. 2d 45, 49 (D. Mass. 2005) (asserting that uniform resource locators (“URLs”) may contain content); *In re Pharmatrak, Inc. Privacy Litigation*, 329 F.3d 9, 16 (1st Cir. 2003) (noting that user-entered search terms are sometimes appended to the query string of the URL for the search results page). Because of these and other issues, the United States Attorneys’ Manual currently requires prior consultation with CCIPS before a pen/trap may be used to collect all or part of a URL. *See* United States Attorneys’ Manual § 9-7.500. Prosecutors who have other questions about whether a particular type of information constitutes contents may contact CCIPS for assistance at (202) 514-1026.

## C. The Pen/Trap Statute, 18 U.S.C. §§ 3121-3127

The Pen/Trap statute authorizes a government attorney to apply to a court for an order authorizing the installation of a pen register and/or trap and trace device if “the information likely to be obtained is relevant to an ongoing criminal investigation.” 18 U.S.C. § 3122(b)(2). In rough terms, a pen register records outgoing addressing information (such as a number dialed from a monitored telephone), and a trap and trace device records incoming addressing information (such as caller ID information). The Pen/Trap statute applies to a wide range of communication technologies, including computer network communications. *See In re Application of United States*, 416 F. Supp. 2d 13, 16 (D.D.C. 2006).

### 1. Definition of Pen Register and Trap and Trace Device

The Pen/Trap statute defines pen registers and trap and trace devices broadly. As defined in 18 U.S.C. § 3127(3), a “pen register” is

a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is

[ pages 154 through the end omitted]

# **EXHIBIT B**

## **9-7.500 - Prior Consultation with the Computer Crime and Intellectual Property Section of the Criminal Division (CCIPS) for Applications for Pen Register and Trap and Trace Orders Capable of Collecting Uniform Resource Locators (URLs)**

In 2001, the USA PATRIOT Act (P.L. 107-56) amended the Pen Register and Trap and Trace Statute (pen/trap statute), 18 U.S.C. § 3121 et seq., to clarify that courts may issue pen/trap orders to collect the non-content information associated with Internet communications. One issue that has been raised in this regard is whether a pen register order may be used to collect (URLs), the terms that a person uses to request information on the World Wide Web (e.g., [www.cybercrime.gov/PatriotAct.htm](http://www.cybercrime.gov/PatriotAct.htm)). Because of privacy and other concerns relating to the use of pen register orders in this fashion, use of pen registers to collect all or part of a URL is prohibited without prior consultation with CCIPS. Among the factors that should be considered in deciding whether to apply for such a pen register are (1) the investigative need for the pen register order, (2) the litigation risk in the individual case, (3) how much of any given URL would be obtained, and (4) the impact of the order on the Department's policy goals.

Consultation with CCIPS can help resolve these issues, as well as ensuring that the contemplated use of a pen register would be consistent with the Deputy Attorney General's May 24, 2002 Memorandum on "Avoiding Collection and Investigative Use of 'Content' in the Operation of Pen Registers and Trap and Trace Devices."

This policy does not apply to applications for pen register orders that would merely authorize collection of Internet Protocol (IP) addresses, even if such IP addresses can be readily translated into URLs or portions of URLs. Similarly, this policy does not apply to the collection, at a web server, of tracing information indicating the source of requests to view a particular URL using a trap and trace order.

No employee of the Department will use the pen register authority to collect URLs without first consulting with the CCIPS of the Criminal Division. Absent emergency circumstances, such an employee will submit a memorandum to CCIPS that contains (a) the basic facts of the investigation, (b) the proposed application and order, (c) the investigative need for the collection of URLs, (d) an analysis of the litigation risk associated with obtaining the order in the context of the particular case, and (e) any other information relevant to evaluating the propriety of the application. In an emergency, such an employee may telephone CCIPS at (202) 514-1026 or, after hours at (202) 514-5000, and be prepared to describe the above information.

[new September 2003]

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

NICHOLAS MERRILL,

Plaintiff,

v.

14 CIV. 09763 (VM)

ERIC HOLDER, Jr., in his official capacity as  
Attorney General of the United States, and  
JAMES B. COMEY, in his official capacity as  
Director of the Federal Bureau of Investigation,

~~SEALED~~

Defendants.

CERTIFICATE OF SERVICE

I, Jonathan Manes, hereby certify that on June 12, 2015, I caused a copy of the following documents to be served upon counsel for the defendants via Federal Express overnight delivery addressed to Benjamin Torrance, Assistant United States Attorney, Southern District of New York, 86 Chambers Street, New York, NY 10007:

- Reply Memorandum of Law in Support of Nicholas Merrill's Motion for Summary Judgment and in Opposition to the Government's Motion to Dismiss or for Summary Judgment.
- Plaintiff's Statement Pursuant to Local Civil Rule 56.1(b).
- Second Declaration of Jonathan Manes, with accompanying Exhibits A and B.

Dated: June 12, 2015



Jonathan Manes