UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

NICHOLAS MERRILL, Plaintiff, v. 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.	14 CIV. 09763 (VM) ~~SEALED~~

DECLARATION OF NICHOLAS MERRILL

I, Nicholas Merrill, hereby declare:

1. I am the Executive Director and Founder of the Calyx Institute, a non-profit education and research organization devoted to studying, testing, developing, and implementing "privacy by design" through functional privacy and anonymity controls. The Institute pursues these aims as part of its mission of promoting free speech, civic engagement, and privacy rights online and in the mobile technology industry.

2. I am a computer scientist and systems administrator dedicated to building experimental privacy-protective options for Internet users, including developing a ubiquitously encrypted public test bed and convenient security software models for public use and education. At the Calyx Institute, for example, I operate an optimally secure experimental free public conferencing service and I am currently working to build an encrypted Internet Exchange called CRYPTO-IX, among other projects. Through the Calyx Institute, I have also launched Canary Watch with several partners to monitor when organizations that post "warrant canaries"—

regularly published statements announcing that the organization has not received a demand from the government to produce information about its users—have altered or taken down those statements.

3. In February 2004, I was the president, owner, and sole employee of Calyx Internet Access, an Internet access and consulting business that was incorporated and located in Manhattan, New York. Calyx Internet Access provided clients with an interface for maintaining their own websites, electronic file storage, email accounts, and sometimes Internet access.

4. Calyx Internet Access had both paying and non-paying clients, some of whom engaged in controversial political speech. Some of our clients communicated anonymously or pseudonymously, allowing them to discuss sensitive or controversial subjects without fear of retaliation or reprisal.

5. I ceased operating Calyx Internet Access in August 2004, and the company is now defunct.

The National Security Letter

6. More than a decade ago, I received a National Security Letter ("NSL") from the FBI. On or about February 4, 2004, an FBI agent served the offices of Calyx Internet Access in Manhattan with a copy of the NSL. Attached as Exhibit A is a true and correct copy of the first two pages of the letter I received in 2004, as previously redacted.

7. The NSL ordered that I "provide the [FBI] the names, addresses, lengths of service and electronic communication transactional records" pertaining to one of Calyx's clients. The letter stated that I was not allowed to tell anyone, including my client, that the FBI was seeking information through an NSL. The letter prohibited me, or my agents or employees, "from disclosing to any person that the FBI has sought or obtained access to information or records

under these provisions," pursuant to 18 U.S.C. § 2709(c). It also required that I provide responsive records personally to an FBI representative. The letter did not permit me to "send the records through the mail nor disclose the substance of [the] request in any telephone conversation."

8. The NSL included a certification that "the information sought [was] relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities."

9. The NSL included an Attachment, which identified specific client records demanded by the FBI and elaborated upon what types of records count as "electronic communication transactional records." Attached as Exhibit B is a true and correct copy of the unredacted Attachment.

10. I understood that the NSL sought to require me to turn over any types of data listed in the NSL, including any and all types of records listed in the Attachment.

Previous Litigation

11. After receiving the NSL, I sought and obtained legal advice and representation from lawyers at the American Civil Liberties Union. On April 6, 2004, I initiated a lawsuit challenging the constitutionality of the NSL statute, both with regard to the FBI's authority to force me to turn over the information sought in the NSL and Attachment as well as the gag order that accompanied the NSL. Because I was forbidden from disclosing the fact that I had received the NSL, I was identified in the lawsuit as "John Doe." Calyx Internet Access (identified as "John Doe, Inc."), the American Civil Liberties Union ("ACLU") and the American Civil Liberties Union Foundation ("ACLUF") were co-plaintiffs in the case, which was filed in the U.S. District Court for the Southern District of New York, Case No. 04 Civ. 2614 (VM).

12. On September 28, 2004, the District Court issued an opinion striking down the NSL statute, 18 U.S.C. § 2709, because it violated the First Amendment to the U.S. Constitution. The Court's opinion also found that the NSL that had been issued to me violated the Fourth Amendment to the U.S. Constitution. The Court's decision is reported as *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

13. The government appealed the District Court's decision. While that appeal was pending, and largely in response to the victory in District Court, Congress amended the NSL statute. In a decision dated May 23, 2006, the Court of Appeals for the Second Circuit remanded the case to the District Court so that the District Court could, in the first instance, address the constitutional infirmities of the law, as revised by Congress. The Court of Appeals' decision is reported as *Doe v. Gonzales*, 449 F.3d 415 (2d Cir. 2006).

14. After my case was remanded to the District Court, the government filed a declaration dated November 7, 2006, indicating that the FBI was no longer demanding that I comply with the 2004 NSL. Even though the government was no longer seeking to force me to disclose records about my client, it nevertheless continued to enforce and defend a total gag order forbidding me from even identifying myself as a plaintiff in the ongoing litigation.

15. In a decision dated September 6, 2007, the District Court again struck down the NSL statute and invalidated the gag order imposed upon me. This decision is reported as *Doe v. Gonzales*, 500 F. Supp. 2d 397 (S.D.N.Y. 2007).

16. The government again appealed the District Court's decision. The Court of Appeals, like the District Court, determined that the NSL statute did not comply with the First Amendment, but it ruled on narrower grounds and issued a narrower remedy, declining to strike the statute down in its entirety. For a second time, the Court of Appeals remanded the case to the

District Court, this time in order to give the government an opportunity to attempt to justify the continuing gag order on me under the newly articulated standards. This decision is reported as *John Doe, Inc. v. Mukasey*, 549 F.3d 861 (2d Cir. 2008).

17. On remand, in a decision dated October 20, 2009, the District Court initially held that the government had met its burden to justify the gag order in its entirety, while emphasizing that the gag did not then constitute a permanent ban on speech. That decision is reported as *Doe v. Holder*, 665 F. Supp. 2d 426 (S.D.N.Y. 2009).

18. On March 18, 2010, in response to a motion for reconsideration filed on behalf of me and my co-plaintiffs, the District Court ordered the government to lift the nondisclosure requirement with respect to certain limited portions of the Attachment listing categories of records that were either mirrored in the NSL statute itself or that the FBI had publicly acknowledged it had previously requested using NSLs. The gag order otherwise remained fully in place. That decision is reported as *Doe v. Holder*, 703 F. Supp. 2d 313 (S.D.N.Y. 2010). A true and correct copy of the redacted Attachment, as made public disclosed following this 2010 decision, is attached as Exhibit C.

19. Along with my co-plaintiffs, I appealed the District Court's decision. While that appeal was pending, I reached a settlement agreement with the FBI. Under that agreement, I was finally allowed to identify myself as the recipient of the 2004 NSL and as the plaintiff in the lawsuit. That settlement was memorialized in a Stipulation and Order of Dismissal filed in the District Court on July 30, 2010.

20. As a result of that settlement, I finally identified myself as the recipient of the NSL at issue after more than six years subject to a complete and debilitating gag order. During those six years, I had been forced to lie to those close to me and many others with whom I interacted in

order to conceal meetings with my attorneys and other activities related to the lawsuit, lest I reveal that I was the "John Doe" plaintiff in the case. This was particularly difficult because the case was often the subject of intense media interest and was extensively discussed among my colleagues in the computer security and privacy field. As a result, I was forced to constantly censor myself, and was almost entirely unable to engage in public advocacy on the issue of NSLs, for fear of violating the gag order imposed on me.

Current Scope of the Gag Order

21. Between the 2010 settlement and 2014, the government never contacted me to assert the continuing necessity of the gag order. To my knowledge, the government also did not contact the Court or any of my attorneys.

22. During this time, I had to continue to carefully censor myself, even though I could identify myself as the recipient of the 2004 NSL and the plaintiff in the long-running litigation. This continued to hamper my ability to participate in public debate and discussion regarding NSLs, and it continued to affect my interactions with relatives, friends, and colleagues.

23. In April 2014, I notified the FBI, through *pro bono* counsel at the Media Freedom and Information Access Clinic at Yale Law School, that I intended once again to challenge the continuing gag order. Given how much time had passed since the NSL was issued, I asked the FBI to voluntarily drop the gag order in its entirety. In response, the government refused to lift the gag order with respect to the contents of the Attachment to the 2004 NSL (except to the extent the District Court had lifted small portions of that gag in its March 2010 decision, described above). The government, however, agreed to lift the gag order in all other respects, citing "changed circumstances." As a result, I was permitted, for example, to disclose the target

of the 2004 NSL, and to discuss the 2004 NSL with its target. But I am still unable to speak about nearly everything included in the 2004 Attachment.

24. After the relevant portion of the gag was lifted, I communicated to the target of the NSL that the FBI had requested information about him or her.

25. It is my understanding that the investigation of which the 2004 NSL was part has now concluded. This understanding is based, among other things, on the fact that I have been permitted by the FBI to discuss the 2004 NSL with its target.

26. I understand from official government reports, news coverage, and other sources that many tens of thousands of NSLs have been issued since 2001.

27. To my knowledge, no other NSL recipient has been permitted to publicly reveal the target of an NSL issued to him or her, or to discuss an NSL with its target. To my knowledge, I am the only NSL recipient who remains subject to an NSL gag order that is limited solely to the contents of the Attachment – *i.e.*, a gag order that only forbids discussion of the *types* of records sought in an NSL, while permitting unfettered discussion of any and all other circumstances relating to the issuance of the NSL, its target, and the particular investigation that prompted it. To my knowledge no NSL recipient has yet been permitted to disclose the full contents of the Attachment or to discuss the FBI's understanding of the scope of its authority to compel disclosure of "electronic communication transactional records" ("ECTR").

Interference with Public Participation and Advocacy

28. Since I first received the NSL in 2004, I have been strongly committed to engaging in public advocacy regarding the FBI's use and abuse of NSLs. Even while I was subject to a complete gag order prior to the 2010 settlement, I sought to engage in the public and legislative

debate regarding NSLs by publishing an anonymous op-ed in the *Washington Post* in 2007. But the gag order consistently and significantly constrained my efforts at public advocacy.

29. Even now, more than a decade later, I cannot speak about the contents of the 2004 Attachment.

30. The Attachment identifies the categories of records the FBI ordered me to produce and reveals what the FBI considers to be ECTR under the NSL statute.

31. I believe that the public would be alarmed if they knew what kinds of records the FBI apparently believes constitute ECTR and can therefore obtain simply by issuing an NSL, without any prior judicial review or any meaningful likelihood of judicial oversight. I would like to explain to the public why various categories of records listed in the Attachment implicate significant concerns in terms of individual privacy, freedom of speech, and freedom of association. I would also like to be able to advocate for legislative changes to the NSL statute that would clarify and rein in the FBI's authority. But because I remain gagged with respect to the Attachment, I am unable to engage in such public education and advocacy. In fact, because of the remaining gag order, I must vigilantly censor myself when discussing the FBI's abuses and potential abuses of NSLs. The current nondisclosure order therefore continues to restrict my ability to speak out on important matters of public concern about which I would otherwise speak.

32. The government has not indicated that it will ever undertake to review the continuing necessity of the gag order, absent the threat of another legal challenge. I have no reason to believe that the government will contact me if ever the government were to decide that the gag is no longer necessary. Indeed, if I had not found and engaged *pro bono* counsel to threaten the present litigation, I would remain subject to the 2010 gag order, even though the FBI readily

conceded (in response to the threat of litigation) that "changed circumstances" had rendered most of the gag order unnecessary.

33. Therefore, if the gag order is not lifted in its entirety during the course of this litigation, I will remain subject to a gag order permanently. It is my understanding that the gag order has now become untethered from any circumstances specific to the 2004 NSL, or the investigation of which it was part, and that the government intends to permanently forbid me from discussing the contents of the Attachment.

34. Given my personal and professional commitment to discussing online privacy and government surveillance policy, the government's permanent gag on my speech continues to significantly hamper my ability to engage in the public debates in which I am most professionally and personally invested.

The Scope of Information Subject to Disclosure via NSLs

35. NSLs implicate serious privacy, free speech, and freedom of association concerns because of (i) the wide variety of electronic service providers potentially subject to NSLs, (ii) the vast amount of potentially sensitive information that such electronic service providers maintain about their clients, and (iii) the FBI's expansive understanding of the types of records that count as ECTR and are subject to compelled disclosure in response to an NSL.

36. These concerns are particularly acute because NSLs may be issued without any prior judicial oversight, and without any real prospect of judicial review after their issuance. To my knowledge, only a handful of the more than tens of thousands of NSLs issued by the FBI since 2001 have been challenged in court. I am aware of no court decision that has ever determined the lawful scope of the FBI's authority to compel production of records using NSLs, including whether its understanding of what constitutes ECTR complies with the NSL statute or with the

Constitution. In my case, the government mooted my ability to challenge the lawfulness of the FBI's claimed NSL authority when it indicated in 2006 that the FBI was no longer demanding that I comply with the NSL.

Businesses and Other Organizations Subject to NSLs

37. A potentially vast array of businesses and organizations are potentially subject to NSLs. According to the NSL statute, 18 U.S.C. § 2709, any "electronic communication service provider" may be served with an NSL demanding disclosure of records. Given the expansive meaning of electronic communications service, defined in 18 U.S.C § 2510(15) as "any service which provides to users thereof the ability to send or receive wire or electronic communications," it is my belief and understanding that the term applies to an extremely broad range of businesses and organizations. It clearly applies to Internet Service Providers, like Calyx Internet Access as it existed in 2004. However, the statute also appears to cover any business or organization with a website that enables users to communicate through email or web forms. For example, the Calyx Institute's website, which includes sign-up and contact forms for interested users, may well qualify.

38. The statute also clearly covers search engines like Google. To use a search engine, users enter requests and send them to the search engine, which performs the requested search and then transmits back the results. All websites that allow users to post their own content or that enable users to send emails and information requests also likely fall under the statute. Websites like Amazon or Yelp.com would therefore also appear to qualify as electronic communication service providers.

39. Most businesses and organizations, as well as schools and universities, provide Internet connectivity to their employees or students so that they can communicate. Each of these entities is therefore also likely to be considered a service provider under the statute.

Sensitive Information Typically Maintained by Organizations Subject to NSLs

40. Businesses and other organizations subject to NSLs will often maintain a large amount of sensitive information about individuals using their online services.

41. Based on my extensive experience working as an ISP operator, systems administrator, and experimental software designer since 1995, and based on my extensive collaborations with other computer scientists, computer engineers, and information technology professionals, I have a detailed understanding of the kinds of records that electronic communication service providers can and do typically maintain.

42. Each device participating in a specific network is assigned a unique, 32-bit numerical label, which is that computer's Internet Protocol ("IP") address. In order to send information over the Internet, the information must first be separated into small "packets," each of which consists of a header and a data payload. The header includes the originating IP address, the destination IP address, a number defining the IP protocol in use, and other information used to interpret the data payload.

43. Electronic communication service providers can maintain records of the IP addresses assigned to particular individuals and of the electronic communications involving that IP address. These records can identify, among other things, the identity of an otherwise anonymous individual communicating on the Internet, the identities of individuals in communication with one another, and the websites (or other Internet content) that an individual has accessed.

44. Electronic communication service providers can also monitor and store information regarding web transactions by their users. These transaction logs can be very detailed, including the name of every web page accessed, information about the page's content, the names of accounts accessed, and sometimes username and password combinations. This monitoring can occur by routing all of a user's traffic through a proxy server or by using a network monitoring system.

45. Electronic communication service providers can also record Internet "NetFlow" data. This data consists of a set of packets that travel between two points. Routers can be set to automatically record a list of all the NetFlows that they see, or all the NetFlows to or from a specific IP address. This NetFlow data can essentially provide a complete history of each electronic communications service used by a particular Internet user.

46. Electronic communication service providers that provide email services also maintain "log" files that monitor every email message sent or received on the provider's servers. These logs typically include the email headers, including the sender and recipient(s) as well as the subject line. This information can reveal the name of the organization associated with the sender or recipient, the subject matter of the emails, where the message is to be posted, and any descriptive content included in a user's email address. Many communication service providers also use network monitoring systems to create log files for messages that merely pass through their networks.

47. Web servers also often maintain logs of every request that they receive and every web page that is served. This could include a complete list of all web pages seen by an individual, all search terms, names of email accounts, passwords, purchases made, names of other individuals with whom the user has communicated, and so on.

48. Content Delivery Networks, such as Akamai and Limelight Networks, are high-availability networks that popular websites use to increase the speed at which their content is delivered to users. For example, many of the country's top media, entertainment, and electronic commerce companies use Akamai's services to store images and other rich content so that users can download their pages more quickly. These Content Delivery Networks record every image, webpage, video clip, or other "object" downloaded by every user of their client websites. Content Delivery Networks can therefore serve as independent sources of a user's web browsing history through the records that they store.

49. Calyx Internet Access, like most ISPs, collected a wide array of information about its clients. For a given client, we may have collected their name, address and telephone number; other addresses associated with the account; email addresses associated with the account; IP addresses associated with the account; Uniform Resource Locator (URL) addresses assigned to the account; activity logs for the account; logs tracking visitors to the client's website; the content of a client's electronic communications; data files residing on Calyx's server; the client's customer list; the client's bank account and credit card numbers; records relating to merchandise bought and sold; and the date the account was opened or closed.

Records Regarded by the FBI as ECTR Can Reveal Sensitive Personal Information

50. The Attachment to the NSL that the FBI served me with listed various categories of records constituting ECTR that the FBI sought to obtain. These categories of records constituting ECTR included:

- [redacted]
- [redacted]
- Subscriber name [redacted]
- [redacted]
- Address [redacted]
- [redacted] telephone numbers

- [redacted]
- billing [redacted]
- e-mail address [redacted]
- [redacted]

51. Even though the types of information collected by NSLs have been characterized as "non-content" data, they can nonetheless reveal extremely sensitive, substantive and personal information. Even a cursory analysis of electronic communications transactional records—such as [redacted]—can reveal a person's intimate relationships, religious, political and community affiliations, intellectual pursuits, political leanings, long-term plans, financial condition, medical concerns, and more.

52. It is often trivially easy to connect a single data point to an identity. Particular email addresses, telephone numbers, or [redacted] can be matched with organizations whose identity is inherently revealing—for example, Alcoholics Anonymous, a lawyer, a psychiatrist, or a newspaper tip line.

53. Even merely identifying the name of a client associated with a particular [redacted] can reveal sensitive information. Such disclosure can serve to unmask an individual engaging in protected anonymous speech online. It can also reveal the identities of individuals involved in religious or political associations.

54. Because "non-content" data is constantly generated, is often highly structured, and can therefore be more easily analyzed, the informational yields can be much higher. It is easy to draw inferences from patterns of communication using non-content information. Publicly available software packages like MIT's Immersion permit users to generate social graphs from

datasets like those that NSLs could be used generate. These graphs map out the individuals and organizations with whom an individual has communicated. Predictive models allow analysts to use known patterns of activity to predict certain attributes of individuals and organizations, like race, religion, leadership structure, or strength of certain personal and professional relationships.

55. In short, understanding which types of records the FBI believes it is authorized to obtain from electronic communication service providers by merely issuing an NSL is critical to assessing the substantial privacy interests at stake.

56. The Attachment to the 2004 NSL describes many of the types of records that the FBI evidently believes it can obtain using an NSL. Because I am forbidden from discussing the contents of the Attachment, I am unable to explain the significant privacy concerns implicated by the FBI's expansive use of NSLs and to alert the public to the significant potential for abuse. For the same reason, I am unable to contribute to recurrent debates in Congress over the legitimate scope of—and necessary checks on—the government's surveillance powers under the NSL statute and other provisions of the USA PATRIOT Act and other laws.

I declare under penalty of perjury that the foregoing is true and correct. Executed on March 9, 2015 at New York, NY.

Nicholas Merrill

EXHIBIT A

U.S. Department of Justice

Federal Bureau of Investigation

In Reply, Please Refer to
File No.

[redacted] 2004

[redacted]

President

[redacted]

Dear [redacted]

Under the authority of Executive Order 12333, dated December 4, 1981, and pursuant to Title 18, United States Code (U.S.C.), Section 2709 (as amended, October 26, 2001), you are hereby directed to provide the Federal Bureau of Investigation (FBI) the names, addresses, lengths of service and electronic communication transactional records, to include existing transaction/activity logs and all e-mail header information (not to include message content and/or subject fields), for the below-listed email address:

[redacted]

In accordance with Title 18, U.S.C., Section 2709(b), I certify that the information sought is relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, and that such an investigation of a United States person is not conducted solely on the basis of activities protected by the First Amendment to the Constitution of the United States.

You are further advised that Title 18, U.S.C., Section 2709(c), prohibits any officer, employee or agent of yours from disclosing to any person that the FBI has sought or obtained access to information or records under these provisions.

You are requested to provide records responsive to this request personally to a representative of the [redacted] of the FBI. Any questions you have regarding this request should be directed only to the [redacted] Due to security considerations, you should neither send the records through the mail nor disclose the substance of this request in any telephone conversation.

[redacted]

Your cooperation in this matter is greatly appreciated.

Sincerely,

Marion E. Bowman
Senior Counsel
National Security Affairs
Office of the General Counsel

EXHIBIT B

Mr. Nicholas Merrill

ATTACHMENT

"In preparing your response to this request, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communication transactional record in accordance with Title 18, United States Code, Section 2709:

-- [redacted]
-- [redacted]
-- Subscriber name
-- Account number
-- [redacted]
-- Address
-- [redacted]
-- telephone number
-- [redacted]
-- [redacted]
-- billing
-- [redacted]
-- e-mail address
-- [redacted]
-- [redacted]
-- [redacted]
-- Any other information which you consider to be an electronic communication transactional record

We are not requesting, and you should not provide, information pursuant to this request that would disclose the content of any electronic communication as defined in Title 18, United States Code, Section 2510(8)."

EXHIBIT C

[redacted]

ATTACHMENT

"In preparing your response to this request, you should determine whether your company maintains the following types of information which may be considered by you to be an electronic communication transactional record in accordance with Title 18, United States Code, Section 2709:

-- [redacted]
-- [redacted]
-- Subscriber name [redacted]
-- Account number
-- [redacted]
-- Address
-- [redacted] telephone number
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- [redacted]
-- Any other information which you consider to be an electronic communication transactional record

We are not requesting, and you should not provide, information pursuant to this request that would disclose the content of any electronic communication as defined in Title 18, United States Code, Section 2510(8)."