THE YALE LAW JOURNAL FORUM
MARCH 3, 2016

Online Service Providers and Surveillance Law Transparency

Jonathan Manes

On June 5, 2013, the first revelation hit the front pages: documents provided by Edward Snowden showed that the National Security Agency (NSA) had for years ordered telephone companies to turn over our domestic telephone calling records en masse.[1] The government had created a database of our phone calls going back years—a virtual time machine capable of reconstructing anybody's past communications, should they come under scrutiny in the future. The program, we learned, had been authorized under section 215 of the USA PATRIOT Act.[2]

But this authorization required an extraordinarily broad reading of the law. On its face, the statute permitted only the collection of records that were "relevant" to an authorized national security or counterterrorism investigation.[3] Yet behind closed doors, the Foreign Intelligence Surveillance Court (FISC) had stretched the statute to encompass *all* telephone records. Its theory was that all phone records are "relevant" to counterterrorism investigations because it is impossible to say in advance which will become useful in the future.[4]

1. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [http://perma.cc/5PLD-MUDX].

2. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287-88 (codified as amended at 50 U.S.C. §§ 1861-1862 (2012)).

3. 50 U.S.C. § 1861(b)(2)(B).

4. *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 812 (2d Cir. 2015) ("[T]he government takes the position that the metadata collected—a vast amount of which does not contain directly 'relevant' information, as the government concedes—are nevertheless 'relevant' because they may allow the NSA, at some unknown time in the future, utilizing its ability to sift through the trove of irrelevant data it has collected up to that point, to identify information that *is* relevant."); *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR-13-109, slip op. at 18-23 (FISA Ct. Aug. 29, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf [http://perma.cc/A57P-FU6R].

Apparently, nobody outside the government knew or foresaw that section 215 could be interpreted in this way.

Nobody, that is, except the companies who received these FISC orders and were obligated to carry them out by turning over all of their customers' telephone records on a daily basis.

The Snowden disclosures, and others that followed, illuminated a troubling feature of surveillance law: examining the statute books and other public sources of law can paint a radically incomplete or even misleading picture of how the government actually construes its legal authority to conduct surveillance. In other words, the government can reinterpret surveillance laws in secret, leaving the public in the dark if the rules have been stretched beyond recognition. This observation raises profound anxieties about public democratic control of the surveillance state. And these anxieties make a hard question very salient: how can we ensure a measure of transparency about how the law has been interpreted in practice?

This Essay argues that online service providers and other companies that mediate our digital communications are in a special position to enhance surveillance transparency. Because these private companies are subject to surveillance orders, they (or some of their employees) are privy to information that the rest of public is not: they know what kinds of information the government demands of them under a given surveillance law. For example, as alluded already, the phone companies that were ordered to comply with FISC surveillance orders knew all along that the government believed section 215 authorized bulk collection.[5]

If these companies could win the right to speak about the *kinds* of records the government is ordering them to disclose, they would be able to provide the public with crucial information about how the surveillance laws have been interpreted and applied in practice. This kind of limited disclosure would do much to allay democratic anxieties about secret reinterpretations of surveillance laws, and it need not reveal truly sensitive operational detail like the targets of surveillance, the circumstances in which particular surveillance tools are used, or other sensitive investigatory matters.

Unfortunately, the law forbids companies from engaging in this kind of speech. Gag orders routinely prevent companies from disclosing nearly everything about the surveillance orders they receive. Companies are forbidden even from providing a precise count of the number of orders received.

---

5. *See, e.g.*, Secondary Order, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc., No. BR-13-80 (FISA Ct. Apr. 25, 2013), http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order [http://perma.cc/5MM9-UAAS].

In this legal environment, it is simply off limits for a company to disclose how the government has construed its surveillance authority. But it need not remain so. This Essay offers a First Amendment strategy that online service providers (and others subject to surveillance orders) could pursue to attempt to improve surveillance transparency and reclaim their simple right to speak.

This First Amendment strategy was tested in a recent victory in court that may serve as a proof of concept for future legal challenges. The case was brought by Nicholas Merrill, a privacy advocate who previously operated Calyx Internet Access, a small service provider that counted various non-profit organizations among its clients.[6] In 2004, the FBI served an administrative subpoena, known as a National Security Letter (NSL), on Merrill. The NSL—one of tens of thousands issued every year—demanded that he turn over records about a client. It was accompanied by a gag order that forbade him from disclosing it to anyone—it did not even specify an exception for speaking with legal counsel. Merrill consulted a lawyer anyway. With the help of the ACLU and, more recently, the Media Freedom and Information Access Clinic (MFIA Clinic) at Yale Law School, he challenged the order over more than a decade of litigation, asserting his First Amendment right to speak about what, exactly, the FBI believed it could obtain with the NSL.

Last August, following the latest round of litigation, the federal district court in Manhattan finally invalidated the gag order in full. On November 30, 2015, the court's decision went into effect.[7] Merrill was finally able to reveal previously unconfirmed details about how the government has interpreted and applied the NSL statute in practice—for instance, he was able to disclose that the government believes it can lawfully compel production of individuals' cellphone location information, online purchase records, and IP addresses by

6. Merrill v. Lynch, No. 14-CV-9763, 2015 WL 9450650, at *2 (S.D.N.Y. Aug. 28, 2015) (unredacted order), http://isp.yale.edu/sites/default/files/page-attachments/merrill_v._lynch_-_unredacted_decision_vacating_gag_order.pdf [http://perma.cc/DK8L-SWCW]. Calyx Internet Access is now defunct. *Id*. Merrill is now the Executive Director of the Calyx Institute, a nonprofit education and research organization dedicated to educating the public about privacy in digital communications and developing platforms that service providers can use to build "privacy by design" into the architecture of their service offerings. *See About the Calyx Institute*, CALYX INST., http://www.calyxinstitute.org/about [http://perma.cc/6U9R-5Y2A]; *see also* Spencer Ackerman, *Nick Merrill: The Man Who May Unlock the Secrecy of the FBI's Controversial Subpoenas*, GUARDIAN (Sept. 17, 2015), http://www.theguardian.com/us-news/2015/sep/17/fbi-national-security-letters-nick-merrill-surveillance [http://perma.cc/5WET-HADM].

7. *See* Ellen Nakashima, *After 11 Years, a Curtain Is Lifted on a Secret FBI Demand for a Target's Data*, WASH. POST (Nov. 30, 2015), http://www.washingtonpost.com/world/national-security/after-11-years-a-curtain-is-lifted-on-a-secret-fbi-demand-for-a-targets-data/2015/11/30/aefc6838-9776-11e5-94f0-9eeaff906ef3_story.html [http://perma.cc/UQE2-BP7H].

issuing this kind of letter.[8] (Mr. Merrill was represented in the most recent phase of this litigation by the MFIA Clinic, where I was the supervising attorney on the case.)

This Essay explores how Merrill's victory might open up a new strategy for achieving greater transparency about the interpretation of surveillance laws. If online service providers set their minds to win the First Amendment right to tell the public what they know about the government's claimed surveillance powers, we might yet achieve a significant measure of transparency.

Part I describes the notion of surveillance transparency and how it has instigated legal reforms. Part II focuses on how online service providers may be well positioned to address the problem of surveillance transparency and uses NSLs as an example. Part III sketches the First Amendment legal strategy.

I. SURVEILLANCE TRANSPARENCY AND SURVEILLANCE REFORM

Over the past two-and-a-half years, we have had the most robust public discussion about surveillance in a generation. Edward Snowden's disclosures have had a remarkable half-life, fueling a debate about the scope of the government's surveillance powers that continues even today.[9] In newspapers, on the Internet, in all three branches of the federal government, and in state capitals, citizens have been debating what limits and safeguards should be placed on the government's surveillance powers.

This discussion led Congress to pass the USA FREEDOM Act, the first surveillance law in decades to curtail rather than expand surveillance powers.[10] That law effectively ends the section 215 bulk data-collection program, replacing it with a system in which the government must bring more specific requests for information to the phone companies.[11] At the same time, the U.S.

8. *See* Nicky Woolf, *Removing the Gag: How One Man Took On the FBI for Nearly 12 Years and Won*, GUARDIAN (Dec. 6, 2015), http://www.theguardian.com/law/2015/dec/06/fbi-national-security-letter-gag-order-nick-merrill [http://perma.cc/QAN6-SSQV].

9. *See, e.g.*, Michael Isikoff, *Eric Holder: The Justice Department Could Strike Deal with Edward Snowden*, YAHOO! POLITICS (July 6, 2015), http://www.yahoo.com/politics/eric-holder-the-justice-department-could-strike-123393663066.html [http://perma.cc/5PEY-9MEH] (quoting former Attorney General Eric Holder saying that Snowden's "actions spurred a necessary debate" and that "we are in a different place as a result of the Snowden disclosures").

10. United and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring (USA FREEDOM) Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (codified at 50 U.S.C. §§ 1872-1874 (2012) and 18 U.S.C. §§ 2280-2281, 2332 (2012)).

11. *See* USA FREEDOM Act §§ 101-107, 129 Stat. 269-74; *In re* Application of the Fed. Bureau of Investigation for an Order Requiring Prod. of Tangible Things, No. BR 15-75, slip op. at 10-11 (FISA Ct. June 29, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR%2015-75%20Misc%2015-01%20Opinion%20and%20Order_0.pdf [http://perma.cc/SY3S-5UWP] (discussing Congress's intent in passing the USA FREEDOM Act).

Court of Appeals for the Second Circuit and U.S. District Court for the District of Columbia recently found the mass call-tracking program unlawful.[12]

The legal challenges that led to those rulings were possible only because the surveillance program was publicly disclosed.[13] Indeed, if these programs had remained a secret, the extraordinary public ferment, policy debates, and legal reforms we have seen would have been impossible.

To those that view these democratic deliberations as a good thing, this insight provokes a number of anxieties. Have *other* surveillance laws been radically reinterpreted behind closed doors? Will the limits that we think various statutes impose on governmental surveillance prove illusory if the government continues to embroider them with layers of secret meaning? Must we depend on the happenstance of a public-spirited whistleblower willing to risk years in prison—or exile—to learn how the government understands the laws meant to constrain surveillance?

These anxieties have led many privacy advocates to search for a more durable (and legally sanctioned) way for the public to keep tabs on how the government interprets or reinterprets the surveillance laws in practice.[14] Those efforts have largely focused on two fronts: (1) Reforming the practice of the FISC so that it publishes its significant legal opinions interpreting the

---

12. *See* ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015) (holding that the bulk telephone collection program violated section 215 of the PATRIOT Act); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015), *reinstated on remand*, No. 13-851 (RJL), 2015 WL 6873127, at *14 (D.D.C. Nov. 9, 2015) (holding that plaintiffs would "likely succeed in showing that the [bulk collection program] is . . . an unreasonable search under the Fourth Amendment").

13. *Clapper*, 785 F.3d at 800-01 (holding that plaintiffs had standing only because they could prove, based on the FISC order originally disclosed by Snowden, that their telephone records had been collected); Obama v. Klayman, 800 F.3d 559, 565 (D.C. Cir. 2015) (Williams, J., writing separately) (holding that plaintiffs lacked standing because they were not customers of the telephone company named in the FISC order disclosed by Snowden and therefore could not establish with sufficient certainty that their records had been collected). *See generally* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1149-50 (2013) (holding that surveillance targets lack standing to sue unless they can show that they were targets of surveillance); Kashmir Hill, *How ACLU Attorney Ben Wizner Became Snowden's Lawyer*, FORBES (Mar. 10, 2014), http://www.forbes.com/sites/kashmirhill/2014/03/10/how-aclu-attorney-ben-wizner-became-snowdens-lawyer [http://perma.cc/97ZM-G5H9] ("'In my first conversation with Snowden, one of his first questions for me was, "Do you have standing now?"' says [Snowden's lawyer Ben] Wizner. 'The first document from the Guardian was about Verizon handing over the metadata for millions of its customers. One of its customers was the ACLU and he gave us a ticket to federal court.'").

14. Transparency about how surveillance laws have been interpreted is particularly important because, unlike other national security policies, surveillance often leaves no public trace. Whereas the public will be tipped off to secret policies regarding, say, targeted killings or harsh interrogation by the missile strikes and broken bodies they produce, the public will generally remain in the dark about surveillance programs that raise legal doubts because such programs are designed precisely not to be detected.

surveillance laws;[15] and (2) Seeking information directly from the executive branch through Freedom of Information Act lawsuits.[16] Both of these strategies seek disclosure from officials who know about the secret legal interpretations of surveillance laws. But there is a third set of actors, often overlooked, who have that knowledge too: the technology companies forced to carry out the government's surveillance orders.

II. ONLINE SERVICE PROVIDERS AND SECRET INTERPRETATIONS OF LAW

Because private online platforms mediate so much of our communication and commerce, government surveillance efforts must focus on obtaining information from them.[17] The government has many tools at its disposal to obtain this information, many of which involve an explicit demand to an online company that it turn over client data. For instance, in the context of national security and counterterrorism investigations, the FBI can issue NSLs directly to online companies without judicial approval, requiring them to disclose a variety of business records.[18] Various provisions of the Foreign Intelligence Surveillance Act (FISA) authorize surveillance of the content of communications with prior approval from the FISC.[19] Because online companies receive subpoenas and court orders under these kinds of authorities, they know firsthand how the government is using each one of them. They know, in other words, how the authorities are being construed in secret.

---

15. *See In re* Orders of this Court Interpreting Section 215 of the Patriot Act, No. Misc. 13-02, 2014 WL 5442058 (FISA Ct. Aug. 7, 2014); Motion of the American Civil Liberties Union et al. for the Release of Court Records, *In re* Ops. & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act, No Misc. 13-08 (FISA Ct. Nov. 7, 2013); *see also* USA FREEDOM Act of 2015, Pub. L. No. 114-23, §§ 402, 602, 129 Stat. 268, 281-82 (to be codified at 50 U.S.C. § 1871) (directing the Attorney General and Director of National Intelligence to declassify or provide unclassified summaries of significant FISC opinions). The author is among counsel for the movants in both cases.

16. *See, e.g.*, ACLU v. FBI, 59 F. Supp. 3d 584, 584 (S.D.N.Y. 2014); Complaint for Injunctive Relief at 1, ACLU v. NSA, No. 1:13-cv-09198 (S.D.N.Y. Dec. 30, 2013); Complaint for Injunctive Relief at 1, Elec. Frontier Found. v. Dep't of Justice, No. 4:11-cv-05221 (N.D. Cal. Oct. 26, 2011). The author is among counsel for the plaintiffs in the latter case.

17. Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296 (2014).

18. *See* 18 U.S.C. § 2709 (2012).

19. FISA includes several distinct surveillance authorities including the business records provision authorizing collection of "any tangible things (including books, records, papers, documents, and other items)," 50 U.S.C. § 1861 (2012); the provision authorizing the use of pen registers and trap and trace devices, 50 U.S.C. § 1842 (2012); the provisions authorizing targeted electronic surveillance, 50 U.S.C. §§ 1804-05 (2012); and the FISA Amendments Act provisions authorizing broad programmatic surveillance without individualized warrants, 50 U.S.C. § 1881a (2012).

There is good reason to believe that, even now, the government is construing its surveillance authorities in ways that are surprising, aggressive or otherwise troubling. Take, for instance, the government's authority to issue NSLs, which it uses more than 10,000 times a year.[20] The law permits the FBI to order disclosure of "subscriber information and toll billing records information" as well as "electronic communication transactional records" (ECTR).[21] The scope of this warrantless surveillance authority therefore depends crucially on what constitutes ECTR. But the statute does not define the term. Even though the statute has included the phrase since 1986,[22] the judiciary has not had an opportunity to interpret its meaning.[23]

Until November 30, 2015, when Merrill won the right to speak about the NSL his company received in 2004, the only official legal interpretation of ECTR was found in a 2008 memo from the Department of Justice's Office of Legal Counsel to the FBI. That memo explains, in a footnote, that the inclusion of the phrase ECTR "clarif[ies] that NSLs can extend to other types of services" and "reaches only those categories of information parallel to subscriber information and toll billing records for ordinary telephone service."[24]

But this footnote hardly clarified anything. The architecture of modern online services is so unlike "ordinary telephone service" that it is impossible to know what online records the FBI will regard as "parallel to" ordinary toll billing records. Moreover, because online service providers don't typically bill users on a per-transaction basis, as legacy phone companies did, there is no telling which transactions the FBI believes are "parallel" to the call logs on a phone bill. Plus, online companies maintain a wide variety of "transactional" data about us that phone companies never did. Internet service providers know the websites we have viewed. Google keeps records of our searches. Facebook keeps records of our "friends," our communications, and what we "like." This just scratches the surface—Internet companies have gathered vast troves of data about us.

---

20. Letter from Peter J. Kadzik, Assistant Att'y Gen., to Chairmen of the Cong. Intelligence and Judiciary Comms. 3 (Apr. 20, 2015), http://fas.org/irp/agency/doj/fisa/2014rept.pdf [http://perma.cc/GPZ9-3Q27].

21. 18 U.S.C. § 2709(a) (2012).

22. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, § 201, 100 Stat. 1848, 1867 (codified as amended at 18 U.S.C. § 2709 (2012)).

23. In Merrill's case, the government withdrew the demand for records contained in the NSL, thereby mooting his challenge to the lawfulness of its disclosure order. *See* John Doe, Inc. v, Mukasey, 549 F.3d 861, 869 (2d Cir. 2008).

24. Memorandum Opinion for the General Counsel FBI, Requests for Information Under the Electronic Communications Privacy Act, 32 Op. O.L.C. 145, 147 n.3 (Nov. 5, 2008), http://www.justice.gov/sites/default/files/olc/opinions/attachments/2015/06/23/op-olc-v032-p0145.pdf [http://perma.cc/ZLS4-3938].

The OLC memo interpreting the scope of NSL authority thus left the most important question unanswered—which parts of the universe of customer data does the FBI believe constitute ECTR? In other words, how much of the data we create online, both intentionally and unintentionally, can the FBI gather up simply by issuing a letter?

As a result of Merrill's successful lawsuit, he was able to disclose publicly a list of sixteen specific categories of information that the FBI believes it can obtain—and believed it could obtain from him—using an NSL.[25] For instance, the public now knows that the FBI claims the authority to use NSLs to obtain records of an individual's cell phone location based on cell tower pings; a person's record of online purchases; and the IP addresses assigned to a user, which can serve to unmask anonymous online speech.[26] The list that Merrill is now able to disclose is not exhaustive, representing only the categories specified in the NSL that he received more than a decade ago. But even this limited disclosure has raised significant concerns about whether these kinds of data should be accessible to the FBI simply by writing a letter, without any genuine prospect of judicial oversight.[27]

Other surveillance authorities contain similar ambiguities that may have enormous consequences for the scope of the government's surveillance authority. For instance, even though the newly amended Section 215 no longer authorizes bulk telephone data collection, questions remain about how other key provisions will be interpreted, including the new "specific selection term" targeting requirement.[28] Nor can we be sure how broadly the FISC has construed the government's authority under Section 702 of the FISA Amendment Act, which goes beyond particularized court orders targeting individuals and instead appears to permit programmatic bulk surveillance of

---

25. *See Attachment to 2004 NSL*, FED. BUREAU INVESTIGATION, http://isp.yale.edu/sites/default/files/page-attachments/merrill_v._lynch_-_unredacted_attachment_to_2004_nsl.pdf [http://perma.cc/T9MS-BJAN].

26. Merrill v. Lynch, No. 14-CV-9763, 2015 WL 9450650, at *7, *9 (S.D.N.Y. Aug. 28, 2015) (unredacted order), http://isp.yale.edu/sites/default/files/page-attachments/merrill_v._lynch_-_unredacted_decision_vacating_gag_order.pdf [http://perma.cc/DK8L-SWCW]. The government has stated that, as a matter of policy, it does not currently seek cell phone location information using NSLs but that it believes it has the legal authority to do so. *Id.* at *9.

27. David Kravets, *The National Security Letter Spy Tool Has Been Uncloaked, and It's Bad*, ARSTECHNICA (Nov. 30, 2015, 2:25 PM), http://arstechnica.com/tech-policy/2015/11/the-national-security-letter-spy-tool-has-been-uncloaked-and-its-bad [http://perma.cc/DTY9-MQ95]; Steve Nelson, *Internet Provider Gagged for Decade Reveals What FBI Wanted Without Warrant*, U.S. NEWS & WORLD REP. (Nov. 30, 2015, 4:18 PM), http://www.usnews.com/news/articles/2015/11/30/internet-provider-gagged-for-decade-reveals-what-fbi-wanted-without-warrant [http://perma.cc/NMG4-SV97].

28. USA FREEDOM Act of 2015, Pub. L. No. 114-23, §§ 101, 103, 107, 129 Stat. 268, 269-74 (to be codified at 50 U.S.C. § 1861 (2012)).

the content of electronic communications.[29] Online service providers who receive surveillance demands from the government would be able to fill in pieces of these puzzles.

As it stands, however, online companies are almost entirely forbidden from discussing the surveillance orders they face. All of the surveillance laws discussed thus far include gag order provisions.[30] These gags are not time-limited and do not simply prevent companies from tipping off the government's targets. They are nearly absolute, forbidding discussion of nearly any aspect of the surveillance order. They typically prohibit companies even from acknowledging whether they have received an order or disclosing exactly how many they have received. As it stands now, it is strictly out of bounds for companies (or their employees) to describe the kinds of information that the government has sought to obtain.[31]

III. A FIRST AMENDMENT STRATEGY FOR SURVEILLANCE TRANSPARENCY

Even though these gag orders would appear to preclude online service providers from becoming outspoken agents for surveillance transparency, there may yet be a way for them to do so. The First Amendment, after all, commands that Congress "make no law . . . abridging the freedom of speech,"[32] and there have now been a number of First Amendment challenges to these kinds of surveillance gag orders.[33] So far, however, most plaintiffs asserting their free speech rights have primarily sought the freedom to disclose that they have *received* a surveillance order, or to disclose the precise the number they have received. But disclosing these statistical facts will not shed much light on how the government is construing its statutory authority in practice. Moreover, unlike the *Merrill* case, these challenges do not ask courts to confront directly the question of whether the government may impose permanent gag orders on private citizens in order to keep secrets about the scope of the surveillance powers it claims.

---

29. For a succinct summary of what has been made public about the FISC's consideration of Section 702, see EDWARD C. LIU ET AL., CONG. RESEARCH SERV., R43459, OVERVIEW OF CONSTITUTIONAL CHALLENGES TO NSA COLLECTION ACTIVITIES 11-12 (2015), http://fas.org/sgp/crs/intel/R43459.pdf [http://perma.cc/JD93-CCBX].

30. *See* 18 U.S.C. § 2709(c)(1) (2012); 50 U.S.C. §§ 1805(c)(2)(B)-(C), 1842(d)(2)(B)(ii), 1861(d), 1881a(h)(1)(B) (2012).

31. *See* sources cited *supra* note 15; *see also* USA FREEDOM Act of 2015 § 603, 129 Stat. at 295-97.

32. U.S. CONST. amend. I.

33. *See infra* notes 41-49 and accompanying text.

Thus, if tech companies and service providers are to educate the public about what surveillance laws mean in practice, the next wave of First Amendment litigation against surveillance gag orders must focus on establishing their right to speak about *how* the government has used its surveillance authority, not simply the fact that it has done so or how often.

A brief tour of First Amendment litigation against surveillance gag orders will help explain the legal landscape that awaits such challenges. The first wave of litigation began a little more than a decade ago, focusing on the nondisclosure orders that routinely accompany NSLs. These challenges were brought mainly by small, non-profit groups: Calyx Internet Access and its president, Nicholas Merrill,[34] the Internet Archive,[35] and a group of Connecticut librarians.[36] Each group ultimately won the right to say that they had in fact received an NSL. But none of them won the right to disclose what kinds of information the FBI demanded, and so none could describe how the FBI interpreted the key ambiguous language in the NSL statute authorizing it to obtain ECTR.[37]

The second wave of surveillance gag litigation began in 2011, when certain still-unnamed companies filed suit to challenge again the constitutionality of NSL gag orders.[38] But in 2013, following the Snowden disclosures, challenges to surveillance gag orders truly went mainstream. Five major tech companies—

---

34. *See Doe v. Holder*, ACLU (Nov. 17, 2009), http://www.aclu.org/cases/doe-v-holder [http://perma.cc/Z485-HYNP] (discussing Merrill's role as John Doe in *John Doe, Inc. v. Mukasey*, 549 F.3d 861 (2d Cir. 2008)).

35. Complaint for Declaratory and Injunctive Relief, Internet Archive v. Mukasey, No. 07-6346-CW (N.D. Cal. filed Dec. 14, 2007), http://www.eff.org/node/55596 [http://perma.cc/B67Q_-5ZTL]; *see also Internet Archive et al v Mukasey et al*, ELEC. FRONTIER FOUND., http://www.eff.org/cases/archive-v-mukasey [http://perma.cc/U6C9-WSYS].

36. Doe v. Gonzales, 449 F.3d 415 (2d Cir. 2006); *Librarians' NSL Challenge*, ACLU, http://www.aclu.org/librarians-nsl-challenge [http://perma.cc/BJ3W-94HV].

37. *See* Doe v. Holder, 703 F. Supp. 2d 313, 316-18 (S.D.N.Y. 2010) (upholding gag with respect to document identifying the categories of records sought in response to an NSL).

38. *In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064 (N.D. Cal. 2013) (holding that the NSL gag order provisions violated both the First Amendment and separation of powers principles); Petition of Plaintiff [Redacted] To Set Aside National Security Letter and Nondisclosure Requirement Imposed in Connection Therewith; Memorandum of Points and Authorities, *In re* Nat'l Sec. Letter Issued to [Redacted], No. 11-cv-2173 (N.D. Cal. filed May 2, 2011), http://www.eff.org/sites/default/files/filenode/petition-redacted.pdf [http://perma.cc/JU49-U3MB]. While the case was pending on appeal, Congress amended nondisclosure provisions of the NSL statute and the Ninth Circuit subsequently vacated the decision and remanded to the district court to consider the constitutionality of the revised statute. *See* Order, *In re* Nat'l Sec. Letter, No. 13-15957 (9th Cir. Aug. 24, 2015), http://cdn.ca9.uscourts.gov/datastore/general/2015/08/31/13-15957%20Order%208-24.pdf [http://perma.cc/N44W-AH7C]; *see also* Memorandum and Order, Loretta Lynch v. Under Seal, No. 15-cv-1180 (D. Md. Sep. 17, 2015), ECF No. 26-10 (redacted decision unsealed by order dated Dec. 14, 2015) (rejecting challenge to NSL gag order by unidentified company).

Google, Yahoo, Microsoft, Facebook, and LinkedIn—opened a new front by filing suit in the FISC asserting a First Amendment right to publish aggregate statistics about the number of surveillance orders they had received from that court. Like the NSL lawsuits before, however, the FISC lawsuit did not envision a role for the companies to disclose the *kinds* of records sought or other information that might illuminate how the FISC interprets FISA.[39]

The fact many of the largest tech companies have entered the fray has the potential to change the course of the legal dispute over surveillance law transparency. These companies bring enormous legal resources to the table, as well as formidable political clout. By taking up a fight that had previously been populated mostly by small non-profits, privacy activists, and civil libertarians, they can make surveillance transparency a mainstream concern. They could stand as a major institutional counterweight pressing for transparency on surveillance policy.[40] Indeed, since they have become involved, the transparency landscape has already begun to shift.[41]

---

39. Order, *In re* Amended Motion for a Declaratory Judgment of a First Amendment Right to Publish Aggregate Info. About FISA Orders, No. Misc. 13-03 (FISA Ct. Sept. 18, 2013), http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Order-10.pdf [http://perma.cc/JQJ7-AVGY].

40. The newly assertive and powerful role of the large tech companies in matters of technology and surveillance has been illustrated most recently by Apple's public confrontation with the FBI regarding a court order that would require Apple to create software to disable certain security protections of an iPhone. *See* Timothy B. Lee, *Apple's Battle with the FBI over iPhone Security, Explained*, VOX (Feb. 17, 2016), http://www.vox.com/2016/2/17/11037748/fbi-apple-san-bernardino [http://perma.cc/4MFA-JZ4D]. At least five major tech companies—Facebook, Google, Microsoft, Twitter, and Yahoo—have signaled that they will support Apple in its court fight with the FBI. *See* Katie Benner et al., *Apple Goes to Court, and F.B.I. Presses Congress To Settle iPhone Privacy Fight*, N.Y. TIMES (Feb. 25, 2016), http://www.nytimes.com/2016/02/26/technology/apple-unlock-iphone-fbi-san-bernardino-brief.html [http://perma.cc/5GPC-B8B4].

41. The lawsuits brought by Google and others in the FISC resulted in a settlement agreement that permitted companies to report the number of orders they received within wide bands—for example, between 0 and 999, between 1000 and 1999, etc. *See* Letter from James M. Cole, Deputy Att'y Gen., to Colin Stretch, Vice President & Gen. Counsel, Facebook, et al., (Jan. 27, 2014), http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf [http://perma.cc/9S86-RQNJ]. Unsatisfied with this state of affairs, Twitter filed a separate lawsuit in district court attacking these disclosure guidelines primarily on the basis that the First Amendment protects its right to disclose whether it has in fact received *zero* requests, something the settlement did not permit because it required disclosure in bands starting at zero. *See, e.g.*, Complaint for Declaratory Judgment, Twitter, Inc. v. Holder, No. 14-cv-4480 (N.D. Cal. Oct. 7, 2014), http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/07/National-Security/Graphics/Complaintnew.pdf [http://perma.cc/M9QH-YSEG]. Congress subsequently codified a somewhat more permissive version of the settlement guidelines in the USA FREEDOM Act. *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 603, 129 Stat. 267, 295. The Twitter lawsuit remains ongoing, now challenging the

Meanwhile, Nicholas Merrill, one of the first-wave plaintiffs, went back to court. This time, he focused squarely on winning the right to speak about the contents of the NSL his service company had received, and, specifically, the scope of authority the FBI claimed to compel his company to disclose ECTR.[42] The case may therefore serve as a bellwether for larger tech companies and service providers seeking to make similar disclosures.

By the time he filed his second lawsuit, in 2014, it was more than 10 years after the NSL had been served. The surrounding circumstances had changed, neutralizing many of the government's arguments for maintaining secrecy. The investigation had ended, the FBI had long since withdrawn its demand for Merrill's records, and it had conceded that there was no longer any need to conceal the target of the investigation.[43] Thus, the FBI could no longer argue that secrecy was necessary to protect the integrity an ongoing investigation or to avoid tipping off the target. Instead, as the district court put it, "the asserted government interest in keeping the [list of categories sought] confidential [was] based solely on protecting law enforcement sensitive information that is relevant to *future* or *potential* national security investigations."[44]

The case thus squarely pitted the First Amendment right to speak against the government's interest in keeping its surveillance methods secret. On the one hand, a private citizen asserted a right to speak truthful information about the government's activities and its secret interpretation of a statute—clearly a matter of core public concern.[45] On the other hand, the government asserted that preventing this disclosure was essential to protect investigatory methods for as long as the FBI deemed necessary.[46]

The *Merrill* case presented a number of powerful First Amendment arguments that would be available to a tech company facing a gag order in this posture. First, facts already in the public domain about the government's

constitutionality of this provision of the USA FREEDOM Act rather than the DAG Letter. *See* Twitter, Inc. v. Lynch, No. 14-cv-4480, 2015 WL 5970295 (N.D. Cal. Oct. 14, 2015).

42. Complaint for Injunctive Relief, Merrill v. Holder, No. 14-cv-9763 (S.D.N.Y. Dec. 11, 2014), http://isp.yale.edu/sites/default/files/page-attachments/merrill_v._holder_-_file-stamped_complaint.pdf [http://perma.cc/FVY7-BEX3]. Mr. Merrill is represented by the Media Freedom and Information Access Clinic at Yale Law School. The author serves as Abrams Clinical Fellow in the clinic and is the supervising attorney on the case.

43. Merrill v. Lynch, No. 14-CV-9763, 2015 WL 9450650, at *9-10 (S.D.N.Y. Aug. 28, 2015) (unredacted order), http://isp.yale.edu/sites/default/files/page-attachments/merrill_v._lynch_-_unredacted_decision_vacating_gag_order.pdf [http://perma.cc/DK8L-SWCW].

44. *Id.* at 28.

45. *See id.* at 32.

46. *See id.* at 31-32; Reply Memorandum of Law in Support of the Government's Motion to Dismiss or for Summary Judgment, and in Opposition to Plaintiff's Motion for Summary Judgment at 4-8, *Merrill*, No. 14-cv-9763 (S.D.N.Y. filed July 31, 2015), http://cryptome.org/2015/08/merrill-042.pdf [http://perma.cc/GXF5-NZB8].

surveillance powers might render a gag order untenable under the First Amendment.[47] Second, and more categorically, a gag order is a highly suspect content-based restriction on speech because "on its face [it] draws distinctions based on the message [the] speaker conveys" and because it "cannot be justified without reference to the content of the regulated speech."[48] Third, gag orders can be likened to classic prior restraints, which are generally forbidden by the First Amendment. Like a prior restraint, the gag order prevents speech in advance, in circumstances where the speaker is a private citizen who has not agreed to be censored.[49] Fourth, when the investigation concludes but the gag order remains, it effectively becomes an indefinite prohibition. Historically, the First Amendment has been especially hostile to such unlimited restrictions.[50] Finally, the gag order is anathema to the First Amendment precisely because the information it restrains is important, true and newsworthy speech regarding "the manner in which government is operated"—specifically, the manner in which it interprets and carries out a statute.[51] Surveillance gag

---

47. For instance, Merrill pointed out that it was no secret that every category of information sought using an NSL could be obtained by the government using *some* authority. So disclosing that such information can be obtained using *NSLs*, in particular, would not tip off any targets, but would simply inform the public about how broadly this warrantless surveillance power had been construed. *See* 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, at 17-22, *Merrill*, No. 14-cv-9763 (S.D.N.Y. filed June 26, 2015).

48. Reed v. Town of Gilbert, 135 S. Ct. 2218, 2227 (2015) (internal quotation marks omitted); *see* Memorandum of Law in Support of Plaintiff Nicholas Merrill's Motion for Summary Judgment at 15, *Merrill*, No. 14-cv-9763 (S.D.N.Y. Mar. 20, 2015) [hereinafter Merrill Brief].

49. *See* Brief of Amici Curiae Floyd Abrams Institute for Freedom of Expression and First Amendment Scholars in Support of the Parties Under Seal at 3-14, *In re* Nat'l Security Letter, Nos. 13-15957 & 13-16731 (9th Cir. filed Mar. 31, 2014), http://cdn.ca9.uscourts.gov/datastore/general/2014/05/23/13-15957,13-16731Floyd.pdf [http://perma.cc/N7YH-MVV4]; Rebecca Wexler, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, 124 YALE L.J. F. 158 (2014), http://www.yalelawjournal.org/forum/warrant-canaries-and-disclosure-by-design [http://perma.cc/8BR8-VYJQ].

50. *See, e.g.*, Butterworth v. Smith, 494 U.S. 624, 635 (1990) (stating, with respect to a nondisclosure obligation imposed on a grand jury witness, that the "ban [that] extends not merely to the life of the grand jury but into the indefinite future" is indefensible under the First Amendment); *Doe*, 449 F.3d at 422 ("A permanent ban on speech seems highly unlikely to survive the test of strict scrutiny, one where the government must show that the statute is narrowly tailored to meet a compelling government interest.") (Cardamone, J., concurring); Merrill Brief, *supra note* 48, at 13-14.

51. Mills v. Alabama, 384 U.S. 214, 218-19 (1966); *see also* Landmark Commc'ns, Inc. v. Virginia, 435 U.S. 829, 838-39 (1978) ("Whatever differences may exist about interpretations of the First Amendment, there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs." (quoting *Mills*, 384 U.S. at 218)).

orders thus "deprive[the community] of informed opinions on important public issues."[52]

The upshot of most of these arguments would be to subject the gag order to the most stringent test of constitutional necessity.[53] The Court, faced with such a challenge, would have to judge whether the government may suppress truthful speech regarding the manner in which the government has interpreted and applied a surveillance law. The government would undoubtedly claim a compelling interest in protecting investigatory methods and, by extension, national security.[54] But it is not at all clear that the specific interest in preserving the secrecy of an investigatory tool is sufficiently strong to justify a restraint of truthful speech about the scope of the government's claimed authority.[55] And even if the government could state a sufficiently compelling interest, the question of whether a gag order is strictly necessary and narrowly tailored to serve that interest is a difficult case-specific question. So far, no court has held that, outside of an ongoing investigation, the government may permanently ban public discussion on investigatory techniques.[56]

In the *Merrill* case, the district court sidestepped a direct constitutional confrontation, ruling instead on the first basis mentioned above: that the government could not meet its burden to justify the continuing necessity of the

---

52. Garcetti v. Ceballos, 547 U.S. 410, 419-20 (2006) (quoting San Diego v. Roe, 543 U.S. 77, 82 (2004) (per curiam)) (holding that public employees, whose free speech rights are limited because they have taken a job with the government, nevertheless retain some First Amendment protection for speech about "matters of public concern" because of the "importance of promoting the public's interest in receiving the well-informed views of government employees engaging in civic discussion"). Like government employees, individuals working at online companies are particularly well-informed regarding government surveillance and have much to contribute to public discussion. But unlike government employees, these are private citizens who have not ceded their free speech rights by entering government and they thus enjoy full First Amendment protections. *See* John Doe, Inc. v. Mukasey, 549 F.3d 861, 877-78 (2d Cir. 2008).

53. *See, e.g.*, *Reed*, 135 S. Ct. at 2222 (holding that content-based restrictions are subject to strict scrutiny); *Butterworth*, 494 U.S. at 626, 631-33, 635-36 (holding that permanent or indefinite bans on speech are constitutionally suspect); Neb. Press Ass'n v. Stuart, 427 U.S. 539, 562, 569-70 (1976) (holding that prior restraints are unjustified except in the narrowest circumstances); *see also* In re Nat'l Security Letter, 930 F. Supp. 2d at 1075-76 (holding that strict scrutiny applies to NSL gag orders), *vacated and remanded on other grounds*, No. 13-15957 (9th Cir. Aug. 24, 2015), http://cdn.ca9.uscourts.gov/datastore/general/2015/08/31/13-15957%20Order%208-24.pdf [http://perma.cc/GP57-AWQP].

54. *See* sources cited *supra* note 53.

55. *See* 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, *supra* note 47, at 2-13 (arguing that the First Amendment cannot be used to suppress portions of a surveillance order that disclose the interpretation of key statutory terms).

56. *See id.* at 13-14 (arguing that the government has failed to identify any cases in which the First Amendment was abridged to suppress discussion of an investigatory tool).

gag order because there was already significant information in the public domain suggesting what kinds of information the FBI obtained using NSLs.[57] Because of this public information, the Court concluded that the government could not show that disclosure would create a substantial risk of the harms the government asserted.[58] As a result, the Court ordered the gag order to be lifted in full, and the government declined to appeal.

CONCLUSION

Tech companies and online service providers should take note of Merrill's success. They should consider similar challenges to other sources of surveillance authority. In the interest of their customers' privacy (and their own reputations) online companies should strongly consider mounting First Amendment challenges to gag orders—particularly longstanding gag orders in closed investigations—that prevent them from discussing secret surveillance techniques and their underlying legal interpretations.

Such lawsuits could become an important part of our system of surveillance transparency and accountability. In a future challenge to another gag order, the court may not be able to avoid the stark constitutional question, as the court did in Merrill's case. Do national security concerns justify imposing permanent, involuntary restraints on speech about the government's interpretations of surveillance laws? Can gag orders not only protect the integrity of a particular ongoing investigation, but also prevent companies and citizens from disclosing their knowledge of how the government uses a particular surveillance tool in general?

Merrill's recent victory suggests that the courts will not easily acquiesce in such restrictions on free speech.[59] Moreover, the mere fact of such First Amendment challenges would serve to focus the government's attention on questions of surveillance transparency and could prompt voluntarily disclosures by the executive branch or stepped-up oversight by Congress.

Perhaps in the future we will not need to rely on the happenstance of another Snowden to learn whether the limits written into the country's surveillance laws have been contorted in secret. The combined power of the First Amendment and Silicon Valley may yet be strong enough to ensure a measure of transparency about surveillance.

---

57. Merrill v. Lynch, No. 14-CV-9763, 2015 WL 9450650, at *3, *9 (S.D.N.Y. Aug. 28, 2015) (unredacted order), http://isp.yale.edu/sites/default/files/page-attachments/merrill_v._lynch_-_unredacted_decision_vacating_gag_order.pdf [http://perma.cc/DK8L-SWCW].

58. *Id*. at 17-18.

59. *Id*. at 29-32; Doe v. Gonzales, 449 F.3d 415, 422 (2d Cir. 2006) (Cardamone, J.,concurring).

Jonathan Manes is a Research Scholar in Law; Abrams Clinical Fellow, Information Society Project; and Clinical Lecturer in Law at Yale Law School.

Preferred Citation: Jonathan Manes, *Online Service Providers and Surveillance Law Transparency*, 125 YALE L.J. F. 343 (2016), http://www.yalelawjournal.org/forum/online-service-providers-and-surveillance-law-transparency.