Washington University Journal of Law & Policy

Volume 47 *Intellectual Property: From Biodiversity to Technical Standards*

2015

Legal Responses and Countermeasures to National Security Letters

Brett Weinstein

Legal Responses and Countermeasures to National Security Letters

Brett Weinstein*

INTRODUCTION

In early June of 2013, governmental surveillance suddenly and dramatically entered the public consciousness, prompting a torrent of debate and backlash. *The Guardian* published a top secret court order requiring Verizon to hand over all telephone call records to the National Security Agency (NSA); the *Washington Post* disclosed a secret but widespread Internet surveillance program, and months of similar revelations followed, all stemming from leaks by former NSA contractor, Edward Snowden.[1] As a result, the public and the press began to question the tools that the government uses for surveillance, including National Security Letters (NSLs), and the relationship between the government and the technology and telecommunications companies that seemingly possess all personal and private information generated in the modern, digital world.[2]

---

* J.D. (2015), Washington University School of Law; B.A. (2010), Emory University. Thanks to Professor Neil Richards for his guidance regarding this Note, the *Journal* staff for assistance editing, my grandfather, Max Weinstein, for proofreading, and my parents, family, and others for their ideas, encouragement, and support.

1. Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily*, THE GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order, *available at* http://perma.cc/DU3S-28JB; Barton Gellman & Laura Poitras, *U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program*, WASH. POST (June 6, 2013), http://articles.washingtonpost.com/2013-06-06/news/39784046_1_prism-nsa-u-s-servers, *available at* http://perma.cc/QNJ5-E3FF; Paul Szoldra, *SNOWDEN: Here's Everything We've Learned In One Year Of Unprecedented Top-Secret Leaks*, BUS. INSIDER (June 7, 2014), http://www.businessinsider.com/snowden-leaks-timeline-2014-6, *available at* http://perma.cc/RM6G-Y2Q9; Matthew Cole & Mike Brunker, *Edward Snowden: A Timeline*, NBC NEWS (May 26, 2014), http://www.nbcnews.com/feature/edward-snowden-interview/edward-snowden-timeline-n114871, *available at* http://perma.cc/2WP5-QNG6.

2. The *New York Times* editorial board stated, "[T]he administration has now lost all credibility on this issue. Mr. Obama is proving the truism that the executive branch will use any

Facing pressure from customers and the public, businesses were pressed to explain publically what records the government secretly requests, how often it makes such requests, and how often they comply.[3] The government prohibited businesses from publicly disclosing the answers to these questions, but several major technology companies filed lawsuits hoping to allow disclosure of these figures.[4] Several smaller, privacy-focused companies also faced governmental demands for user data or cooperation and chose to either cease functioning or change their business practices in an effort to avoid compromising their customers' expectation of privacy.[5]

---

power it is given and very likely abuse it." Editorial Board, *President Obama's Dragnet*, N.Y. TIMES (June 6, 2013), http://www.nytimes.com/2013/06/07/opinion/president-obamas-dragnet.html?pagewanted=all, *available at* http://perma.cc/F5BB-67BW. The editorial board expressed even more distrust two months later, stating,

> Apparently no espionage tool that Congress gives the National Security Agency is big enough or intrusive enough to satisfy the agency's inexhaustible appetite for delving into the communications of Americans. Time and again, the N.S.A. has pushed past the limits that lawmakers thought they had imposed to prevent it from invading basic privacy, as guaranteed by the Constitution.

Editorial Board, *Breaking Through Limits on Spying*, N.Y. TIMES (Aug. 8, 2013), http://www.nytimes.com/2013/08/09/opinion/breaking-through-limits-on-spying.html, *available at* http://perma.cc/3BZL-RUXP. New organizations were founded to oppose surveillance, such as Restore the Fourth and Stop Watching Us. RESTORE THE FOURTH, *FAQ*, http://www.restorethe4th.com/faq/ (last visited Dec. 24, 2014); STOP WATCHING US, *Frequently Asked Questions*, https://rally. stopwatching.us/faq.html (last visited Dec. 24, 2013). A little over a year following Snowden's disclosures, a poll found most American citizens felt it unacceptable for the US government to monitor American citizen's communications. PEW RESEARCH CTR., *Global Opinions of U.S. Surveillance: United States* (July 14, 2014), http://www.pewglobal.org/2014/07/14/nsa-opinion/country/united-states/, *available at* http://perma.cc/8HMY-WTSY.

3. The government allowed Google to publish a wide range of the number of NSLs it receives yearly prior to Snowden's revelations—between zero and 999. However, the technology companies sought to disclose these numbers in greater detail. David Kravets, *Google Says the FBI Is Secretly Spying on Some of Its Customers*, WIRED (Mar. 5, 2013), http://www.wired.com/threatlevel/2013/03/google-nsl-range/, *available at* http://perma.cc/8V25-7U88; Kim Zetter, *Google Seeks OK From Feds to Disclose Stats on Secret Court Orders*, WIRED (June 13, 2013), http://www.wired.com/threatlevel/2013/06/google-fisa-requests/, *available at* http://perma.cc/EFB2-9U2N.

4. Ewen MacAskill, *Yahoo files lawsuit against NSA over user data requests*, THE GUARDIAN (Sept. 9, 2013), http://www.theguardian.com/world/2013/sep/09/yahoo-lawsuit-nsa-surveillance-requests, *available at* http://perma.cc/GSE9-2U7U; Liz Gannes, *U.S. Opposes Tech Companies' Requests to Disclose Surveillance*, ALL THINGS D (Oct. 2, 2013), http://allthingsd.com/20131002/u-s-opposes-tech-companies-requests-to-disclose-surveillance/, *available at* http://perma.cc/WVL7-9BXL.

5. Russell Brandom, *Lavabit vs. the FBI: the fight for the soul of American Software*, THE VERGE (Oct. 7, 2013), http://www.theverge.com/2013/10/7/4812102/lavabit-and-the-fight-

The government has several tools at its disposal when it seeks to obtain information as part of a national security investigation. First, it may use a traditional grand jury subpoena, however, the recipient is usually under no obligation to keep the subpoena secret.[6] Second, the government may seek an order from the Foreign Intelligence Surveillance Court (FISC), which the recipient must keep secret, for the production of documents or things.[7] Finally, the government may, without any judicial review or approval, issue an NSL to compel a recipient to produce certain kinds of records while keeping the issuance of the NSL a secret.[8] NSLs are often deployed at the beginning of national security investigations to determine who a suspected terrorist is associated with.[9] In addition to furthering a national security investigation, the information gained from an NSL can then be used for a more onerous Foreign Intelligence Surveillance Act application.[10]

Although neither judicial review nor approval is required, the government must certify that the records sought through an NSL are for use in a national security investigation.[11] NSLs are usually issued by the Federal Bureau of Investigation (FBI), and the records sought can include subscriber information, toll billing information, and other electronic communication transaction records.[12]

---

for-the-soul-of-american-software, *available at* http://perma.cc/FRL3-HYHV; Joe Mullin, *After Lavabit Shutdown, Another Encrypted E-Mail Service Closes*, ARS TECHNICA (Aug. 9, 2013), http://arstechnica.com/tech-policy/2013/08/in-wake-of-lavabit-shutdown-another-secure-e-mail-service-goes-offline/, *available at* http://perma.cc/XT4F-7PVN; Russell Brandom, *Cryptoseal Shuts Down Consumer VPN Service Over Legal Concerns*, THE VERGE (Oct. 22, 2013), http://www.theverge.com/2013/10/22/4866362/cryptoseal-shuts-down-consumer-vpn-service-over-lavabit-concerns, *available at* http://perma.cc/H25K-EZA6; Jon Brodkin, *CryptoSeal VPN Shuts Down Rather Than Risk NSA Demands for Crypto Keys*, ARS TECHNICA (Oct. 21, 2013), http://arstechnica.com/information-technology/2013/10/cryptoseal-vpn-shuts-down-rather-than-risk-nsa-demands-for-crypto-keys/, *available at* http://perma.cc/X2TT-9L5K.

6. DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 20:1 (updated Aug. 2014). A grand jury subpoena may be inappropriate for national security investigations because the recipient of the subpoena is not barred from making disclosures, though the grand jurors are. *Id.*

7. *Id.*; *see infra* note 74 and accompanying text.

8. Kris & Wilson, *supra* note 6, § 20:1.

9. *Id.* § 20:2.

10. *Id.*; Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C.A. §§ 1801 to 1871 (West 2010).

11. Kris & Wilson, *supra* note 6, § 20:2.

12. *Id.*

There are five distinct NSL statutes,[13] but most NSLs are issued under 18 U.S.C. § 2709 to communications firms—including Internet service providers (ISPs), telephone companies, universities, libraries, businesses, political organizations, and charities.[14] The NSL's prohibition on revealing to anyone that a request had been made is popularly referred to as a "gag order."[15] Although ostensibly aimed at foreign counterintelligence and terrorism, relaxed standards allow any person's information to be requested so long as field officers certify, without providing any specific facts, that a target's data will be used to "protect against international terrorism or clandestine intelligence activities."[16]

The development of NSLs is rooted in the Right to Financial Privacy Act of 1978.[17] Originally weaker than a standard subpoena, they were strengthened over time and extended in the Electronic Communications Privacy Act of 1986 (ECPA), which created 18 U.S.C. § 2709, the statute underlying the communications record

13. 12 U.S.C.A. § 3414(a)(5)(A) (West 2006) (part of the Right to Financial Privacy Act (RFPA) allowing the FBI to request records from financial institutions); 15 U.S.C.A. § 1681u(a) & (b) (West 2006) and 15 U.S.C.A. § 1681v(a) (West 2006) (provisions of the Fair Credit Reporting Act (FCRA), which allow the government to request records from consumer reporting agencies); 18 U.S.C.A. § 2709(a) (West 2006) (part of the Electronic Communications Privacy Act (ECPA) allowing the FBI to require a "wire or electronic communication service provider" to provide "subscriber information and toll billing information" and "electronic communication transaction records"; 50 U.S.C.A. § 3162 (West) (allowing the government to obtain records to investigate government employees suspected of improperly disclosing classified information).

14. OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NAT'L SEC. LETTERS: ASSESSMENT OF CORRECTIVE ACTIONS AND EXAMINATION OF NSL USAGE IN 2006 (2008), at 107, http://www.justice.gov/oig/special/s0803b/final.pdf; Andrew E. Nieland, Note, *National Security Letters and the Amended Patriot Act*, 92 CORNELL L. REV. 1201, 1214 (2007).

15. Jay M. Zitter, Annotation, *Constitutionality of National Security Letters Issued Pursuant to 18 U.S.C.A. § 2709*, 25 A.L.R. FED. 2d 547 (2008); Nieland, *supra* note 14, at 1204 (describing current NSL statutes, including gag order provisions). NSLs may be used only to obtain subscriber, toll billing information, and other electronic communication transaction records. Kris & Wilson, *supra* note 6, § 20:8. A gag order forbids "public comment about a pending criminal case." 75 Am. Jur. *Trial* § 138 (2014).

16. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 505(a)(2)(B), 115 Stat. 272, 365 (2001) (amending 18 U.S.C. § 2709(b) (1986) which used the far more narrow scope of "authorized foreign counterintelligence investigation[s]"); Patrick P. Garlinger, Note, *Privacy, Free Speech, and the Patriot Act: First and Fourth Amendment Limits on National Security Letters*, 84 N.Y.U. L. REV. 1105, 1111 (2009).

17. Nieland, *supra* note 14, at 1207. "Ironically, the national security letter . . . originated in legislation designed to safeguard individual privacy." *Id.*

NSL.[18] The USA PATRIOT Act, signed into law on October 26, 2001, bolstered the government's ability to use NSLs to demand information by weakening the requirement for individualized suspicion and increasing the number of agents who can certify the need for an NSL.[19] As a result, the use of NSLs has since skyrocketed.[20] A 2006 amendment to the PATRIOT Act altered 18 U.S.C. § 2709, making changes to the gag order and creating a pathway for judicial review.[21] Companies that cooperate with NSLs in good faith are shielded from liability by various statutes.[22]

---

18. *Id.* at 1208-09. ECPA was intended to give significant consideration to individual privacy, forbidding government agencies from obtaining "stored electronic communications information" without the customer's permission, unless it did so "through compulsory process, such as a subpoena, warrant, or court order." *Id.* at 1209 (internal quotation marks omitted) (citing Doe v. Ashcroft, 334 F. Supp. 2d 471, 481 (2004)). However, ECPA also created the exception to the requirement of a subpoena in 18 U.S.C. § 2709(a), which allowed records to be demanded so long as four factors were met. *Id.* at 1209–10. First, requests could only be made to wire or electronic communication services providers. *Id.* Second, obtainable information was limited to subscriber information and toll billing records information. *Id.* Third, the FBI had to certify that the information was relevant to an authorized foreign counterintelligence investigation and there were specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power. *Id.* Fourth, only the Director of the FBI or an individual within the FBI designated for this purpose by the Director could make this certification. *Id.*

19. *Id.* at 1211. As a result of these changes, "an FBI agent could (and still can) issue an NSL upon internal certification that the information sought is 'relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities.'" *Id.* (quoting 18 U.S.C. § 2709(b)).

20. *National Security Letters-NSL Statistics*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/nsl/#stats (last visited Oct. 23, 2013); *See* U.S. DEP'T OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FED. BUREAU OF INVESTIGATION'S USE OF NAT'L SEC. LETTERS 36–38 (2007), *available at* http://www.justice.gov/oig/special/s0703b/final.pdf.

21. USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (Mar. 9, 2006); Zitter, *supra* note 15. The amendments did away with the blanket prohibition on disclosure regarding NSLs under § 2709(c) and replaced it with a mechanism for a case-by-case determination by the FBI of the need for a gag order. *Id*. The 2006 amendments also created a mechanism for judicial review of nondisclosure orders issued under § 2709(c). *See infra* note 201–202 and accompanying text.

22. *See* 12 U.S.C.A. § 3417(c) (West 2006); 18 U.S.C.A. § 2703(e) (West 2006); 15 U.S.C.A. § 1681u(k) (West 2006); 15 U.S.C.A. § 1681v(e) (West 2006); 50 U.S.C.A. § 3162(c)(2) (West); *see also* DAVID P. FIDLER & SARAH JANE HUGHES, RESPONDING TO NATIONAL SECURITY LETTERS: A PRACTICAL GUIDE FOR LEGAL COUNSEL 72–73 (2009). However, companies must take care to ensure they have acted in good faith. *See infra* note 217 and accompanying text.

Critics have condemned NSLs as unnecessary, subject to abuse, and unconstitutional on both First and Fourth Amendment grounds.[23] NSLs requesting information about a person do not implicate that person's Fourth Amendment rights under the so-called "third party doctrine."[24] The third party doctrine, first described in *United States v. Miller*[25] and more fully developed in *Smith v. Maryland*,[26] "provides that if information is possessed or known by third parties, then, for purposes of the Fourth Amendment, an individual lacks a reasonable expectation of privacy in the information."[27] The First

23. Among the critics is the American Civil Liberties Union (ACLU), which stated,

> The ACLU's legal challenge argues that the amended law violates the First and Fourth Amendments because it does not impose adequate safeguards on the FBI's authority to force disclosure of sensitive and constitutionally protected information. The lawsuit also challenges the constitutionality of the statute's gag provision, which prohibits anyone who receives an NSL from disclosing even the mere fact that the FBI has sought information.

Challenge to National Security Letter Authority, AM. CIVIL LIBERTIES UNION (Sept. 29, 2004), https://www.aclu.org/national-security/challenge-national-security-letter-authority, *available at* https://perma.cc/F3GT-MLHY; the Electronic Frontier Foundation, also a critic, and stated,

> In 2013, EFF won a landmark decision in the Northern District of California in which Judge Susan Illston declared one of the statutes unconstitutional in its entirety. EFF's petition, brought on behalf of an unidentified telephone service provider, challenged both the underlying authority to obtain customer records as well as the concurrent gag provision that prevented the recipient from disclosing even that it had receiving an NSL.

National Security Letters, ELEC. FRONTIER FOUND., https://www.eff.org/issues/national-security-letters (last visited Oct. 24, 2013), *available at* https://perma.cc/QM8Q-7MQH; the Electronic Privacy Information Center (EPIC) has stated that, in light of NSL abuses, the NSL statutes "should be repealed." Letter from the Electronic Privacy Information Center (EPIC) to Senators Patrick Leahy and Arlen Specter, Committee of the Judiciary Members, (Mar. 21, 2007) (https://epic.org/privacy/pdf/nsl_letter.pdf, *available at* https://perma.cc/Z5RE-YNGE). Additionally, critics have speculated that the government is using NSLs for bulk collection of Americans' information, rather than targeting specific individuals. Marcy Wheeler, *The FBI (or NSA?)'s Bulk National Security Letters*, EMPTYWHEEL (Jan. 8, 2014), https://www.emptywheel.net/2014/01/08/the-fbi-or-nsas-bulk-national-security-letters/, *available at* https://perma.cc/X49Q-U5UE.

24. Garlinger, *supra* note 16, at 1105; *see also* Daniel J. Solove, *The First Amendment As Criminal Procedure*, 82 N.Y.U. L. REV. 112, 125–27 (2007) (explaining that under the third party doctrine, "the Fourth Amendment does not provide protection when the government seeks information about a person from a third party, whether through a subpoena or through some other means.").

25. 425 U.S. 435 (1976).

26. 442 U.S. 735 (1979).

27. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 528 (2006).

Amendment is therefore the primary pathway for challenging NSLs, although several recent cases have made Fourth Amendment challenges once again colorable.[28]

The Office of the Inspector General (OIG) in the US Department of Justice (DOJ) found widespread misuse of NSLs from 2003 to 2006, including obtaining records and information regarding the wrong individuals, seeking records not permitted by statute (including educational records and associations with campus organizations), issuing letters without following statutorily required protocol, and issuing NSLs after authority to do so expired.[29] Moreover, the FBI used information gleaned from NSLs to investigate targets' "communities of interest"—"the network of people that the target was in contact with."[30] NSLs have also been used to unearth journalists' sources.[31] Perhaps the most egregious example occurred where the FISC specifically rejected an FBI application for a FISA order due to First Amendment concerns and the FBI simply issued NSLs instead, even though statutes proscribe the use of NSLs in certain cases implicating the First Amendment.[32] In 2008 the OIG of the DOJ estimated that there were as many as 6,400 incidents of abuse using NSLs.[33]

In December 2013, the President's Review Group on Intelligence and Communications Technologies, created by President Obama shortly after the Snowden revelations, issued recommendations

28. *See* discussion *infra* Part I.

29. A REVIEW OF THE FED. BUREAU OF INVESTIGATION'S USE OF NAT'L SEC. LETTERS, *supra* note 14, at 83.

30. Eric Lichtblau, *F.B.I. Data Mining Reached Beyond Initial Targets*, N.Y. TIMES (Sept. 9, 2007), http://www.nytimes.com/2007/09/09/washington/09fbi.html?pagewanted=all, *available at* http://perma.cc/Q5G8-LSGG.

31. Trevor Timm, *When Can the FBI Use National Security Letters to Go After Journalists? That's Classified*, FREEDOM OF THE PRESS FOUND. (Sept. 3, 2014), https://freedom.press/blog/2014/09/when-can-fbi-use-national-security-letters-go-after-journalists-thats-classified, *available at* https://perma.cc/6QER-PT3U.

32. OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006 (2008), at 65, http://www.justice.gov/oig/reports/2014/215-II.pdf.

33. Jason Ryan, *FBI Search Abuses Could Number Thousands*, ABC NEWS (Apr. 16, 2008), http://abcnews.go.com/TheLaw/DOJ/story?id=4661216, *available at* http://perma.cc/SW3W-MTCQ.

regarding how to reform surveillance practices.[34] The report recommended that NSL statutes be significantly altered to require specific judicial findings before NSLs can be issued.[35]

Courts reviewing NSLs have disagreed about the constitutionality of several provisions of the NSL-enabling statutes.[36] Despite most recently having been declared unconstitutional, the statutes authorizing NSLs still stand, the FBI continues to issue NSLs, and the President and members of the national security and intelligence communities describe NSLs as vital to preventing terrorist strikes in America.[37]

This Note describes what strategies and countermeasures American entities (including businesses, organizations, and individuals) have used and can use to minimize or avoid their exposure to NSLs. Additionally, this Note describes what American

34. PRESIDENT'S REV. GRP. ON INTELL. & COMMC'NS TECHS, *Liberty and Security in a Changing World* (2013) *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, *also available at* http://perma.cc/9R4D-VTLH.

35. *Id.* Specifically, the Report recommended that "statutes that authorize the issuance of National Security Letters should be amended to permit the issuance of National Security Letters only upon a judicial finding that: (1) the government has reasonable grounds to believe that the particular information sought is relevant to an authorized investigation intended to protect 'against international terrorism or clandestine intelligence activities' and (2) like a subpoena, the order is reasonable in focus, scope, and breadth." *Id.* at 24.

36. *See generally* Zitter, *supra* note 15 (compiling cases both supporting and questioning the legality of NSLs).

37. President Obama stated, "the FBI also relies on what's called national security letters . . ." President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17 2014, 11:15 AM), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence, *also available at* http://perma.cc/T8YZ-AAF7. In 2014, FBI Director James Comey stated "[t]he national security letter is . . . a very important building block tool of our national security investigations." He added, "[w]hat worries me about their suggestion that we impose a judicial procedure on NSLs, is that it would actually make it harder for us to do national security investigations than bank fraud investigations." Josh Gerstein, *FBI chief warns on intel reforms, Snowden*, POLITICO (Jan. 9, 2014), http://www.politico.com/blogs/under-the-radar/2014/01/fbi-chief-warns-on-intel-reforms-snowden-180920.html, *available at* http://perma.cc/UL9T-6ERU. The Acting Assistant Attorney General for National Security in the Department of Justice in a 2011 statement wrote, "I'll address in detail one type of investigative tool . . . that remains critical to our ability to keep the country safe: national security letters." *Hearing on the Permanent Provisions of the Patriot Act Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 12-13 (2011) (statement of Todd Hinnen, acting Assistant Attorney General for National Security, Department of Justice), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-112hhrg65486/pdf/CHRG-112hhrg65486.pdf, *also available at* http://perma.cc/A2UZ-6DHM.

entities can do if they receive an NSL, regardless of the letter's constitutionality.

Part I of this Note briefly examines past court rulings and current litigation regarding NSLs. Part II discusses the disclosure of aggregate statistics of issued NSLs. Part III explores potential countermeasures to NSLs (assuming the letters are constitutional), including a warrant canary, anonymization of user data, use of Tor, avoiding US jurisdiction, using alternative networks and protocols, and challenging the NSL itself. It also discusses cases that bear on these countermeasures and briefly explores the repercussions of not complying. Part IV analyzes the likelihood of success in utilizing each of these countermeasures and concludes that telecommunications companies should collect as little information as possible, and entities should choose to use those telecommunications companies that have committed to protecting user data.

I. HISTORY: NSL LITIGATION AND COURT RULINGS

The leading case on Fourth Amendment searches is *Katz v. United* States.[38] Under the test articulated in *Katz*, the "Fourth Amendment protects privacy, not property, and . . . it protects privacy primarily by answering the normative question of when an expectation of privacy should be deemed constitutionally 'reasonable.'"[39]

In 2012 the Supreme Court in *United States v. Jones* held that the government's attachment of a Global Positioning System (GPS) device to a vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment.[40] However, the majority opinion did not merely conduct a *Katz* analysis. Indeed, the Court stated that the defendant's "Fourth Amendment rights do not rise or fall with the *Katz* formulation" concerning a reasonable expectation of privacy.[41] The Court emphasized the importance of the government's trespass necessary to

38. 389 U.S. 347 (1967).

39. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 816 (2004).

40. United States v. Jones, 132 S. Ct. 945, 949 (2012).

41. *Jones*, 132 S. Ct. at 950.

install the device.[42] The Court decided the case under the theory that a vehicle is an "effect" per the Fourth Amendment, and using a device to monitor the vehicle's movements, constitutes a "search."[43]

Many additional cases have brought the Fourth Amendment into the electronic age. In *Gonzales v. Google, Inc.*, the government sought to compel Google to turn over a massive number of user searches.[44] Google argued that it would be unduly burdened by loss of user trust if forced to produce users' queries.[45] A district court in Northern California agreed with Google and held that "there is a potential burden as to Google's loss of goodwill if Google is forced to disclose search queries to the Government."[46]

In *United States v. Warshak*, the Sixth Circuit held that a criminal defendant enjoys a reasonable expectation of privacy in his email, even when an ISP possesses it.[47] Government agents therefore violated the Fourth Amendment by compelling the ISP to turn over emails without first obtaining a warrant based on probable cause.[48]

Litigation regarding NSLs is largely under seal and often heavily redacted due to the secrecy provisions of the NSL statutes and governmental claims regarding national security.[49] Nonetheless, a

42. *Id.* at 949–53. Justice Sotomayor's concurring opinion, however, justified the outcome using the *Katz* test, explaining that the test can stand side-by-side with the trespass theory. *See id.* at 955 (Sotomayor, J., concurring) (stating that "Katz 's reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.").

43. *Id.* at 949. The Court also stated, "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis." *Id.* at 953 (emphasis in original).

44. 234 F.R.D. 674, 682 (N.D. Cal. 2006).

45. *Id.* at 683–84.

46. *Id.*

47. 631 F.3d 266, 288 (6th Cir. 2010).

48. *Id.* The government's attempt to compel the ISP to turn over the email was based on a portion of the Stored Communications Act (itself a portion of ECPA), 18 U.S.C. §§ 2701 et seq. *Id.* at 282.

49. *See, e.g.*, Tim Cushing, *Government Forces Free Press Advocacy Group To File Its Amicus Brief In NSL Case Under Seal*, TECHDIRT (Apr. 14, 2014), https://www.techdirt.com/articles/20140410/09452626868/government-forces-free-press-advocacy-group-to-file-its-amicus-brief-nsl-case-under-seal.shtml, *available at* https://perma.cc/5BK5-T35M; *see also* ELEC. FRONTIER FOUND., *EFF Fights National Security Letter Demands on Behalf of Telecom, Internet Company* (Mar. 3, 2014), https://www.eff.org/press/releases/eff-fights-national-security-letter-demands-behalf-telecom-internet-company (noting that the challengers to an NSL "remain under seal because the government continues to insist that even identifying the

number of cases have analyzed the constitutionality of NSL-enabling statutes.[50] *Doe v. Ashcroft*,[51] brought by the American Civil Liberties Union (ACLU) and an anonymous ISP, first evaluated the constitutionality of NSLs.[52] The ISP received an NSL but refused to comply. The district court judge awarded summary judgment for the plaintiffs and held the NSL provisions unconstitutional.[53] The court found that the NSL provision violated the Fourth Amendment as applied.[54] Additionally, the disclosure bar was not narrowly tailored to further the government's interest in protecting the integrity and efficacy of international terrorism and counterintelligence investigations, in violation of First Amendment free speech protections.[55] The Court found the disclosure bar was not severable from the NSL provision.[56] Additionally, the Court found that the NSL statutes had "the effect of authorizing coercive searches effectively immune from any judicial process."[57]

The DOJ filed an appeal, but before the court reached a decision, Congress passed the USA PATRIOT Act Reauthorization Act,[58] requiring government certification that the matter pertains to national security, allowing for disclosure to a recipient's lawyer, and creating

companies involved might endanger national security."), *available at* https://perma.cc/9ZJ8-KV2M.

50. *See generally* Zitter, *supra* note 15 (discussing NSL cases).

51. 334 F. Supp. 2d 471 (S.D.N.Y. 2004). Many of the NSL cases follow the naming pattern of *Doe v. [the name of the Attorney General at the time of the lawsuit]*.

52. The ISP was later revealed to be Calyx Internet Access and its president, Nicholas Merrill. Kim Zetter, *'John Doe' Who Fought FBI Spying Freed From Gag Order After 6 Years*, WIRED (Aug. 10, 2010), http://www.wired.com/threatlevel/2010/08/nsl-gag-order-lifted/#ixzz0wcPM40Dg, *available at* http://perma.cc/P3BN-46LS.

53. Doe v. Ashcroft, 334 F. Supp. 2d at 526–27.

54. *Id.* A court may declare a statute unconstitutional on its face, or, more commonly, as applied. Where a court holds a statute unconstitutional on its face, "the state may not enforce it under any circumstances, unless an appropriate court narrows its application; in contrast, when a court holds a statute unconstitutional as applied to particular facts, the state may enforce the statute in different circumstances." Michael C. Dorf, *Facial Challenges to State and Federal Statutes*, 46 STAN. L. REV. 235, 236 (1994). Importantly, "a facial challenge to a statute will fail if the statute has any constitutional application." *Id.* at 239 (citing United States v. Salerno, 481 U.S. 739, 745 (1987)).

55. *Ashcroft*, 334 F. Supp. 2d at 516. At the time the NSL provisions forbade an NSL recipient from consulting with any party, including an attorney, and did not permit any judicial review. Nieland, *supra* note 14, at 1215.

56. *Ashcroft*, 334 F. Supp. 2d at 526–27.

57. *Id.* at 506.

58. Pub. L. No. 109-177, 120 Stat. 192 (Mar. 9, 2006).

a pathway for judicial review.[59] After reaching the Second Circuit, the case was remanded, and the district court again held the surviving portion of the challenge unconstitutional on First Amendment grounds.[60]

In *John Doe, Inc. v. Mukasey*,[61] the Second Circuit affirmed the district court decision in part, holding that because the gag order accompanying an NSL is a restraint on expression imposed prior to judicial review, it must be subject to strict scrutiny.[62] Further, the court held that a statutorily created, mandatory standard of review and level of deference to a government certification of the need for a gag order is unconstitutional.[63] While the court allowed part of the NSL provisions to stand, it enjoined "FBI officials from enforcing the nondisclosure requirement of section 2709(c) in the absence of Government-initiated judicial review."[64]

In 2011, on behalf of an unnamed NSL recipient, the Electronic Frontier Foundation (EFF) brought a new challenge to NSLs in *In Re National Security Letter*.[65] On March 14, 2013, the District Court for

---

59. Kris & Wilson, *supra* note 6, § 20:10.

60. The Court stated,

> § 2709(c) is unconstitutional under the First Amendment because it functions as a licensing scheme that does not afford adequate procedural safeguards, and because it is not a sufficiently narrowly tailored restriction on protected speech. Because the Court finds that § 2709(c) cannot be severed from the remainder of the statute, the Court finds the entirety of § 2709 unconstitutional. Additionally, the Court concludes that § 3511(b) is unconstitutional under the First Amendment and the doctrine of separation of powers.

Doe v. Gonzales, 500 F. Supp. 2d 379, 425 (S.D.N.Y. 2007) aff'd in part, rev'd in part and remanded sub nom. Before this decision the challenging ISP abandoned the Fourth Amendment challenge, and the Second Circuit therefore vacated that portion of the District Court's opinion on appeal. Doe v. Gonzales, 449 F.3d 415, 419 (2d Cir. 2006). The Second Circuit then remanded the ISP's First Amendment claims for further consideration in light of the PATRIOT Act Reauthorization Act. *Id*.

61. 549 F.3d 861, 881 (2d Cir. 2008), as modified (Mar. 26, 2009).

62. *See id*. at 879–80 (citing Freedman v. State of Md., 380 U.S. 51 (1965)).

63. *Id.* at 882. The Court stated that allowing the certification to be conclusive would "reduce strict scrutiny to no scrutiny." *Id.*

64. *Id.* at 885.

65. 930 F. Supp. 2d 1064 (N.D. Cal. 2013). The Wall Street Journal has reported that the unnamed ISP is likely a subsidiary of Working Assets Inc. named CREDO Mobile. Jennifer Valentino-DeVries, *Covert FBI Power to Obtain Phone Data Faces Rare Test*, WALL ST. J. (July 18, 2012), http://online.wsj.com/news/articles/SB10001424052702303567704577519213906388708, *available at* http://perma.cc/CZP6-8QHN.

the Northern District of California granted the petition and declared that the nondisclosure provisions of the NSL statutes are not sufficiently narrowly tailored to serve compelling governmental interests in national security without unduly burdening speech protected by the First Amendment.[66] This court also agreed with the *Mukasey* decision and found that the provisions of NSL statutes which mandate the standard of review and level of deference applied to the government certifications were violative of the First Amendment and separation of powers principles.[67] The court also ruled that the nondisclosure portion of the statute was not severable in that NSLs could not achieve their function without the nondisclosure order, and therefore the entire statute, including the underlying power to obtain customer records, is unenforceable.[68] The government appealed.[69] Since this ruling declaring the NSL statutes illegal, Google has tried and failed at least twice to avoid complying with them.[70]

66. *In Re National Security Letter*, 930 F. Supp. 2d at 1075. Specifically, the court concluded that the nondisclosure provision of 18 U.S.C. § 2709(c) violates the First Amendment and 18 U.S.C. § 3511(b)(2) and (b)(3) violate the First Amendment and separation of powers principles. *Id.* at 1081.

67. The court found that the "NSL nondisclosure provisions are not narrowly tailored on their face, since they apply, without distinction, to both the content of the NSLs and to the very fact of having received one." *Id.* The court also found that, "as written, the statute impermissibly attempts to circumscribe a court's ability to review the necessity of nondisclosure orders." *Id.* at 1077.

68. The court stated, "[t]he statutory provisions at issue—as written, adopted and amended by Congress in the face of a constitutional challenge—are not susceptible to narrowing or conforming constructions to save their constitutionality." *Id.* at 1080. The government would therefore have been enjoined from issuing NSLs under § 2709 or from enforcing the nondisclosure provision in this or any other case, however the court's judgment was stayed pending appeal. *Id.* at 1081.

69. Notice of Appeal In re Nat'l Sec. Letter, (N.D. Cal. 2013) (No. C 11-2173 SI), *available at* https://www.eff.org/files/filenode/noticeofappeal.pdf, *also available at* https://perma.cc/N7YC-D4HP.

70. Although the cases are seemingly under seal, it appears Google has twice refused to cooperate with NSLs following *In Re National Security Letter*. Karen Gullo, *Google Fights U.S. National Security Probe Data Demand*, BLOOMBERG (Apr. 3, 2013), http://www.bloomberg.com/news/2013-04-04/google-fights-u-s-national-security-probe-data-demand.html [hereinafter Gullo, *Google Fights NSL Demand*] (regarding N.D. Cal. suit), *available at* http://perma.cc/QD86-AU2Y; Declan McCullagh, *Judge orders Google to comply with FBI's secret NSL demands*, CNET (May 31, 2013), http://www.cnet.com/news/judge-orders-google-to-comply-with-fbis-secret-nsl-demands/ [hereinafter McCullagh, *Judge orders Google*] (regarding N.D. Cal. suit), *available at* http://perma.cc/Y8NK-W5LC; Declan McCullagh, *Justice Department tries to force Google to hand over user data*, CNET (May 31, 2013), http://

Challenges have also been mounted against other statutes purporting to allow the government to collect electronic communications information without a warrant. *Klayman v. Obama*[71] and *ACLU v. Clapper*[72] concern the warrantless collection of so-called "metadata"[73] pursuant to 50 U.S.C.A. § 1861, otherwise known as Section 215 of the PATRIOT Act.[74] Section 215 permits the government to obtain metadata records related to foreign

www.cnet.com/news/justice-department-tries-to-force-google-to-hand-over-user-data/ [hereinafter McCullagh, *Justice Department*] (regarding S.D.N.Y. suit), *available at* http://perma.cc/NJX6-82UM. According to press accounts, the DOJ has filed "petitions to enforce" to compel Google to cooperate with the NSLs—once before the same judge who decided *In Re National Security Letter* in the Northern District of California, and once in the Southern District of New York. Gullo, *Google Fights NSL Demand*, *supra*. Press accounts indicate that the Northern District of California judge rejected Google's request to modify or throw out nineteen NSLs at issue because Google had raised arguments broadly against NSLs, not related specifically to the nineteen before the Court. McCullagh, *Judge orders Google*, *supra* Additionally the judge did not want to "interfere while the Ninth Circuit Court of Appeals is reviewing the constitutionality of NSLs in an unrelated case that she also oversaw." *Id.* The unrelated case was presumably *In Re National Security Letter* itself. In yet another case brought by a different petitioner before the same judge, the Court stated that because NSLs are "under review at the Ninth Circuit," and because the subsequent petitioner "did not raise arguments *specific* to the two NSLs at issue," their petition to modify or set aside two NSLs was denied. Order Denying Petition to Set Aside and Granting Cross-Petition to Enforce In re Matter of Nat'l Sec. Letters, No. C 13-1165 SI (N.D. Cal. Aug. 12, 2013) No. C 13-1165 SI, *available at* https://www.eff.org/files/2014/01/16/008_-redacted_order_enforcing_nsls_1165.pdf, also *available at* https://perma.cc/4BHG-XAQH. The judge in the Southern District of New York had not made a final ruling as of May 31, 2013. McCullagh, *Justice Department*, *supra.* Although the case is under seal, according to press accounts, the California case is *In Re Google Inc.'s Petition to Set Aside Legal Process* (No. 13-80063) (N.D. Cal 2013); Gullo, *Google Fights NSL Demand*, *supra*.

71. No. 13-0881 (RJL), 2013 WL 6598728 (D.D.C. Dec. 16, 2013).

72. 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

73. Metadata are "information about information." Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2070 (2004). For example, metadata generated in a Microsoft Word document "can include the author's name and initials; the names of previous document authors; the name of the author's company or organization; the name of one's computer; the name of the network server or hard disk where the document was saved; document revisions; hidden text or cells; and personalized editing comments. *Id.*

74. 50 U.S.C. § 1861 (2009). Section 215 of the USA PATRIOT Act, which amended FISA 50 U.S.C.A. § 1861, is one of the most frequently discussed tools for requesting data other than NSLs. Section 215 "allows the government to file an application with the FISC for an order compelling production of business records or other tangible things." Kris & Wilson, *supra* note 6, § 20:8. Some of the so-called "tangible things" in question are in fact records similar to those obtainable through an NSL. *See* Kris & Wilson, *supra* note 6, § 19:1. Another widely discussed tool for acquiring data is Section 702 of the FISA Amendments Act, codified at 50 U.S.C.A. §§ 1881a, which allows the targeting on non-U.S. persons reasonably believed to be outside the US. *Id.* § 17:3.

intelligence through an *ex parte* appearance before the FISC.[75] Bulk collection under Section 215 is premised upon the third party doctrine described in *Smith v. Maryland*.[76]

In a marked shift, the District Court for the District of Columbia in *Klayman v. Obama* found that *Smith v. Maryland* and the third party doctrine were not controlling and therefore did not extinguish the expectation of privacy a person has when using a telephone company or ISP.[77] Accordingly, the court held that Section 215 is likely unconstitutional.[78] The court based its decision on *United States v. Jones*, the vastly altered technological landscape since the Supreme Court handed down *Smith*, and the scale of the mass surveillance presented by the case.[79]

In contrast, *ACLU v. Clapper*, handed down by the District Court for the Southern District of New York just days after *Klayman v. Obama*, raised the same question regarding the constitutionality of mass metadata collection under Section 215 and came to the opposite decision.[80] The court found that *Smith* and the third party doctrine *are* controlling and bar an attack on Section 215 based on the reasonable expectation of privacy.[81] A District Court in the District of Ohio held similarly in *Smith v. Obama*.[82]

---

75. 50 U.S.C. § 1861 (2009).

76. *See* In re F.B.I. for an Order Requiring Prod. of Tangible Things from Redacted, No. BR 13-109, 2013 WL 5741573, at *2 (Foreign Intel. Surv. Ct. Aug. 29, 2013) (holding in a case challenging Section 215 that "[t]he production of telephone service provider metadata is squarely controlled by the Court's decision in Smith v. Maryland, 442 U.S. 735, 99 S. Ct. 2577, 61 L.Ed. 2d 220 (1979)").

77. No. 13-0881 (RJL), 2013 WL 6598728 at *17-22 (D.D.C. Dec. 16, 2013); *see* Laura K. Donohue, *Fisa Reform*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 599, 639 n.45 (2014) (comparing the holding in ACLU v. Clapper which found that *Smith* controls with the holding in *Klayman*, which found *Smith* does not control).

78. *Klayman*, 2013 WL 6598728 at *17-22.

79. The Court stated, "Like the concurring justices in Jones, I cannot 'identify with precision the point at which' bulk metadata collection becomes a search, but there is a substantial likelihood that the line was crossed under the circumstances presented in this case." *Id.* at *20 n.48. It added, "the *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones." *Id.* at *22.

80. 959 F. Supp. 2d 724 (S.D.N.Y. 2013).

81. *See id.* at 751; *see also* Donohue, *supra* note 77.

82. No. 2:13-CV-257-BLW, 2014 WL 2506421 (D. Idaho June 3, 2014).

Crucially, the NSL statutes rely upon the same exception to the Fourth Amendment as bulk collection under Section 215: the third party doctrine established by *Smith*.[83] If the third party doctrine is overturned or ruled inapplicable to Section 215, it should be overturned or ruled inapplicable to the even more relaxed standards of NSLs. Should both opinions be affirmed on appeal (or should they both be reversed), the issue will be ripe for Supreme Court review.[84]

II. DISCLOSURE OF AGGREGATE STATISTICS OF ISSUED NSLS

Customers of businesses that collect user data and records expect that data to be kept private unless permission is granted for the data to be shared, or unless the government has proper legal authority to obtain them. The secrecy of NSLs undermines that trust because customers do not know how frequently a business passes its data or records on to the government. This problem is particularly acute for companies with business models that emphasize the security of housing data in the cloud—storage on dispersed, third party servers rather than the customers' own servers.

Even prior to the disclosures in June of 2013 by NSA contractor Edward Snowden revealing the extent of US governmental surveillance,[85] several American technology companies began to issue "transparency reports" to allow the public to discern how frequently the government requests and gains access to private data through search warrants and court subpoenas.[86] In March of 2013, Google, with the government's permission, began to publish broad ranges of figures describing the number of NSLs it has received

83. *See supra* note 76; *see also* Klayman, 2013 WL 6598728 at *17-22; Smith 2014 WL 2506421 at *1007.

84. One news article following the conflicting opinions stated, "Pauley's ruling contrasted with one issued Dec. 16 by Judge Richard Leon for the District Court for the District of Columbia, thus increasing the possibility that the United States Supreme Court will have to settle the matter." Joel Stashenko, *Federal Judge Backs Collection of Phone Data*, N.Y.L.J. (Dec. 30, 2013), http://www.newyorklawjournal.com/id=1388149352034?slreturn=20140106025319, *available at* http://perma.cc/A89S-46UD.

85. *See supra* note 1.

86. *See* Kashmir Hill, *Thanks, Snowden! Now All The Major Tech Companies Reveal How Often They Give Data To Government*, FORBES (Nov. 14, 2013), http://www.forbes. com/sites/kashmirhill/2013/11/14/silicon-valley-data-handover-infographic/, *available at* http://perma.cc/5MWT-6XX4.

annually.[87] Following Edward Snowden's disclosures, many more companies sought to make clear that their cooperation with the government is compulsory, and that requests for information are not frequent or routine.[88]

AOL, Apple, Facebook, Google, LinkedIn, Microsoft, and Yahoo recently signed an open letter in support of a bill entitled the USA Freedom Act.[89] The letter focuses primarily on the issue of transparency, namely, allowing these companies to disclose more information about what data the government has requested of them.[90] The Act aims to rein in dragnet collection of data,[91] increase transparency of the FISC, provide companies the ability to release information regarding FISA requests, and create an independent constitutional advocate to argue cases before the FISC.[92] The bill would also require unclassified reports on NSLs, including "aggregate number of requests relating to US persons, non-US persons, persons subject to national security investigation, persons

87. In March of 2013, Google began to report NSL statistics, stating,

> Starting today, we're now including data about NSLs in our Transparency Report. We're thankful to U.S. government officials for working with us to provide greater insight into the use of NSLs. Visit our page on user data requests in the U.S. and you'll see, in broad strokes, how many NSLs for user data Google receives, as well as the number of accounts in question.

Transparency Report: Shedding more light on National Security Letters, GOOGLE (Mar. 5, 2013), http://googleblog.blogspot.com/2013/03/transparency-report-shedding-more-light.html, *available at* http://perma.cc/AE7Z-UYUM.

88. Hill, *supra* note 86.

89. USA FREEDOM Act, H.R. 3361, S. 1599, 113th Cong. § 1 (2013); Letter from AOL, Apple, Facebook, Google, LinkedIn, Microsoft, and Yahoo, to Patrick Leahy, Chairman, Committee on the Judiciary, et al. (Oct. 31, 2013), (http://sensenbrenner.house.gov/uploadedfiles/usa_freedom_act_letter.pdf, *available at* http://perma.cc/8KQ7-BTMH).

90. Dieter Bohn, *Apple, Microsoft, Google, and others urge Congress to enact NSA reforms*, THE VERGE (Oct. 31, 2013), http://www.theverge.com/2013/10/31/5053438/apple-microsoft-google-and-others-urge-congress-to-enact-nsa-reforms/in/4483763, *available at* http://perma.cc/9YGC-AR6C.

91. *See, e.g.*, Berger v. State of New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring) (explaining that *dragnet* electronic surveillance "sweep[s] in all conversations within its scope—without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations.").

92. *The USA FREEDOM Act*, JIM SENSENBRENNER'S CONG. WEBSITE http://sensenbrenner.house.gov/legislation/theusafreedomact.htm (last visited Feb. 6, 2014), *available at* http://perma.cc/SYD7-XQQV.

linked to a subject of a national security investigation, and persons not subject to an investigation or linked to a subject of an investigation."[93] Although the bill failed in the Senate on November 18, 2014, in a 58–42 vote, Senator Patrick Leahy has committed to continue working towards its passage.[94]

On June 11, 2013, Google asked the Attorney General and FBI for permission to publish more explicitly the number and scope of secret subpoenas, including NSLs and FISA requests.[95] When the government refused to allow such disclosures, Google filed a motion seeking a declaratory judgment of its right to publish aggregate information about the subpoenas, such as the total number of requests for data received and users of accounts encompassed within such requests.[96] Shortly thereafter Microsoft filed a similar motion.[97] Yahoo, Facebook, and LinkedIn filed motions seeking the same declaratory judgment in September.[98] Moreover, Apple stated that it

93. Alan Butler, *Standing Up to Clapper: How to Increase Transparency and Oversight of Fisa Surveillance*, 48 NEW ENG. L. REV. 55, 95 (2013) (citing USA FREEDOM Act, *supra* note 89).

94. Bill Chappell, *Bill Limiting NSA Surveillance Practices Fails In Senate*, NPR (Nov. 18, 2014), http://www.npr.org/blogs/thetwo-way/2014/11/18/365073310/bill-limiting-nsa-surveillance-practices-fails-in-senate, *available at* http://perma.cc/BB7R-7Y2Z.

95. Google's blog post stated,

> We therefore ask you to help make it possible for Google to publish in our Transparency Report aggregate numbers of national security requests, including FISA disclosures—in terms of both the number we receive and their scope. Google's numbers would clearly show that our compliance with these requests falls far short of the claims being made. Google has nothing to hide.

Asking the U.S. Government to Allow Google to Publish More National Security Request Data, GOOGLE (June 11, 2013), http://googleblog.blogspot.com/2013/06/asking-us-government-to-allow-google-to.html, *available at* http://perma.cc/QS8G-WAT6.

96. In re Mot. for Declaratory Judgment of Google Inc.'s First Amendment Right to Publish Aggregate Information about FISA Orders (FISA Ct. 2013), *available at* http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Motion-10.pdf.

97. In re Mot. for Declaratory Judgment of Microsoft Inc.'s First Amendment Right to Publish Aggregate Information about FISA Orders (FISA Ct. 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/misc-13-04-motion.pdf.

98. In re Mot. to Disclose Aggregate Data Regarding FISA Orders (FISA Ct. 2013), *available at* http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-05%20Motion-12.pdf; In re Mot. for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives (FISA Ct. 2013), *available at* http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-06%20Motion-3.pdf; In re Mot. for Declaratory Judgment that LinkedIn Corporation May Report Aggregate Data Regarding FISA Orders (FISA Ct. 2013), *available at* http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-07%20Motion-3.pdf.

would file an amicus brief with the Ninth Circuit in support of greater transparency regarding NSLs.[99]

On January 17, 2014, President Obama announced reforms to the various surveillance activities revealed by Snowden. Among them, Obama pledged that with regard to NSLs,

> [S]ecrecy will not be indefinite, so that it will terminate within a fixed time unless the government demonstrates a real need for further secrecy. We will also enable communications providers to make public more information than ever before about the orders that they have received to provide data to the government.[100]

On January 27, 2014, the Obama administration announced that it would allow aggregate numbers of secret data requests to be disclosed pursuant to Executive Order 13526, § 3.1(c) to settle the filed motions and create a new framework for reporting on national surveillance requests.[101] According to a letter written by James M. Cole, Deputy Attorney General (DAG Letter), going forward, the settling companies and all others may begin reporting the number of NSLs (and FISA orders) received in bands of 1,000. Further, each company may also report the number of accounts affected collectively by the NSLs (and FISA orders), in ranges of 1,000.[102] Companies may publish the figures once every six months, with a

---

99. Apple stated in its Transparency Report, "later this year, we will file a second Amicus brief at the Ninth Circuit in support of a case seeking greater transparency with respect to National Security Letters." *Report on Government Information Requests*, APPLE (Nov. 5, 2013), https://www.apple.com/pr/pdf/131105reportongovinforequests3.pdf, *available at* https://perma.cc/EC7E-MY8N.

100. Obama, *supra* note 37. The announcement coincided with the President's signing of Presidential Policy Directive—28, *Signals Intelligence Activities* (PPD-28) (Jan. 17, 2015), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities, *available at* http://perma.cc/98PY-AV5G.

101. Gov. Notice, Nos. Misc 13-03, 13-04, 13-05, 13-06, 13-07 (FISA Ct. Jan. 27, 2014), *available at* http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Notice.pdf; Letter from James M. Cole, Deputy Attorney Gen., to Colin Stretch, Vice President and Gen. Counsel, Facebook, et al. (Jan. 27, 2014) (http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf, *available at* http://perma.cc/A7R9-GNG5) [hereinafter *DAG Letter*]; David Kravets, *Tech Giants, Telcos Get OK to Release Stats on NSASpying*, WIRED (Jan. 27, 2014), http://www.wired.com/threatlevel/2014/01/nsa-public-spying-data/, *available at* http://perma.cc/6LRK-4MYA.

102. *See* DAG Letter, *supra* note 101.

six-month delay in reporting periods.[103] There is a two-year delay for any "new capability"–any new type of service a company offers.[104] Alternatively, a company may report the total number of all "national security process" received, including all NSLs and FISA orders (and the total number of "customer selectors"—i.e., accounts), reported as a single number in bands of 0-249 and thereafter in bands of 250.[105]

The exception allowing for perpetual gag orders when "the government demonstrates a real need for further secrecy" is a loophole that may render the announced changes meaningless.[106] Opponents of dragnet government surveillance generally felt that the reforms announced by the President did not go far enough.[107] Twitter, for instance, decried the improvements as not meaningful.[108]

Indeed, in October of 2014, Twitter filed a lawsuit seeking declaratory judgment that it has the right to publish a Transparency Report that does not follow the framework established in the DAG

---

103. *Id.*

104. *Id.*

105. *Id.*

106. *See* Meghan Neal, *Obama's Linguistic Loopholes*, VICE MOTHERBOARD (Jan. 17, 2014, 5:30 PM), http://motherboard.vice.com/blog/obamas-linguistic-loopholes (stating that "instead of introducing concrete actions to curtail government spying, the president offered up a cocktail of ambiguous proposals, explained with carefully chosen vague language riddled with qualifiers and escape clauses that leave a lot of wiggle room for the NSA to continue business as usual."), *available at* http://perma.cc/HZG3-LDZE.

107. *See, e.g.*, Neil M. Richards, *Obama's Surveillance Reforms*, BOSTON REV. (Jan. 22, 2014), https://www.bostonreview.net/blog/richards-nsa-obama-surveillance, *available at* https://perma.cc/3JW7-RL2J; Mike Masnick, *Feds Reach Settlement With Internet Companies Allowing Them To Report Not Nearly Enough Details On Surveillance Efforts*, TECHDIRT (Jan. 27, 2014), https://www.techdirt.com/articles/20140127/17253826014/feds-reach-settlement-with-internet-companies-allowing-them-to-report-not-nearly-enough-details-surveillance-efforts.shtml, *available at* https://perma.cc/HSE9-TRSV; Tony Romm, *Obama administration to allow Facebook, Google, others more NSA transparency*, POLITICO (Jan. 27 2014), http://www.politico.com/story/2014/01/barack-obama-administration-nsa-national-security-agency-tech-technology-transparency-eric-holder-james-clapper-102677.html, *available at* http://perma.cc/73GP-ZJJ2.

108. Twitter explained in a blog post that

> allowing Twitter, or any other similarly situated company, to only disclose national security requests within an overly broad range seriously undermines the objective of transparency. In addition, we also want the freedom to disclose that we do not receive certain types of requests, if, in fact, we have not received any.

Jeremy Kessel, *Fighting for more #transparency*, TWITTER BLOG (Feb. 6, 2014), https://blog.twitter.com/2014/fighting-for-more-transparency, *available at* https://perma.cc/X5SG-ETTQ.

Letter.[109] Twitter alleged that the government prohibits services like Twitter "from providing their own informed perspective as potential recipients of various national security-related requests."[110] Twitter explained that it submitted a draft Transparency Report to the government, but after five months, the government informed Twitter that "information contained in the [transparency] report is classified and cannot be publicly released" because it does not comply with the DAG Letter framework.[111] The complaint stated that the government's "position forces Twitter either to engage in speech that has been preapproved by government officials or else to refrain from speaking altogether."[112]

Specifically, Twitter objects to the requirement that the first interval that can be reported ranges from 0-249, precluding an announcement that Twitter has received zero NSLs.[113] Twitter's argument mirrors many of the arguments made in *In Re National Security Letter* with a few additions.[114] Like the plaintiff in that case, Twitter claims "The nondisclosure and judicial review provisions of 18 U.S.C. § 2709(c) are facially unconstitutional under the First Amendment."[115] It also claims that 18 U.S.C. § 2709(c) is unconstitutional as applied to Twitter.[116] Like the plaintiffs in *In Re National Security Letter*, Twitter claims that altering of the standard of review for NSLs represents a violation of separation of powers principles.[117] Twitter additionally claims that the DAG Letter violates the Administrative Procedure Act for a variety of reasons, including

109. Complaint for Declaratory Judgment 28 U.S.C. §§ 2201 and 2202, Twitter v. Holder, No. 14-CV-4480, 2014 WL 5012514 (N.D. Cal. Oct. 27, 2014); *see also* Ben Lee, *Taking the Fight For #transparency to court*, TWITTER (Oct. 7, 2014), https://blog.twitter.com/2014/taking-the-fight-for-transparency-to-court, *available at* https://perma.cc/2CRY-VRBQ.

110. Complaint, *supra* note 109, ¶ 2.

111. *Id.* ¶ 3.

112. *Id.* ¶ 4. The complaint also emphasizes that Twitter cannot be bound by the terms of the January 27th notice, which settled other companies' claims. *Id.*

113. *Id.* ¶ 5, ¶ 27. Because Twitter is seeking the right to affirmatively state it has received zero NSLs rather than the right to cease making a statement saying as much, the case is slightly different from litigation that might take place regarding a normal warrant canary (discussed below) in that it does not implicate compelled speech. *See infra* note 125 and accompanying text.

114. 930 F. Supp. 2d 1064 (N.D. Cal. 2013). *See supra* note 65 and accompanying text.

115. Complaint, *supra* note 109, ¶ 46.

116. *Id.* ¶ 47.

117. *Id.* ¶ 48.

that it "represents a final agency action not in accordance with law."[118]

In seeking dismissal, the government has responded that the DAG Letter itself does not limit Twitter's ability to publish its Transparency Report.[119] Instead, "any such restrictions stem from other authority, including statutory law such as FISA, applicable orders and directives issued through the [FISC], and from any applicable nondisclosure agreements."[120] The government explained that on "January 27, 2014, the Director of National Intelligence declassified certain aggregate data concerning national security legal process so that recipients of such process could reveal aggregate data," and the DAG Letter merely defines what may be published following this declassification.[121] The outcome of this case may help to clarify not only which statistics companies may disclose in the interests of transparency, but whether warrant canaries, discussed below, are legal.

On February 3, 2015, Director of National Intelligence James Clapper announced changes to government surveillance policies which implement the reforms outlined by President Obama in January, 2014.[122] Among them,

> In response to the President's new direction, the FBI will now presumptively terminate National Security Letter nondisclosure orders at the earlier of three years after the opening of a fully predicated investigation or the investigation's close.

---

118. *Id.* ¶ 44.

119. Defendant's Notice of Motion and Partial Motion to Dismiss, Twitter v. Holder, No. 14-CV-4480 (N.D. Cal. Oct. 27, 2014).

120. *Id.* at 2.

121. *Id.* at 7.

122. *Signals Intelligence Reform, 2015 Anniversary Report*, IC ON THE RECORD, (Feb. 3, 2015), http://icontherecord.tumblr.com/ppd-28/2015/overview, *available at* http://perma.cc/TD6P-74YX. Specifically, the changes are intended to implement PPD-28. *See supra* note 100. *Statement by Assistant to the President for Homeland Security and Counterterrorism Lisa Monaco: Update on Implementation of Signals Intelligence Reform and Issuance of PPD-28*, THE WHITE HOUSE, OFFICE OF THE PRESS SEC'RETARY (Feb. 3, 2015), http://www.whitehouse.gov/the-press-office/2015/02/03/statement-assistant-president-homeland-security-and-counterterrorism-lis, *available at* http://perma.cc/NQ3B-ZEH4.

> Continued nondisclosures orders beyond this period are permitted only if a Special Agent in Charge or a Deputy Assistant Director determines that the statutory standards for nondisclosure continue to be satisfied and that the case agent has justified, in writing, why continued nondisclosure is appropriate.[123]

In other words, although NSLs statutorily may continue to be issued with a perpetual gag order, the FBI will adopt a policy whereby it sometimes voluntarily terminates the gag order after three years.

This change, while an improvement over the previous policy of allowing all gag orders to stand in perpetuity, does not implement the changes recommended by the President's Review Group on Intelligence and Communications Technologies or dragnet surveillance opponents. The new policy "doesn't address concerns that NSL gag orders lack adequate due process protections, lack basic judicial oversight, and may violate the First Amendment."[124]

III. COUNTERMEASURES TO NSLS AND LEGAL PRECEDENT

Some companies have expressed an interest in going beyond disclosing the number of NSLs received by either actively fighting the gag order associated with an NSL, or adjusting policies so that cooperation with an NSL is impossible or useless to the government.

---

123. *Signals Intelligence Reform, 2015 Anniversary Report: Strengthening Privacy & Civil Liberties Protections*, IC ON THE RECORD (Feb. 3, 2015), http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#letters, *available at* http://perma.cc/BE6E-K9WX.

124. Megan Graham, *The Newest Reforms on SIGINT Collection Still Leave Loopholes*, JUST SECURITY (Feb. 3 2015), http://justsecurity.org/19665/newest-reforms-sigint-collection-leave-plenty-loopholes/, *available at* http://perma.cc/EF5C-7M3U; *see also* Cyrus Farivar, *Experts decry "nibbling at the edges" rather than real surveillance reform*, ARS TECHNICA (Feb. 3 2015), http://arstechnica.com/tech-policy/2015/02/experts-decry-nibbling-at-the-edges-rather-than-real-surveillance-reform/ (quoting Mark Rumold, a staff attorney with the EFF, who stated "[i]t's still an unconstitutional gag, and they just changed it from an indefinite unconstitutional gag to a three-year unconstitutional gag."), *available at* http://perma.cc/7MDT-F3FR.

A. The Warrant Canary and Coerced Speech

One proposed countermeasure is the warrant canary, a regularly issued statement by an entity asserting that it has not received an NSL or secret warrant recently.[125] If the entity does receive an NSL, it would simply stop issuing the statement rather than violate the prohibition on disclosing the receipt of the NSL.[126] Users of the service offered by the entity would be instructed to watch for continued issuance of the statement.[127] When a user of the service notices the absence of the statement, that user would assume that the entity has in fact received an NSL.[128] Because it is the failure to take action rather than actual action that triggers the alert, this countermeasure acts as a dead-man's-switch.[129] If the FBI wanted to avoid alerting the service's users to the fact that an NSL has been

125. For additional, recent analyses of warrant canaries, *see* Rebecca Wexler, Note, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, 124 YALE L.J. FORUM 158 (2014) and Naomi Gilens, The NSA Has Not Been Here: Warrant Canaries as Tools for Transparency in the Wake of the Snowden Disclosures (Apr. 2014) (unpublished Note, Harvard Law School) *available at* http://ssrn.com/abstract=2498150, *also available at* http://perma.cc/P45G-5Y3J.

126. The "warrant canary" may have been first proposed by Steven Schear on the cypherpunks mailing list in 2002 at https://groups.yahoo.com/neo/groups/cypherpunks-lne-archive/conversations/topics/5869, *available at* https://perma.cc/9U5Y-ERFS. The below image (and several more available at http://www.librarian.net/technicality.html, *also available at* http://perma.cc/SA5H-6FTP) represents a physical incarnation of a warrant canary created by Jessamyn West in 2002 to be used in libraries:

127. *See* Kurt Opsahl, *Warrant Canary Frequently Asked Questions*, ELEC. FRONTIER FOUND. (Apr. 10, 2014), https://www.eff.org/deeplinks/2014/04/warrant-canary-faq, *available at* http://perma.cc/MM8R-6TVT.

128. *See id.*

129. Cory Doctorow, *How to foil NSA sabotage: use a dead man's switch*, THE GUARDIAN, (Sept. 9, 2013), http://www.theguardian.com/technology/2013/sep/09/nsa-sabotage-dead-mans-switch, *available at* http://perma.cc/39UY-ZR8A.

issued, it would have to coerce the entity to continue issuing the statement against its will.[130] However, alerting a user targeted by an NSL that one has been received is not the primary purpose of a warrant canary.[131] Instead, a warrant canary helps expose how often the government uses NSLs—exceptional legal tools—so the public can have an informed debate about whether they are being abused (or should continue to exist). Without these disclosures there can be no public debate.[132]

Online storage and backup host rsync.net (rsync) has publicly issued a warrant canary since roughly 2005.[133] Rsync's warrant canary currently reads, "[n]o warrants have ever been served to rsync.net, or rsync.net principals or employees. No searches or seizures of any kind have ever been performed on rsync.net assets."[134] If rsync receives a (traditional) warrant, the text would be updated to describe the warrant.[135] If, however, it receives an NSL or other secret request, the warrant canary would cease to be updated or issued entirely.[136] Similarly, Lookout, a mobile security company, began publishing a warrant canary in its September 2013

130. *See* Gilens, *supra* note 125, at 7 (stating "[u]ltimately, no matter how informative the canary is in theory, it is of no practical use if the government can compel a company to publish its canary untruthfully after serving the company with a surveillance request that should kill it.").

131. *See About Canary Watch*, CANARYWATCH.ORG, https://canarywatch.org/about.html, *available at* https://perma.cc/EXL8-A7QE (explaining the intent of a warrant canary "is not to harm the judicial process, but rather to engage in a public conversation about the extent of government investigatory powers.").

132. *See id.* at 4 (stating, "[t]here are three primary purposes for which a company may adopt a canary. What I term 'performative canaries' are exercises in public relations meant to show that a company cares about user privacy; 'granular canaries' provide useful notification to individual users when the security of their personal data is compromised; and 'public policy canaries' speak to how the government is interpreting and using its surveillance powers broadly."). Most companies are unlikely to implement a warrant canary with the sole purpose of alerting a single target to the receipt of an NSL. *See id.* at 6 (explaining "no company has yet taken the concept so far—nor is any company likely to—as doing so would jeopardize legitimate investigations into individuals who pose actual threats.").

133. "We have been publishing our Warrant Canary weekly at rsync.net for almost five years now." John Kozubik, *The Warrant Canary in 2010 and Beyond*, JOHN KOZUBIK'S BLOG (Aug. 06, 2010), http://blog.kozubik.com/john_kozubik/2010/08/the-warrant-canary-in-2010-and-beyond.html, *available at* http://perma.cc/83UK-T4TV.

134. *rsync.net Warrant Canary*, RSYNC.NET (Feb. 22, 2015), www.rsync.net/resources/notices/canary.txt, *available at* http://perma.cc/4XML-FXXV.

135. Kozubik, *supra* note 133.

136. *Id.*

transparency report, stating "as of the date of this report, Lookout has not received a national security order and we have not been required by a FISA court to keep any secrets that are not in this transparency report."[137] In January of 2015, reddit posted a transparency report covering all of 2014.[138] It contained a warrant canary stating "[a]s of January 29, 2015, reddit has never received a National Security Letter, an order under the Foreign Intelligence Surveillance Act, or any other classified request for user information. If we ever receive such a request, we would seek to let the public know it existed."[139]

At the end of January a coalition of organizations including the EFF, the Berkman Center for Internet and Society at Harvard University, New York University's Technology Law & Policy Clinic, and the Calyx Institute created canarywatch.org, which "tracks and documents" warrant canaries and "tracks changes or disappearances of canaries."[140] The website encourages individuals to submit known warrant canaries, and it will thereby become a one-stop-shop for the monitoring of warrant canaries.[141] Additionally, it educates individuals and those interested in implementing a warrant canary regarding their purpose as well as their basic legal underpinnings.[142]

Apple was the most prominent example of a company using a warrant canary.[143] In Apple's November 5, 2013 transparency report,

137. 2013 Transparency Report, LOOKOUT, https://www.lookout.com/transparency/report-2013 (last visited Feb. 22, 2015), *available at* https://perma.cc/RC5Q-UMUT.

138. *reddit transparency report*, 2014, REDDIT (Jan. 29, 2015), https://www.reddit.com/wiki/transparency/2014, *available at* https://perma.cc/FY6Q-XSVJ.

139. *Id.* Reddit's transparency report also stated "reddit supports reform of government surveillance programs and joined 86 other groups by signing an open letter to Congress in 2013." *Id.*

140. *See* About Canary Watch, *supra* note 131.

141. *Id.* At the time of publication, canarywatch.org listed twenty-one organizations publishing a warrant canary. *Canary Watch*, CANARYWATCH.ORG, https://canarywatch.org, *available at* https://perma.cc/CGX8-LAT9.

142. *Frequently Asked Questions*, CANARYWATCH.ORG, https://canarywatch.org/faq.html, *available at* https://perma.cc/X6BN-77LB.

143. By publishing its warrant canary, Apple became

> one of the first big-name tech companies to use a novel legal tactic to indicate whether the government has requested user information in conjunction with a gag order. Known as a 'warrant canary, this language is encapsulated on Apple's fifth page of its new transparency report, which was published on Tuesday.

Cyrus Farivar, *Apple Takes Strong Privacy Stance in New Report, Publishes Rare "Warrant Canary"*, ARS TECHNICA (Nov. 2013), http://arstechnica.com/tech-policy/2013/11/apple-takes-

the company stated for the first time, "Apple has never received an order under Section 215 of the USA Patriot Act. We would expect to challenge such an order if served on us."[144] Although Apple's statement pertained to Section 215 of the USA PATRIOT Act, a different but equally contentious section of the law regarding secret data requests, the principle remains the same, and the language could easily be adjusted to refer to NSLs. Further, some have speculated that by *excluding* language related to NSLs or other provisions of FISA from this statement, Apple was indicating that it *had* in fact received such requests.[145]

Apple and rsync differed in that rsync publishes its warrant canary weekly while Apple's, like most companies', was published only in its transparency reports.[146] Such reports were issued only every six months and contained data that lagged by several months. For example, Apple's November, 2013 transparency report contained data from between January 1 to June 30 of 2013.[147] As discussed below, Apple ceased publication of its warrant canary at the end of 2014.[148]

Although the warrant canary has never been tested in court, several prior cases provide helpful guidance in determining its legality. In order to defeat a warrant canary, the government must force the NSL recipient to continue to publish a lie—that the

---

strong-privacy-stance-in-new-report-publishes-rare-warrant-canary/, *available at* http://perma.cc/8HUS-6YET.

144. *Report on Government Information Requests*, *supra* note 99.

145. One article speculated,

> Apple might have also managed to inform customers that it's been served with a subpoena for customer data, with attendant gag order, under Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act, all without breaking the law, moving its lips or saying a word about FISA. The fact that it didn't mention FISA could mean that it has been served, given that it did mention the subpoenas it hasn't received.

Lisa Vaas, *Apple Publishes New Transparency Report. Is There A 'Warrant Canary' Nesting Inside?*, NAKED SEC. (Nov. 7, 2013), http://nakedsecurity.sophos.com/2013/11/07/apple-publishes-new-transparency-report-is-there-a-warrant-canary-nesting-inside/, *available at* http://perma.cc/G8MT-EANQ.

146. April Glaser, *Apple Issues First Transparency Report, Includes "Warrant Canary"*, ELEC. FRONTIER FOUND. (Nov. 7, 2013), https://www.eff.org/deeplinks/2013/ 11/apples-first-transparency-report-gets-warrant-canaries-right, *available at* https://perma.cc/5KGF-UP54.

147. *Report on Government Information Requests*, *supra* note 99.

148. *See infra* note 165 and accompanying text.

recipient has never received an NSL. Cases where the government has forced someone to speak—coerced speech—are therefore relevant.

In *West Virginia State Board of Education v. Barnette*,[149] the Supreme Court stated that "to sustain [a statute requiring students to salute a flag] we are required to say that a Bill of Rights which guards the individual's right to speak his own mind, left it open to public authorities to compel him to utter what is not in his mind."[150]

In *Wooley v. Maynard*,[151] the next major case concerning compelled speech, the Supreme Court stated that "the right of freedom of thought protected by the First Amendment against state action includes both the right to speak freely and the right to refrain from speaking at all."[152] The Court, however, left open the possibility that a message could be coerced if the state's countervailing interest were sufficiently compelling.[153]

In *Riley v. National Federation of the Blind of North Carolina, Inc.*,[154] the Court stated that the difference between compelled speech and compelled silence "is without constitutional significance, for the First Amendment guarantees 'freedom of speech,' a term necessarily comprising the decision of both what to say and what not to say."[155]

Applied to NSLs, as the Court in *Mukasey* recognized, the restriction on speech must be narrowly tailored to promote a compelling government interest, and there must be no "less restrictive alternatives that would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve."[156] Because "it is obvious and unarguable that no governmental interest is more compelling than the security of the Nation, the principal strict

149. 319 U.S. 624 (1943).

150. *Id*. at 634.

151. 430 U.S. 705 (1977); Larry Alexander, *Compelled Speech*, 23 CONST. COMMENT. 147, 151 (2006). Unlike Barnette, which required an affirmative duty to act on behalf of the students (saluting the flag), Wooley concerned a negative duty not to obscure any part of a license plate. *Alexander*, supra. However, the Court found that the negative duty not to obscure the license plate was itself entangled in the affirmative duty to display a license plate. *Id*.

152. *Maynard*, 430 U.S. at 714.

153. *See id*. at 717.

154. 487 U.S. 781 (1988).

155. *Id.* at 782 (1988).

156. John Doe, Inc. v. Mukasey, 549 F.3d at 878.

scrutiny issue turns on whether the narrow tailoring requirement is met."[157]

Therefore, given the relevant case history, the only substantive difference between an analysis of the constitutionality of the gag order and the constitutionality of a warrant canary hinges on whether a prohibition on the use of a warrant canary is narrowly tailored to promote the government's national security interest.

The court in *Doe v. Gonzales* specified how an analysis of narrow tailoring in the context of NSLs should proceed.[158] Based on *Freedman v. Maryland*,[159] three safeguards must be in place:

> (1) any restraint in advance of judicial review may be imposed only for "a specified brief period," (2) any further restraint prior to "a final judicial determination on the merits" must be limited to "the shortest fixed period compatible with sound judicial resolution," and (3) the burden of going to court to suppress the speech and the burden of proof once in court must rest on the censoring government.[160]

In *Gonzales*, the court found the first two elements were satisfied by the NSL statutes, but the third was not.[161] To satisfy this third prong, the court stated that the "government must either affirmatively terminate the nondisclosure requirement or bear the burden of justifying to a court why continued secrecy is necessary within a reasonable period of time after the FBI issues an NSL containing a nondisclosure order."[162] *Mukasey* affirmed this portion of the opinion,[163] and a warrant canary would therefore presumably be subject to a similar analysis.

However the DAG Letter dramatically altered the landscape for warrant canaries, and the government has implicitly argued that they are illegal. The DAG Letter stated "[i]t is the Government's position that the terms outlined in the Deputy Attorney General's letter define

157. *Id.* (quoting Haig v. Agee, 453 U.S. 280, 307 (1981)).
158. Doe v. Gonzales, 500 F. Supp. 2d at 400.
159. 380 U.S. 51 (1965).
160. *Gonzales*, 500 F. Supp. 2d at 400.
161. *Id.* at 406.
162. *Id.* at 395.
163. *Mukasey*, 549 F.3d at 881.

the limits of permissible reporting for the parties and other similarly situated companies."[164] That is, it is the government's position that the DAG Letter defines the reporting methods which all companies similar to those that settled must follow. Since the DAG Letter prohibits the reporting of zero received NSLs, by implication, it prohibits warrant canaries, which usually state a given company has never received an NSL.

This may explain why Apple "killed" its warrant canary in September of 2014.[165] Although some claimed Apple was trying to alert readers of its Transparency Report that it had received some sort of national security request for data (fulfilling the purpose of a warrant canary), it is more likely the company saw the warrant canary as incompatible with the DAG Letter. Indeed, the company simultaneously explained that it would be reporting the number of national security requests using the DAG Letter framework.[166] Switching to the framework necessitated "disarming" the warrant canary.

Apple claims it was "pleased" to utilize the new framework.[167] While some companies may see the DAG Letter framework as an improvement, others, including Twitter, clearly disagree, as discussed above.[168] However, even under the DAG Letter framework, the loophole allowing a prohibition on disclosure within a two-year delay for any "new capability" gives the warrant canary continued relevancy and makes it particularly important for new and young businesses.[169] Additionally, companies which are not "similarly situated" to those that reached a settlement through the DAG Letter may continue to see value in a warrant canary.

---

164. *See* DAG Letter, *supra* note 109.

165. Cyrus Farivar, *No, Apple probably didn't get new secret gov't orders to hand over data*, ARS TECHNICA (Sept. 18, 2014), http://arstechnica.com/tech-policy/2014/09/no-apple-probably-didnt-get-new-secret-govt-orders-to-hand-over-data/, *available at* http://perma.cc/Y6Q9-MBYK.

166. *Update on National Security and Law Enforcement Orders*, APPLE (Jan. 27, 2014) https://www.documentcloud.org/documents/1302789-upd-nat-sec-and-law-enf-orders-20140127.html, *available at* https://perma.cc/Y3YP-SVC2.

167. *Id.*

168. *See infra* notes 109–18 and accompanying text.

169. *See* Wexler, *supra* note 125, at 166 (stating "[i]n a constitutionally suspect speaker-based distinction, younger companies and those who provide new-capability services lack permission to disclose at all.).

B. Total Anonymization and Tor

Another proposed tactic for avoiding exposure to NSLs is for companies to forego all collection of user data. Under this proposal, the company would have no user data to disclose if the FBI, NSA, or any other government agency requested data. Several companies have adopted this model and use it as their primary selling point.

DuckDuckGo, an Internet search engine, promises users they can "search anonymously," and that unlike Google and its ilk, it makes no attempt to match searches to individuals.[170] French search engine Qwant makes similar claims.[171] Additionally, several virtual private networks (VPNs), services through which a user can mask his or her Internet connection through a remote computer, promise to be fully anonymous.[172]

ISPs such as Charter, Comcast, AT&T, and Verizon, are perhaps the most important gatekeepers in challenging NSLs and maintaining privacy generally. As the company providing the connection between the subscriber and the Internet, an ISP is positioned to observe, inspect, store, and share with the government every byte of data that flows between the user and the Internet.[173] NSLs and other requests

---

170. *DuckDuckGo Privacy*, DUCKDUCKGO, https://duckduckgo.com/privacy#s3 (last visited Feb. 22, 2015) (stating "When you access DuckDuckGo (or any Web site), your Web browser automatically sends information about your computer, e.g., your User agent and IP address. Because this information could be used to link you to your searches, we do not log (store) it at all. This is a very unusual practice, but we feel it is an important step to protect your privacy."), *available at* https://perma.cc/D62G-7QZQ; s*ee also* Charles Arthur, *NSA scandal delivers record numbers of internet users to DuckDuckGo*, THE GUARDIAN (July 10, 2013), http://www.theguardian.com/world/2013/jul/10/nsa-duckduckgo-gabriel-weinberg-prism, *available at* http://perma.cc/Q82V-6C98. DuckDuckGo does not use cookies, does not store users' IP addresses, does not have any log-in system, and uses an encrypted connection for user searches by default. *Id.*

171. *Privacy Statement*, QWANT, https://www.qwant.com/privacy (last visited Feb. 22, 2015) (stating "Qwant's philosophy is based on 2 pillars: No tracking cookies, No filter bubble. We make everything possible to respect your privacy while guaranteeing security and relevant results."), *available at* https://perma.cc/F66C-6374.

172. *Which VPN Service Providers Really Take Anonymity Seriously?*, TORRENTFREAK (Oct. 7, 2011), http://torrentfreak.com/which-vpn-providers-really-take-anonymity-seriously-111007/ (listing examples including Anonine, IVPN, and Proxy.sh), *available at* http://perma.cc/4Y4A-ZCG7.

173. *See* Paul Ohm, *The Rise and Fall of Invasive Isp Surveillance*, 2009 U. ILL. L. REV. 1417, 1420 (2009) (noting that "[e]verything we say, hear, read, or do on the Internet first

issued to ISPs therefore have the potential to unearth a tremendous amount of data.[174]

NSLs are directed to an ISP wile targeting one of that ISP's users. Therefore the only two parties with standing to challenge an NSL are the ISP and the individual target. However, the gag order prevents the ISP from communicating to the targeted user that he or she has been targeted, making the ISP almost always the *only* entity capable of challenging an NSL.[175] Further, because ISPs are predominantly large corporations, regulated by the government and with major business and political ties to it, most are unwilling to fight NSLs on behalf of their users and do not adopt practices, such as limited data retention, which would protect users' privacy.[176]

Some ISPs, such as Sonic.net, XMission, and CREDO Mobile, have committed to informing users, when possible, that they have been targeted by an NSL, fought NSLs in court, and adopted data retention policies that make any compelled response to the government far less useful.[177] Aside from the obvious benefit of

passes through ISP computers. If ISPs wanted, they could store it all, compiling a perfect transcript of our online lives.").

174. *See* Mike Masnick, *ISP CEO Explains What Happens When The NSA Shows Up At Your Door*, TECHDIRT (July 22, 2013), http://www.techdirt.com/articles/20130722/00303923879/isp-ceo-explains-what-happens-when-nsa-shows-up-your-door.shtml, *available at* http://perma.cc/4F4J-DSWH.

175. Theories of "hypothetical future harm that is not certainly impending" are too speculative, thus eliminating lawsuits by plaintiffs who suspect but cannot conclusively prove they are the subject of surveillance. *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1143 (2013).

176. *See* Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 437 (2008). Specifically, "when government seeks intellectual information, businesses often have the choice whether or not to do so, but will likely do so based upon an internal profit-making calculus rather than one which takes into account the interests of their customers in preserving their cognitive autonomy." *Id.*; *see also*, Kris & Wilson, *supra* note 6, at § 20:10 (stating "NSL recipients nearly always will be third-party commercial entities, and not the subject of the investigation in which the NSL was issued. The recipient therefore will have little incentive to assert that the NSL seeks irrelevant information.").

177. Sonic.net has stated that as of 2011, it retains "most IP allocation logs for just two weeks." Dane Jasper, *Help us, protect your privacy online*, SONIC.NET CEO BLOG (Aug. 1, 2011, 10:32 AM), http://corp.sonic.net/ceo/2011/08/01/help-us-protect-your-privacy-online/, *available at* http://perma.cc/Y4WX-K736. Additionally, "it is Sonic.net's policy to notify customers upon receipt of a civil subpoena demand of their account information." *Legal Process Policy*, SONIC.NET, https://wiki.sonic.net/wiki/Legal_Proccess_Policy (last visited Feb. 22, 2014), *available at* https://perma.cc/VGU5-3JHR. CREDO states "Unless specifically prohibited by court order or statute, CREDO will notify you in writing of the request prior to

having an ISP fight NSLs in court, limited data retention policies, such as minimizing the amount of time that the IP address assigned to each user can be matched to the user's name, are one of the strongest countermeasures to the NSL. An ISP simply cannot fulfill an NSL request if the ISP does not possess the information requested, allowing the user to remain anonymous.[178]

Tor (formerly an acronym for The Onion Router) is software which uses a series of relays to conceal a user's location and thereby makes his or her Internet traffic anonymous to both ISPs and the government.[179] Because Tor effectively encrypts and anonymizes users' data, US government agencies consider the traffic running through the service suspicious and retain it longer than data otherwise traversing the Internet.[180] Tor has been specifically targeted by the

releasing such information." *Privacy and Security Policy*, CREDO, MOBILE, http://www.credomobile.com/privacy (last visited Feb. 22, 2015), *available at* http://perma.cc/6D7K-P9Q9. XMission has committed to fighting NSLs as well. Cyrus Farivar, *The only Utah ISP (and one of the few nationwide) standing up for user privacy*, ARS TECHNICA (July 15, 2013), http://arstechnica.com/tech-policy/2013/07/the-only-utah-isp-and-one-of-the-few-nationwide-standing-up-for-user-privacy/, *available at* http://perma.cc/UT4J-9C8B. Google has twice challenged NSLs in court following *In Re National Security Letter*. *See supra* note 69 and accompanying text.

178. *See supra* notes 172–74 and accompanying text.

179. *See Tor: Overview*, THE TOR PROJECT, https://www.torproject.org/about/overview.html.en (last visited Feb. 22, 2015), *available at* https://perma.cc/58NN-43GC. Tor was originally sponsored by the US Naval Research Laboratory and continues to receive support from the US State Department, the Broadcasting Board of Governors, and the National Science Foundation, among others. 60 percent of the Tor Project's 2 million dollar annual budget came from the United States government as of 2012. *Annual Report 2012*, TOR (2012) https://www.torproject.org/about/findoc/2012-TorProject-Annual-Report.pdf. The US government supports Tor in part to aid dissidents in countries such as Iran and China that place restrictions on, censor, or surveil their citizens' access to the Internet. *See* Indira A.R. Lakshmanan, *Supporting Dissent With Technology*, N.Y. TIMES (Feb. 23, 2010), http://www.nytimes.com/2010/02/24/us/24iht-letter.html, *available at* http://perma.cc/3KBE-GR9G.

180. Documents leaked by Edward Snowden and published by THE GUARDIAN indicate the NSA will retain any encrypted data and "hold it for as long as it takes to crack the data's privacy protections." Andy Greenberg, *Leaked NSA Doc Says It Can Collect And Keep Your Encrypted Data As Long As It Takes To Crack It*, FORBES (June 20, 2013), http://www.forbes.com/sites/andygreenberg/2013/06/20/leaked-nsa-doc-says-it-can-collect-and-keep-your-encrypted-data-as-long-as-it-takes-to-crack-it/, *available at* http://perma.cc/J3E6-4WR4; *Procedures used by NSA to minimize data collection from US persons: Exhibit B – full document*, THE GUARDIAN (June 20, 2013), http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document, *available at* http://perma.cc/9JFP-S3GW. The document was subsequently declassified. *See DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, IC ON THE RECORD (Aug. 21, 2013), http://icontherecord.tumblr.com/post/58944252298/dni-declassifies-intelligence-

NSA and foreign intelligence services, though apparently with only partial success.[181] Although government agencies have attacked and partially compromised Tor in investigations into child pornography rings and online black markets, Tor is still considered an effective tool in remaining anonymous.[182]

C. Avoiding the United States' Jurisdiction

Under the theory that statutes requiring cooperation with government surveillance can only be enforced within US jurisdiction, major companies have begun to consider moving to locations that the American government cannot reach. Microsoft has announced that it will begin offering customers in foreign countries the option of having their data stored outside US borders in light of recent surveillance revelations.[183] Microsoft's general counsel stated, "people should have the ability to know whether their data are being subjected to the laws and access of governments in some other country and should have the ability to make an informed choice of where their data resides."[184] Further, Microsoft will "assert available jurisdictional objections to legal demands when governments seek . . . customer content that is stored in another country."[185]

---

community-documents, *available at* http://perma.cc/Z3Y4-LR7G. The declassified version is now available as well. Minimization Procedures Used by The Nat'l Sec. Agency in Connection with Acquisitions of Foreign Intelligence Info. Pursuant to Section 702, as Amended, Eric Holder, Attorney General of the United States (Oct. 31, 2011) (http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf).

181. James Ball, Bruce Schneier & Glenn Greenwald, *NSA and GCHQ target Tor network that protects anonymity of web users*, THE GUARDIAN (Oct. 4, 2013), http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption, *available at* http://perma.cc/Q4LA-YGU8.

182. Cyrus Farivar, *FBI halted one child porn inquiry because Tor got in the way*, ARS TECHNICA (June 12, 2013), http://arstechnica.com/tech-policy/2012/06/fbi-halted-one-child-porn-inquiry-because-tor-got-in-the-way/, *available at* http://perma.cc/8L2A-XVHN.

183. Bill Rigby, *Microsoft lawyer suggests non-U.S. data storage for overseas users: FT*, REUTERS (Jan. 22, 2014), http://www.reuters.com/article/2014/01/23/us-usa-security-microsoft-idUSBREA0M04U20140123, *available at* http://perma.cc/D33N-AEQA.

184. *Id.*

185. Brad Smith, *Protecting customer data from government snooping*, MICROSOFT IMPACT ON SOCIETY BLOG (Dec. 5, 2013), http://www.microsoft.com/eu/impact-on-society/article/protecting-customer-data-from-government-snooping.aspx, *available at* http://perma.cc/CE9H-C9C7.

Indeed, Microsoft has been waging a battle to protect emails stored on servers physically located in Ireland from an American search warrant.[186] In July of 2014, a federal judge in the Southern District of New York ruled that Microsoft must turn the emails over. Microsoft filed a notice of appeal in September 2014.[187]

Google has considered moving its servers outside the United States to avoid national security requests for information.[188] Although it considered the option attractive, Google ultimately decided against the move because it would create new technical hurdles and would promote the "[b]alkanization of the Internet and the creation of a 'splinternet' broken up into smaller national and regional pieces."[189] The "splinternet" Google warns of is a system of "parallel Internets that would be run as distinct, private, and autonomous universes."[190] If balkanization were to occur, the very thing that makes the Internet so powerful—universal connectivity with all others on the Internet—would be destroyed.

Smaller companies and startups without the legacy costs associated with existing infrastructure might not be deterred from moving servers outside of the United States. Startups seeking funding have even begun to pitch their location outside of the United States (often in Europe) as a selling point.[191] Unseen, a private communications company, moved its servers and bank account from the United States to Iceland because it believes Iceland has superior

186. In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained By Microsoft Corporation, Nos. 13-MAG-2814 (S.D.N.Y. filed Dec. 4, 2013).

187. Notice of Appeal, In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained By Microsoft Corporation, Nos. 13-MAG-2814 (S.D.N.Y. filed Dec. 4, 2013).

188. Cadie Thompson, *Google mulled ditching US after NSA scandal*, CNBC (Nov. 22, 2013), http://www.cnbc.com/id/101222237, *available at* http://perma.cc/H8BY-Q6YJ.

189. *Id.*; Claire Cain Miller, *Google Pushes Back Against Data Localization*, N.Y. TIMES (Jan. 24, 2014), http://bits.blogs.nytimes.com/2014/01/24/google-pushes-back-against-data-localization/, *available at* http://perma.cc/P5VR-SR9J.

190. Aparna Kumar, *Libertarian, or Just Bizarro?*, WIRED (Apr. 24, 2001), http://archive.wired.com/politics/law/news/2001/04/43216, *available at* http://perma.cc/HY2Q-GJCC.

191. Steven Levy, *How the NSA Almost Killed the Internet*, WIRED (Jan. 7, 2014), http://www.wired.com/threatlevel/2014/01/how-the-us-almost-killed-the-internet/all/#x, *available at* http://perma.cc/P7HE-EVZN.

data privacy laws.[192] An Australian email provider named FastMail emphasizes that it is located in Australia and claims that "even if a U.S. court were to serve us with a court order, subpoena or other instruction to hand over user data, Australian communications and privacy law explicitly forbids us from doing so."[193] Others have speculated that Germany or Switzerland could provide a haven for companies wishing to keep their data private.[194]

D. Alternative Networks and Protocols

Perhaps the most drastic method to avoid exposure to NSLs and other surveillance would be to cease use of the Internet and to start over with a new network and new protocols built around privacy and encryption.[195] Mesh networks, for instance, are computer networks where nodes—individual computers—communicate directly with each other through wireless connections.[196] This avoids the hub-and-spoke structure whereby connections between computers are facilitated by centralized computers, such as those run by ISPs.[197] Mesh networks do not need designated routers; instead, nodes serve as routers for each other, and this helps eliminate single points at

192. *We've Moved to Iceland and Have a New Domain—Unseen.is*, UNSEEN.IS BLOG (Oct. 6, 2013), http://blog.unseen.is/2013/10/06/weve-moved-to-iceland-and-have-a-new-domain-unseen-is/#awesm=f97470d496e41431728a6d58b34ca183, *available at* http://perma.cc/Z4Z7-BD82.

193. Rob N., *FastMail's servers are in the US: what this means for you*, FASTMAIL WEBLOG (Oct. 7, 2013), http://blog.fastmail.fm/2013/10/07/fastmails-servers-are-in-the-us-what-this-means-for-you/, *available at* http://perma.cc/YG4E-NAYD.

194. Cyrus Farivar, *Europe won't save you: Why e-mail is probably safer in the US*, ARS TECHNICA (Oct. 13, 2013), http://arstechnica.com/tech-policy/2013/10/europe-wont-save-you-why-e-mail-is-probably-safer-in-the-us/2/, *available at* http://perma.cc/57BW-4TRS; Cyrus Farivar, *Switzerland won't save you, either: Why e-mail might still be safer in US*, ARS TECHNICA (Dec. 22, 2013), http://arstechnica.com/tech-policy/2013/12/switzerland-wont-save-you-either-why-e-mail-might-still-be-safer-in-us/, *available at* http://perma.cc/LNW6-BUT8; Germany: *Email Providers 'Seen As Surveillance Safe Haven'*, BBC (Aug. 23, 2013), http://www.bbc.co.uk/news/blogs-news-from-elsewhere-23851780, *available at* http://perma.cc/7XLV-ADJS.

195. *See, e.g.*, Carlotta Gall & James Glanz, *U.S. Promotes Network to Foil Digital Spying*, N.Y. TIMES (Apr. 20, 2014) http://www.nytimes.com/2014/04/21/us/us-promotes-network-to-foil-digital-spying.html, *available at* http://perma.cc/32SL-J5V9.

196. *Mesh Networks*, P2P FOUNDATION, http://p2pfoundation.net/Mesh_Networks (last visited Feb. 22, 2015), *available at* http://perma.cc/TAR5-XERQ.

197. *Id.*

which a government agency could intercept and copy all flowing data. Proponents therefore claim that a mesh network, if widely adopted, could help stave off surveillance and censorship.[198] Networking protocols such as cjdns aim to make encryption and privacy a built-in component of such a network.[199]

The Seattle Meshnet Project provides one example of an attempt to create such a network.[200] The Athens Wireless Metropolitan Network is a similar project in Greece, and Guifi.net has comparable goals in Spain. Because these networks are in their infancy, the legal implications have yet to be considered.

E. Challenging an NSL

A company could also challenge an NSL directly. Under 18 U.S.C.A. § 3511, an NSL may be modified or set aside if "compliance would be unreasonable, oppressive, or otherwise unlawful."[201] Although the term "unreasonable" is not defined, it has been suggested that because the language was borrowed from Federal Rules of Criminal Procedure 17, "Congress is unlikely to have intended to place the burden on the government to show that the NSL seeks relevant and admissible evidence," and therefore "NSLs

198. Clive Thompson, *How to Keep the NSA Out of Your Computer*, MOTHER JONES (Sep./Oct. 2013), http://www.motherjones.com/politics/2013/08/mesh-internet-privacy-nsa-isp, *available at* http://perma.cc/PC52-CTSL.

199. Hal Hodson, *Meshnet Activists Rebuilding The Internet From Scratch*, NEW SCIENTIST (Aug. 8, 2013), http://www.newscientist.com/article/mg21929294.500-meshnet-activists-rebuilding-the-internet-from-scratch.html, *available at* http://perma.cc/27FN-P3HU. Mesh networks which do not incorporate privacy and encryption into their protocols, such as cdjns, may be no more secure than the Internet. *See* Ed Felten, *Mesh Networks Won't Fix Internet Security*, FREEDOM TO TINKER (Apr. 22, 2014) https://freedom-to-tinker.com/blog/felten/mesh-networks-wont-fix-internet-security/ (arguing that the mesh networking model does not inherently protect users from surveillance), *available at* https://perma.cc/2RX2-GJLP.

200. *What is the Seattle Meshnet Project?*, SEATTLEMESH.NET http://www.seattlemesh.net/about (last visited Feb. 22, 2015), *available at* http://perma.cc/TRJ3-5H9S. The project aims to combine wireless mesh networking and cjdns to create a "decentralized, encrypted . . . routing protocol" which "will be resistant towards attempts to censor or otherwise impede free and legal speech, while also being resistant to natural disasters and other events that might take down ISPs today." *Id.*

201. 18 U.S.C.A. § 3511(a).

probably will be presumed to be reasonable unless they appear plainly unreasonable or unduly burdensome."[202]

A company could also attempt to show that the government official's certification that the information is not sought for "an authorized investigation against international terrorism or clandestine intelligence activities" is incorrect.[203] Similarly, a challenger could assert that the investigation is based solely on activities protected by the First Amendment.[204]

Finally, a company could attempt to show that the information requested in the NSL simply may not be disclosed under the NSL statutes. In 2007, the Internet Archive challenged an NSL on the grounds that 18 U.S.C. § 2709 did not apply to it because it was not an electronic communications service provider.[205] It also claimed that it qualified as a library and thus fell under an exclusion that was carved out for libraries in the ECPA in 2006.[206] In April 2008 the government withdrew the NSL and settled the case.[207] Additionally, a 2013 NSL issued to Microsoft was withdrawn after the company challenged it in court.[208]

Further, between 2007 and 2009, at least two Internet companies took perhaps the strongest and most effective countermeasures against NSLs to date: like the Internet Archive, the companies refused to comply with NSLs on the grounds that the FBI was

202. Kris & Wilson, *supra* note 6, § 20:10. Compare 18 U.S.C.A. § 3511(a) with Fed. R. Crim. P. 17(c)(3) (stating a court may "quash or modify the subpoena if compliance would be unreasonable or oppressive").

203. *Id.*

204. *Id.*

205. *See* Memorandum of Points and Authorities in Support of Petition of Plaintiff Internet Archive to Set Aside National Security Letter, at 6–11, Internet Archive v. Mukasey, No. CV-07-6346-CW (N.D. Cal. Dec. 14, 2007).

206. *Id.*

207. *See* Settlement Agreement, Internet Archive v. Mukasey, No. CV-07-6346-CW (N.D. Cal. Dec. 14, 2007).

208. Brad Smith, *New Success In Protecting Customer Rights Unsealed Today*, MICROSOFT ON THE ISSUES (May 22, 2014), http://blogs.microsoft.com/on-the-issues/2014/05/22/new-success-in-protecting-customer-rights-unsealed-today/, *available at* http://perma.cc/49CW-GY58. It appears the government obtained the information it sought through a different company. *See* In Re National Security Letter, No. C13-1048RAJ (W.D. Wash. 2014) (Order) *available at* http://blogs.technet.com/cfs-file.ashx/__key/communityserver-blogs-components-weblogfiles/00-00-00-82-95/Unsealed-NSL-Challenge.pdf, *available at* http://perma.cc/W5YE-FJCM.

requesting information that falls outside the four categories enumerated in 18 U.S.C. § 2709.[209]

In 2008, the Office of Legal Counsel (OLC) in the DOJ released an opinion concluding that pursuant to 18 U.S.C. § 2709, only name, address, length of service, and local and long distance toll billing records may be disclosed by an NSL recipient.[210] As a result of these conclusions, an Internet company took the position that "if the records identified in Section 2709(b) constitute the exclusive list of records that may be obtained through an ECPA NSL, then the FBI does not have the authority to compel the production of electronic communication transactional records because that term dos not appear in subsection (b)."[211]

The OLC memo thereby creates the framework for a credible, non-constitutional challenge to an NSL by virtually all Internet companies. The importance of this development as a countermeasure to NSLs cannot be overstated. Indeed, the OIG of the DOJ wrote, "[t]he resolution of this issue has significant consequences for the FBI's use of NSLs."[212] Further, the FBI, at least as of the issuance of the OIG of the DOJ report, has been unable overcome this opposition.[213] The FBI has apparently been using FISA Section 215 applications instead.[214]

Indeed, although the FBI Office of General Counsel disagrees with the legal position asserted by the redacted Internet company

209. OFFICE OF INSPECTOR GEN., DEP'T OF JUSTICE, A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF PROGRESS IN IMPLEMENTING RECOMMENDATIONS AND EXAMINATIONS OF USE IN 2007 THROUGH 2009 (2014), at 71, http://www.justice.gov/oig/ reports/2014/s1408.pdf; *see also* Marcy Wheeler, *The Majority of 215 Orders Come from Internet Companies that Refuse NSLs*, EMPTYWHEEL (Aug. 14, 2014), https://www.emptywheel.net/2014/08/14/the-bulk-of-215-orders-come-from-internet-companies-that-refuse-nsls/, *available at* https://perma.cc/PG46-WHM5.

210. Requests for Info. under the Elec. Commc'n Privacy Act, 32 Op. O.L.C. 1, 1 (2008). However, it also concluded that "any call record that a communications provider keeps in the regular course of business and could use for billing a subscriber falls within the scope of section 2709." *Id.* at 11. This reading may expand the scope of information the government may request.

211. A REVIEW OF THE FBI'S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF PROGRESS IN IMPLEMENTING RECOMMENDATIONS AND EXAMINATIONS OF USE IN 2007 THROUGH 2009, *supra* note 209, at 72.

212. *Id.*

213. *See id.* at 73.

214. *See id.*

(based on the OLC opinion), "[w]hen the views of the Office of Legal Counsel are sought on the question of the legality of a proposed executive branch action, those views are typically treated as conclusive and binding within the executive branch. The legal advice of the Office, often embodied in formal, written opinions, constitutes the legal position of the executive branch, unless overruled by the President or the Attorney General."[215] Therefore, because the FBI's General Counsel sought OLC's opinion, the opinion is binding on the FBI (though the FBI may argue about the exact meaning of the OLC opinion).

Based on the success of the Internet company that was redacted in the OIG of the DOJ report, all electronic communications companies could raise such an argument, forcing the government to make requests which require greater oversight, such as those requiring FISC approval.[216] In fact, because companies that cooperate with the government too willingly risk lawsuits (despite statutory immunity),[217] Internet companies should now consider the potential liability which might follow from *not* asserting that 18 U.S.C. § 2709 does not apply to them.

Not surprisingly, because a significant percentage of NSLs are issued to electronic communications companies, the FBI has considered proposing legislation that would explicitly allow

---

215. Randolph D. Moss, *Exec. Branch Legal Interpretation: A Perspective from the Office of Legal Counsel*, 52 ADMIN. L. REV. 1303, 1305 (2000); s*ee also* Arthur H. Garrison, *The Opinions by the Attorney General and the Office of Legal Counsel: How and Why They Are Significant*, 76 ALB. L. REV. 217, 242–43 (2013) (explaining that "[t]he power of the Attorney General and the OLC to issue binding opinions of law within the executive branch is based on the opinions by Attorneys General Cushing, Legaré, Writ, Lincoln, Moody, Cummings, Johnson, Olney, and Bates, and Solicitor General Aldrich on the binding and quasi-judicial nature of their legal opinions; administrative tradition within the Executive Branch to honor the legal opinions of the Attorney General as legally binding; Executive Order 2877 issued by President Wilson (1918); Executive Orders 6166 (1933), 6247 (1933), and 7298 (1936) issued by President Franklin D. Roosevelt; Executive Order 12,146 issued by President Carter (1979); the creation of the Assistant Solicitor General (1933) with the specific task of preparing presidential orders and providing legal opinions to executive departments and the President under the name of the Attorney General; the transference of these responsibilities to the OLC (1953); and subsequent opinions issued by the OLC.").

216. *See supra* note 214 and accompanying text.

217. *See* Fidler, *supra* note 22, at 69 n.58 (stating that "the threat of possible litigation is not insignificant.").

electronic communication transaction records to be requested under 18 U.S.C. § 2709.[218]

F. Repercussions for Failing to Comply

Failure to comply with an NSL carried no penalty until the passage of the USA PATRIOT Act Reauthorization in 2006.[219] Although the NSL statutes required a recipient to comply with an NSL, none of them specified any recourse for the government if a recipient failed to produce records in response to an NSL.[220] The 2006 Reauthorization Act allows the DOJ to "invoke the aid of any district court . . . within the jurisdiction in which the investigation is carried on" or where the recipient of the NSL "resides, carries on business, or may be found" to compel compliance with the request.[221] In response to a request from the DOJ, the court "may issue an order requiring the person or entity to comply" with the NSL.[222] The statute does not make clear whether the court has discretion in ordering compliance with an NSL.[223]

Failure to obey a court order under Section 3511(c) "may be punished by the court as contempt."[224] However, the statute does not specify whether a resistant recipient is subject to civil or criminal contempt. In light of the word "punish" in the statute, it has been suggested that a court would likely hold the resisting recipient in criminal contempt.[225] A criminal contempt proceeding can be determined through a trial, and a defendant in a criminal trial has a constitutional right to a public trial.[226] Although any sensitive information would likely be publicly withheld, an NSL recipient could thereby make it publicly known that it resisted a government

218. *Id.*
219. Kris & Wilson, *supra* note 6, § 20:11.
220. *Id.*
221. 18 U.S.C.A. § 3511(c).
222. *Id.*
223. Kris & Wilson, *supra* note 6, § 20:11.
224. *Id.*
225. *Id.*
226. *See In re* Oliver, 333 U.S. 257, 276 (1948).

order, resulting in a contempt charge, though the fact that the order was an NSL may remain secret.[227]

IV. LIKELIHOOD OF SUCCESS

If challenged in court, the constitutionality of the warrant canary will likely hinge on whether prohibiting the warrant canary is narrowly tailored to promote a compelling government interest. Although no governmental interest is more compelling than the nation's security,[228] the government would have to show that requiring an entity to falsely state that it has never received an NSL is narrowly tailored to further national security.[229]

As discussed in *Gonzales*, the court specified three safeguards that must be in place to ensure that an NSL statute is narrowly tailored.[230] There are, however, differences between the treatment of gag order provisions and warrant canaries, which make the analysis distinguishable. First, warrant canaries are usually in reports that cover long periods of time (six months or more), and they are often published well after the period described in the report.[231] This has major repercussions for an analysis of the first *Freedman* safeguard[232]—that the restraint must be for a specified, brief period. Because a delay is already built into most warrant canaries, the necessary period of non-disclosure will have already elapsed, and the government will find it much harder to prove any period of restraint from publishing is necessary.

Additionally, because communications companies subject to NSLs generally have at least thousands of users,[233] it is unlikely that any one person could assume he or she has been the target of an NSL. The knowledge that a large entity has received an NSL, in the

227. Kris & Wilson, *supra* note 6, § 20:11.
228. Haig v. Agee, 453 U.S. 280, 307 (1981).
229. *See supra* note 156–63 and accompanying text.
230. Doe v. Gonzales, 500 F. Supp. 2d at 400.
231. *See supra* note 147 and accompanying text.
232. *See supra* note 160 and accompanying text.
233. *See, e.g.*, *Grading the top 8 U.S. wireless carriers in the third quarter of 2014*, FIERCEWIRELESS (Nov. 10, 2014), http://www.fiercewireless.com/special-reports/grading-top-8-us-wireless-carriers-third-quarter-2014?confirmation=123, *available at* http://perma.cc/H3BW-2HN2.

absence of more specific information about its target, is not valuable to an adversary of the nation and poses virtually no threat to national security. Indeed, this seems to be the premise behind the government's DAG Letter framework. In fact, by allowing companies to abide by the DAG Letter framework, the government is implicitly conceding that aggregate statistics pose no threat to national security, undermining the argument that gag orders must be perpetual, and warrant canaries must be prohibited.

Second, a prohibition on triggering a warrant canary, like the NSL gag order provisions, would be problematic because it would not require the government to initiate judicial review—the third *Freedman* safeguard. This can be seen in the current Twitter case.[234] Twitter sought to publish statistics regarding the receipt of national security requests (specifically, instances where it has received zero), but the government prohibited Twitter from doing so where Twitter was not the party to initiate judicial review.[235] Twitter was obligated to seek the right to publish the statistics, rather than the government being obligated to go to court to stop the publishing of the statistics. This violates the requirement that the government initiate judicial review in exactly the way the *Mukasey* court explained is unconstitutional.

Even if the government could not prohibit the use of a warrant canary, its utility is severely diminished by the fact that it can only be triggered once (at least for those canaries which state a company has *never* received an NSL or national security request). The government need only issue a single NSL to trigger such a canary, henceforth rendering it useless to that company (or requiring language specifying a time frame during which the canary was valid). The government could therefore strategically seek to trigger a warrant canary, disarming it going forward, robbing a company of the chance to alert users of the receipt of further NSLs.

From the perspective of an Internet user or small company, subscribing to an ISP or telecommunications provider that will fight NSLs and retain as little data as possible is the best practical countermeasure to the NSL. All NSL recipients have the right to

234. *See supra* note 109 and accompanying text.
235. *Id.*

challenge an NSL and any applicable nondisclosure provisions in federal court. Because most ISP recipients see no benefit to challenging NSLs on behalf of customers who will never know an NSL was issued, challenges are extremely rare.[236] However, some ISPs have committed to fighting NSLs, and those sensitive to NSLs should seek them out. The Electronic Frontier Foundation makes this task easier with its "Who Has Your Back?" reports detailing "[w]hich companies have resisted improper government demands by fighting for user privacy in the courts and on Capitol Hill."[237] With more widespread understanding of the 2008 OLC opinion, all Internet companies should consider whether they must assert that they do not fit within 18 U.S.C. § 2709 or risk facing liability from customers following inappropriate or inadvertent disclosures.

Similarly, using an ISP that retains as little data as possible is an effective means to combatting NSLs because the requested information simply will not exist. Nonetheless, legislation such as the Communications Assistance for Law Enforcement Act (CALEA) requires that telecommunications carriers modify their equipment, facilities, and services to ensure that they have built-in surveillance capabilities.[238] This allows federal agencies to monitor all telephone, broadband Internet, and Voice over IP (VoIP) traffic in real-time.[239] Additional proposed legislation, such as the Protecting Children from Internet Pornographers Act of 2011, would require ISPs to retain identifiable user data for at least a year.[240]

Tor is also an effective tool to prevent data collection obtainable through an NSL. However, Tor also has functional limitations, as evidenced by the government's ability to identify child pornographers and managers of black markets, despite their usage of Tor.[241]

236. *See supra* note 176 and accompanying text.

237. *Who Has Your Back? 2014: Protecting Your Data From Government Requests*, ELEC. FRONTIER FOUND. (May. 15, 2014), https://www.eff.org/who-has-your-back-2014, *available at* https://perma.cc/3GGW-JVRD.

238. Communications Assistance for Law Enforcement Act 47 U.S.C. §§ 1001–1010 (1994). *See* Barbara J. Van Arsdale, Annotation, *Construction and Application of Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C.A. §§ 1001 to 1010*, 25 A.L.R. FED. 2d 323 (2008).

239. *Id.*

240. H.R. 1981, 112th Cong. (2011).

241. *See supra* notes 181–82 and accompanying text.

Reidentifacation of anonymous users can occur by capitalizing on software flaws and through side-channel attacks. Nonetheless, as acknowledged by the NSA in slides leaked by Snowden, Tor remains one of the few areas the government has had little success compromising.[242]

Moving servers outside the United States seems to be an effective method of avoiding NSLs.[243] However, avoiding NSLs may come at the cost of exposing the servers to even greater scrutiny.[244] Companies outside of the United States are not subject to the protections guaranteed to American companies. The Fourth Amendment, for example, does not restrain the actions of the federal government against aliens outside of US territory.[245] Additionally, the United States has signed treaties and agreements with many of the nations that could potentially act as hosts for servers.[246] Many of these nations have even fewer protections preventing their governments from obtaining information at will.[247] Once obtained,

242. *'Tor Stinks' presentation—read the full document*, THE GUARDIAN (Oct. 4, 2013), http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document, *available at* http://perma.cc/S2AY-H7A5.

243. *See* Fidler, *supra* note 22, at 75 (stating that "international issues have not played a prominent role in the controversies about national security letters," and explaining that DOJ OIG reports "do not mention international concerns."); *see also infra* note 248 and accompanying text.

244. *See supra* notes 183–94 and accompanying text.

245. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 266 (1990). Although other statutes, internal policies, and international norms ostensibly place limits on the international acquisition of data, in the national security context, DOJ OIG reports regarding NSLs make clear the FBI often ignores statutory safeguards, and "[o]ccasionally, the U.S. government does not respect foreign laws blocking disclosure of information sought under subpoenas." *See* Fidler, *supra* note 22, at 84–85. *See also* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 280 (2015) (arguing that "online contacts should not create Fourth Amendment protection under *Verdugo-Urquidez*. The Fourth Amendment should apply only when a person monitored has sufficient physical or legal contacts with the United States. Next, when the government does not know if a person monitored has Fourth Amendment rights, such monitoring should be deemed constitutional as long as investigators had a reasonable, good faith belief that their conduct complied with the Fourth Amendment.").

246. *See generally Treaties in Force*, U.S. DEP'T OF STATE, http://www.state.gov/documents/organization/218912.pdf (last accessed Feb. 22, 2015) (listing, among other treaties, mutual legal assistance treaties under which the US can request a foreign government pass along data from a foreign target).

247. *See, e.g.*, *Sweden Approves Wiretapping Law*, BBC (June 19, 2008), http://news.bbc.co.uk/2/hi/europe/7463333.stm, *available at* http://perma.cc/3CXQ-XNMS; Andrei Soldatov & Irina Borogan, *In Ex-Soviet States, Russian Spy Tech Still Watches You*, WIRED (Dec. 21, 2012), http://www.wired.com/dangerroom/2012/12/russias-hand/all/, *available at* http://perma.cc/

this data is likely to be shared under, for instance, a mutual legal assistance treaty,[248] resulting in the US government acquiring the data faster and with less resistance than if an NSL were issued and fought.[249]

Utilizing alternative networks and privacy-maximizing protocols are some of the best technological methods to avoid exposure to NSLs. Like keeping no logs of user data, the use of such networks and protocols would preclude the disclosure of user information, even if the government requested it. The downside to these countermeasures is that they essentially require recreating a worldwide network, rivaling the Internet, to be built from scratch. Realistically, the necessary interest to accomplish this goal will not exist in the near future.

CONCLUSION

Assuming that NSLs are constitutional, there are a handful of countermeasures that companies and individuals may take to avoid exposure to the government's requests for information. If properly situated, companies should be encouraged to fight NSLs where the government requests information outside of the scope of the NSL statutes. Some additional possibilities include creating a new, privacy-focused global network, and consistently using Tor. Both options, however, are expensive or inefficient. Others, such as limiting the gathering and retention of user logs, can be immediately implemented with limited expense. Although President Obama has announced modest reforms to the infinite gag orders that accompany NSLs, opponents to the instrument generally should campaign not only for changes to the NSL statutes, but for change to the policies of

---

M9Z7-SA7N; Didi Kirsten Tatlow, *U.S. Prism, Meet China's Golden Shield*, N.Y. TIMES (June 28, 2013), http://rendezvous.blogs.nytimes.com/2013/06/28/u-s-prism-meet-chinas-golden-shield, *available at* http://perma.cc/2ASR-6XZL.

248. *See* Fidler, *supra* note 22 at 82 (stating that "we assume the federal government uses MLATS because national security letters issue without court involvement."). A mutual legal assistance treaty "imposes a binding obligation on the treaty partners to provide specific categories of assistance to each other in designated types of criminal investigations and prosecutions." James I. K. Knapp, *Mutual Legal Assistance Treaties As A Way to Pierce Bank Secrecy*, 20 CASE W. RES. J. INT'L L. 405, 406 (1988).

249. *See* Farivar, *supra* note 194.

companies that are the most likely potential recipients of NSLs, making the tool less useful, and generally enhancing user privacy.