THE YALE LAW JOURNAL FORUM
DECEMBER 19, 2014

Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders

Rebecca Wexler

INTRODUCTION

Since the 1980s, the FBI has issued documents referred to as National Security Letters (NSLs), which demand data from companies—including financial institution records and the customer records of telephone companies and communications service providers—for foreign intelligence investigations.[1] The use of the letters increased dramatically after the attacks of September 11, 2001 and the USA PATRIOT Act's expansion of the FBI's statutory NSL authority.[2] But these letters were rarely publicized or publicly challenged,[3] as they often included gag orders that required recipients not to reveal the contents of the letter, or even its existence.[4] After the leak of classified information by Edward

1. *See* CHARLES DOYLE, CONG. RESEARCH SERV., RS22406, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: A GLIMPSE AT THE LEGAL BACKGROUND 1 (2014), http://fas.org/sgp/crs/intel/RS22406.pdf [http://perma.cc/U5PV-PSJ3].

2. *Id*. at 3.

3. By 2008, only three court challenges to NSLs were publicly known. Ryan Singel, *FBI Targets Internet Archive with Secret 'National Security Letter', Loses*, WIRED (May 7, 2008, 10:22 AM), http://www.wired.com/2008/05/internet-archiv [http://perma.cc/T9FR-9G7T]. Nicholas Merrill, the president of a small internet service provider, brought the first of those challenges in 2004, but he was not permitted to reveal his identity to the public until 2010. *Gagged for 6 Years, Nick Merrill Speaks Out on Landmark Court Struggle Against FBI's National Security Letters*, DEMOCRACY NOW! (Aug. 11, 2010), http://www.democracynow.org/2010/8/11/gagged_for_6_years_nick_merrill [http://perma.cc/7WET-42ND].

4. 18 U.S.C. § 2709(c)(1) (2012) ("If the Director of the Federal Bureau of Investigation . . . certifies that otherwise there may result a danger to the national security of the United States . . . no wire or electronic communications service provider, or officer, employee, or agent thereof, shall disclose to any person . . . that the Federal Bureau of Investigation has sought or obtained access to information or records under this section."); *see also* Dave Maass, *Unsealed Filing Shows DOJ Misled Appeals Court About National Security Letter Gag Orders*, ELECTRONIC FRONTIER FOUND. (Nov. 13, 2014), https://www.eff.org/deeplinks/2014/11/unsealed-filing-shows-doj-misled-appeals-court-about-national-security-letter-gag [http://perma.cc/LQW7-QS3M].

Snowden in 2013, however, numerous corporations were criticized for turning over user data to the government.[5] Communications service providers suddenly became more vocal about challenging the gag orders that accompany NSLs. This Essay summarizes the legal challenges to NSL gags currently underway in the courts and recommends that future debate regarding these issues shift focus to extrajudicial measures that communications service providers are adopting unilaterally to cabin the scope of the government's NSL gag authority. The Essay argues that these extrajudicial measures reframe the legal issues that NSLs raise and could make ongoing legal challenges to NSL gags obsolete before courts have a chance to decide them.

On October 8, 2014, the Ninth Circuit heard oral argument in *In re NSL*, a First Amendment challenge to NSL gags.[6] Just the day before, Twitter filed suit to affirm its right to publish a "warrant canary," a technique whereby cheeky corporations notify customers indirectly regarding a covert surveillance order.[7] Warrant canaries are regularly published statements that document the absence of an NSL (or other secret surveillance order).[8] If the company receives an NSL with a gag, it kills the canary. From silence, audiences may infer receipt. While the legal battles continue, some companies have begun to adopt canaries and other self-help measures to test the constraints of their gags—without awaiting court approval. This Essay examines these self-help practices.

Part I provides a brief historical overview of the statutory authority by which the FBI issues NSLs. Part II discusses the doctrinal wrangling over the legality of NSL gags. Parts III and IV describe two recent self-help trends: first, technology companies have negotiated with the government for the right to publish transparency reports that document their relationship to government surveillance. Second, companies have begun to issue warrant canaries to alert users to covert government demands for data.

---

5. *See, e.g.*, Ewen MacAskill & Dominic Rushe, *Snowden Document Reveals Key Role of Companies in NSA Data Collection*, GUARDIAN, Nov. 13, 2013, http://www.theguardian.com/world/2013/nov/01/nsa-data-collection-tech-firms [http://perma.cc/WFY7-QR99].

6. *In re* Nat'l Security Letter, No. 13-16732 (9th Cir. 2013); *see also In re National Security Letter, Under Seal v. Holder (Sealed)*, U.S. CTS. FOR NINTH CIRCUIT (providing a download link for the audio recording of oral argument from October 8, 2014), http://www.ca9.uscourts.gov/content/view.php?pk_id=0000000715 [http://perma.cc/P34D-ZFTS].

7. Complaint for Declaratory Judgment, Twitter, Inc. v. Holder, No. 14-cv-4480 (N.D. Cal. Oct. 7, 2014), http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/07/National-Security/Graphics/Complaintnew.pdf [http://perma.cc/M9QH-YSEG]; *see also* Brett Max Kaufman, *Twitter's First Amendment Suit & the Warrant-Canary Question*, JUST SECURITY (Oct. 10, 2014, 8:42 AM), http://justsecurity.org/16221/twitters-amendment-suit-warrant-canary-question [http://perma.cc/6FYP-5QU7].

8. Kurt Opsahl, *Warrant Canary Frequently Asked Questions*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/deeplinks/2014/04/warrant-canary-faq [https://perma.cc/DG8Y-2RKU]. An early prominent warrant canary was *Warrant Canary*, RSYNC.NET, http://www.rsync.net/resources/notices/canary.txt [http://perma.cc/8YQE-DE2U].

Both transparency reports and warrant canaries challenge one of the government's recurring claims in defense of its current NSL authority: that the class of would-be speakers whom NSL gags suppress is small.[9] These self-help measures expose a large set of prospective speakers who *want* to speak, but who are silenced by NSL gags and might seek to dispute the gags in court. A large class of challengers could overwhelm the government's current procedure for issuing the gags.[10] Warrant canaries also raise the further issue of how to determine which NSL recipients already *are* speaking when NSL gags interrupt them. Canaries thus challenge government assertions that NSL gags merely silence speech about information the government itself has provided.

In addition, warrant canaries raise a novel legal issue: can the government compel a lie? Imagine that the FBI wants to serve a canary-publishing company with an NSL. To maintain secrecy, the government might try to force the company to keep its canary alive. At this point, publishing the canary would mean publishing the now false statement that no NSL had yet been received—in short, lying. Part IV concludes that under certain circumstances, First Amendment challenges to a compelled false canary could limit otherwise permissible NSL gags.

Finally, Part V predicts that companies increasingly will design canary-like alerts embedded into technology to notify users when their data suffers a security breach. I call this post-Snowden emergent phenomenon "disclosure by design." Automated account activity notices are one step in this direction. For instance, Facebook login notices and Gmail account activity disclosures purport to inform users automatically if someone accesses their information.[11] A similar technique might apply to back-end account access by law enforcement. Relatedly, Apple has marketed the iPhone 6 as having an encryption system with the potential to hamper U.S. government surveillance requests.[12] If Apple's claim were suddenly withdrawn, users could perhaps deduce that the government

9. *See, e.g.*, John Doe, Inc. v. Mukasey, 549 F.3d 861, 874, 879 (2d Cir. 2008) (quoting Appellants' Brief).

10. *Id.* at 879.

11. *See Last Account Activity*, GOOGLE, https://support.google.com/mail/answer/45938 [http://perma.cc/Z2C4-8GVP]; *What Are Login Notifications or Alerts?*, FACEBOOK, https://www.facebook.com/help/162968940433354 [http://perma.cc/GM83-L2M3].

12. *See, e.g.*, *Privacy*, APPLE INC., http://www.apple.com/privacy/government-information-requests [http://perma.cc/8R3K-JQU4] ("Unlike our competitors, Apple cannot bypass your passcode and therefore cannot access [your] data. So it's not technically feasible to us to respond to government warrants for the extraction of this data from devices in their possession running iOS 8."); *see also* David E. Sanger & Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES, Sept. 26, 2014, http://www.nytimes.com/2014/09/27/technology/iphone-locks-out-the-nsa-signaling-a-post-snowden-era-.html [http://perma.cc/6JAE-H3JA] (reporting James B. Comey, Director of the FBI, as commenting, "What concerns me about this is companies marketing something expressly to allow people to hold themselves beyond the law.").

had forced Apple to breach its own security. As with a dead canary, users might infer that Apple had received a covert surveillance order.

While transparency reports challenge government claims about who *wants* to speak, and canaries challenge government claims about who already *is* speaking, disclosure by design establishes who *will* speak in the future. Designers speak today about what they want their system to say tomorrow. As a result, to create an effective NSL gag, the government would have to halt a systems design ex ante, again calling into question whether the gag prevents only speech about information that the government has provided. In addition, communications service providers may be more likely to adopt widespread privacy-protective infrastructure than to publish detailed, granular transparency reports or canaries. Thus, disclosure by design may not only reveal, but also help to produce, a larger class of would-be speakers whom NSL gags suppress.

This Essay neither advocates nor decries disclosure by design. It simply predicts that this emergent technological phenomenon could potentially circumvent NSL gag authority. For those seeking to maintain or enhance NSL nondisclosure requirements, acknowledging the possibility of disclosure by design as a circumvention method generates the possibility to regulate it and thereby to enhance enforcement. For those who seek to narrow or eliminate NSL nondisclosure provisions, considering the possibility of disclosure by design creates an opportunity to thwart individual gags and shift the burden to initiate judicial review from the gag recipient to the government. Widespread adoption could raise the cost and political consequence of NSL gag enforcement.

I. PAST AND PRESENT: NSL STATUTORY AUTHORITIES

NSLs are administrative subpoenas that permit the FBI to demand information from phone companies, Internet service providers, financial service providers, and others.[13] Five federal statutes authorize federal intelligence investigations to deploy NSLs.[14] NSL authority is limited in scope to certain categories of information. For instance, 18 U.S.C. § 2709 permits the FBI to obtain the email addresses and telephone numbers associated with communications, but not the content of email or telephone messages.[15] NSL authority also allows the FBI to prevent NSL recipients from disclosing both the contents of an NSL they receive and the mere fact that an NSL exists.[16]

13. *See* DOYLE, *supra* note 1, at 1-2.

14. *Id.* (summarizing the five statutes authorizing NSLs). The issues in this Essay primarily concern 18 U.S.C. § 2709 (2012).

15. *See* 18 U.S.C. § 2709(b) (2012).

16. *Id.* § 2709(c).

This ban on disclosure has come to be known as a "gag." The NSL process takes place without prior judicial oversight.[17]

The USA PATRIOT ACT expanded FBI authority under four preexisting statutes and added a fifth.[18] After two lower federal courts found NSL gag orders to be constitutionally suspect under the First Amendment,[19] Congress reauthorized and amended the NSL nondisclosure provisions in the USA PATRIOT Improvement and Reauthorization Act of 2005 to provide for ex post judicial review.[20]

Congress also strengthened its oversight of NSL authority in 2005, and this led to a series of Department of Justice Inspector General Reports. These reports found that the FBI had increased exponentially the quantity of NSLs issued since 2000 and the use of NSLs to investigate U.S. persons.[21] Even more alarming, the reports exposed FBI abuses of its authority, including issuing NSLs in violation of statutory requirements, Attorney General guidelines, and its own internal policies.[22]

Likewise, the executive branch has expressed concern over the checks and balances for the FBI's NSL authorities. In December 2013, the President's Surveillance Review Group proposed to mandate prior judicial approval for all NSLs.[23] Critics called the proposal a radical intervention that effectively would kill NSL authority.[24] The FBI issued over 15,000 NSLs seeking information on U.S. persons in 2012 alone.[25] Imposing the burden of government-initiated prior judicial review for each NSL could be paralyzing. The USA FREEDOM Act, which passed the House of Representatives last May[26] but was defeated in

17. DOYLE, *supra* note 1, at Summary.

18. *Id*. at 2.

19. *Id*. at 4.

20. *Id*. at 3.

21. *Id*.

22. *Id*. at Summary (quoting the Department of Justice's Inspector General).

23. Julian Sanchez, *Can We Do Without National Security Letters*, JUST SECURITY (Jan. 9, 2014, 8:15 AM), http://justsecurity.org/5351/national-security-letters [http://perma.cc/6BDS-5ACR].

24. *Id*; *see also* Benjamin Wittes, *Assessing the Review Group Recommendations: Part I*, LAWFARE (Dec. 25, 2013, 2:00 PM), http://www.lawfareblog.com/2013/12/assessing-the-review-group-recommendations-part-i [http://perma.cc/EF4A-K2WF].

25. *Foreign Intelligence Surveillance Act Court Orders 1979-2014*, ELECTRONIC PRIVACY INFO. CENTER, http://epic.org/privacy/wiretap/stats/fisa_stats.html#background [http://perma.cc/RK47-8LEG].

26. Off. Clerk, *Final Vote Results for Roll Call 230*, U.S. HOUSE REPRESENTATIVES, http://clerk.house.gov/evs/2014/roll230.xml [http://perma.cc/MTA9-QASM].

the Senate by two votes on November 18, 2014,[27] proposed alternative reforms. It would have added a sunset date to NSL statutes, limited the types of records that NSLs could reach, and codified a procedure that recipients may use to initiate judicial review.[28] Challenges to the government's NSL authority are therefore not new.

II. DOCTRINAL WRANGLING: NSLS, PRIOR RESTRAINTS, AND THE *MUKASEY* PROCEDURE

Judges, lawyers, and legal scholars have questioned whether NSL gag orders are prior restraints, and if so what kind of prior restraints they are and which judicial test should apply to determine their constitutionality.[29] Prior restraints are laws or regulations that require the government to approve speech before it happens. Compared with ex post regulation, prior restraints pose a higher risk of wrongly prohibiting constitutionally protected speech because the barriers to censorship are reduced.[30] For ex post regulation, the government must bring a successful criminal prosecution, with the attendant procedural safeguards, before it can sanction speech.[31] The same procedural safeguards do not apply for prior restraints.

As a result, the Supreme Court held in the *Pentagon Papers* case that prior restraints are presumptively unconstitutional;[32] in *Nebraska Press Association v. Stuart* that prior restraints are "the most serious and the least tolerable infringement on First Amendment rights," and unacceptable if any plausible alternatives exist to further the government's interests;[33] and in *Freedman v. Maryland* that prior restraints directed at obscene films are constitutional only if the government obtains prompt judicial review of speech prohibitions, car-

27. Charlie Savage & Jeremy W. Peters, *Bill To Restrict N.S.A. Data Collection Blocked in Vote by Senate Republicans*, N. Y. TIMES, Nov. 19, 2014, http://www.nytimes.com/2014/11/19/us/nsa-phone-records.html [http://perma.cc/C53Y-8FXF].

28. *Summary: H.R.3361—USA FREEDOM Act*, CONGRESS.GOV (2014), https://www.congress.gov/bill/113th-congress/house-bill/3361 [http://perma.cc/HE5J-PLFT].

29. *See, e.g.*, Brief of Amici Curiae Floyd Abrams Institute for Freedom of Expression and First Amendment Scholars in Support of the Parties Under Seal at 25-28, Nat'l Sec. Letter, Under Seal v. Holder (Sealed), Nos. 13-15957, 13-16732 (9th Cir. Mar. 31, 2014), http://cdn.ca9.uscourts.gov/datastore/general/2014/05/23/13-15957,13-16731Floyd.pdf [http://perma.cc/KX7L-FKG2]; Jack M. Balkin, *Old-School/New-School Speech Regulation*, 127 HARV. L. REV. 2296, 2334-35 (2014).

30. *See generally* Thomas I. Emerson, *The Doctrine of Prior Restraint*, 20 LAW & CONTEMP. PROBS. 648 (1955) (analyzing the concept and doctrine of prior restraint).

31. *Id*.

32. New York Times Co. v. United States (*Pentagon Papers*), 403 U.S. 713, 714 (1971) (citing Bantam Books, Inc v. Sullivan, 372 U.S. 58, 70 (1963)).

33. 'n v. Stuart, 427 U.S. 539, 559, 563-64 (1976).

ries its burden of proof, and lifts the prohibition at the earliest possible moment once its compelling interest has been satisfied.[34] Even the more lenient *Freedman* standards mandate that "only a procedure requiring a judicial determination suffices to impose a valid final restraint."[35]

Whether the test of *Pentagon Papers, Nebraska Press*, or *Freedman* should apply to NSL gags is disputed.[36] But several judicial opinions have identified NSLs as prior restraints and sought to limit NSL authority. In March of 2013, District Judge Susan Illston ruled that NSL gags violate the First Amendment because they both are substantially overbroad and constitute prior restraints that fail to satisfy even the minimum *Freedman* procedural protections.[37] Judge Illston's ruling followed the Second Circuit's similar holding in *John Doe, Inc. v. Mukasey* in 2008.[38] In *Mukasey*, the court declared an NSL gag to be an unconstitutional prior restraint as applied, although it ultimately upheld the NSL nondisclosure statute under the *Freedman* test by reading it to provide a procedure for recipients to challenge their gag orders in court.[39] In the pending case of *In re NSL*, the Ninth Circuit is reviewing Judge Illston's decision and considering the adequacy of the *Mukasey* solution.[40]

III. TRANSPARENCY REPORTS AND NSL RECIPIENTS WHO WANT TO SPEAK

Even beyond legal challenges to NSL gags, technology companies increasingly are taking the campaign against NSLs into their own hands. As one self-help measure, companies have begun to publish transparency reports that document their relationship to government surveillance. This Part examines the possible legal consequences of these actions for the government's NSL gag authority. It finds that transparency reports complicate the crucial, if under-theorized, issue of how to determine the number of speakers whom NSL gags

34. Freedman v. Maryland, 380 U.S. 51, 58-59 (1965).

35. *Id*. at 58.

36. *See, e.g.*, Brief of Amici Curiae Floyd Abrams Institute, *supra* note 29, at 25-28 (arguing that the more stringent tests in *Pentagon Papers* or *Nebraska Press* should apply); Balkin, *supra* note 29, at 2334-35 (2014) (explaining that the Second Circuit applied the *Freedman* standard in one NSL case).

37. *In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064 (N.D. Cal. 2013).

38. 549 F.3d 861 (2d Cir. 2008).

39. *Id*. at 876-81.

40. *See, e.g.*, Oral Argument at 12:40, Under Seal v. Holder, Nos. 13-15957, 13-16731 (9th Cir. Oct. 8, 2014), http://www.ca9.uscourts.gov/media/view.php?pk_id=0000013407 [http://perma.cc/F8GE-5ZZU] ("I don't know that the Second Circuit really addressed it, but why is it that the petitioner is going to be quote-unquote 'gagged' for as long as the government so desires, and the only way the order ever comes up is if the petitioner does something about it and then the petitioner is, is um-prohibited from attacking it for a year?").

suppress. The reports might therefore undermine courts' confidence in the current procedure for issuing NSL gags and encourage judges to start identifying the gags as classic prior restraints and impermissibly overbroad.

A. An Introduction to Transparency Reports

Some technology companies have negotiated with the government for permission to disclose general information about the number of NSLs they receive and the accounts affected.[41] The result has been a series of reports in which companies showcase their commitments to transparency for the privacy-conscious market. As a policy benefit, these reports help to inform public debate about government surveillance.[42]

In 2013, Google published a transparency report detailing receipt of fewer than 1000 NSLs for each six-month period beginning with January 2009.[43] Microsoft, Facebook, Apple, LinkedIn, and others followed.[44] In January 2014, the government agreed to permit companies to publish the aggregate number of NSLs received over a prior six-month period, as long as those NSLs targeted data from a platform, product, or service at least two years old.[45] The companies may publish the aggregate numbers of NSLs either in bands of 0-999 or combined with other national security surveillance orders in bands of 0-249.[46] To some, these limited forms of permissible disclosure are still not enough.[47] Older companies are subject to time and bulk restrictions on disclosure that en-

41. Letter from James M. Cole, Deputy Attorney Gen., to Colin Stretch et al., Gen. Counsels of Tech. Cos. (Jan. 17, 2014), http://www.washingtonpost.com/r/2010-2019/WashingtonPost/2014/10/07/National-Security/Graphics/dagletter.pdf [http://perma.cc/6SE5-2HSW].

42. *See*, *e.g.*, Dan Auerbach & Eva Galperin, *Google Transparency Report Highlights Just How Much We Don't Know About National Security Letters*, ELECTRONIC FRONTIER FOUND. (Mar. 6, 2013), https://www.eff.org/deeplinks/2013/03/new-statistics-about-national-security-letters-google-transparency-report [http://perma.cc/TR7T-U8WN].

43. *See* Auerbach & Galperin, *supra* note 42; *see also Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/US [http://perma.cc/D558-JWZR]. Google first started including NSLs in its transparency report in 2013, though it started including user data requests generally in 2011. *Transparency Report: FAQ*, GOOGLE, https://www.google.com/transparencyreport/userdatarequests/faq [http://perma.cc/3SEV-HPYY].

44. Nick Bilton, *Tech Companies Offer Update on Government Data Requests*, N.Y. TIMES: BITS (Feb. 3, 2014, 4:29 PM), http://bits.blogs.nytimes.com/2014/02/03/tech-companies-release-government-data-requests [http://perma.cc/U5WR-Z4CN].

45. Letter from James M. Cole, *supra* note 41, at 2-3.

46. *Id*.

47. Alex Abdo, an attorney with the American Civil Liberties Union, called the transparency reports "a small step in the right direction, but . . . not nearly enough to allow the public to judge for itself the full extent of government surveillance." Bilton, *supra* note 44.

sure vagueness.[48] In a constitutionally suspect speaker-based distinction, younger companies and those who provide new-capability services lack permission to disclose at all.[49]

B. Transparency Reports and the Number of Speakers Whom NSL Gags Suppress

Despite the dissatisfaction of some, transparency reports complicate certain government assertions about NSL gags. The reports suggest that the class of speakers whom the gags suppress is larger than the government claims.[50] This issue carries both practical and legal consequences because the scale of the suppressed speaker class affects the government's current process for issuing gag orders.[51] Following *Mukasey*, the FBI now uses a "reciprocal notice procedure," by which NSL recipients may notify the government if they wish to challenge a gag order in court.[52] The government then initiates judicial review.[53] And as the Second Circuit ruled in *Mukasey*, NSL gags are unconstitutional unless the government follows this procedure.[54]

For the *Mukasey* solution to work, the class of would-be-speakers who seek to challenge their gag orders must be small. Were a large portion of the telecommunications industry to change its security practices and decide to resist

---

48. Letter from James M. Cole, *supra* note 41, at 3 ("[T]here will be a delay of two years for data relating to the first order that is served on a company for a platform, product, or service . . . for which the company has not previously received such an order . . . . For example, a report published on July 1, 2015, will not reflect data relating to any [new type of order] received during the period ending December 31, 2014. Such data will be reflected in a report published on January 1, 2017.").

49. *See* Kimberly Weisul, *Surveillance Settlement: Big Companies Throw Small Ones Under the Bus*, INC.COM, http://www.inc.com/kimberly-weisul/big-companies-throw-small-ones-under-the-bus-in-surveillance-settlement.html. Kurt Opsahl raised the issue of this speaker-based distinction in oral argument in the *Under Seal v. Holder* appeal. Oral Argument, *supra* note 40, at 30:39 ("[The government has] de facto created a license for some providers to be able to talk, other providers to not be able to talk.").

50. Oral Argument, *supra* note 40, at 27:58 ("Mr. Letter has said that service providers don't want to speak out. And I think that this has not actually been borne out. More and more service providers are issuing transparency reports where they are providing aggregate numbers of the types of legal processes that they receive."). Note that on other fronts, the reports could either strengthen the justification for gag orders by showing them to be narrowly tailored or weaken the justification by undermining the government's assertion of a compelling interest in secrecy. *Id.* at 28:38 ("[Do the reports] show that secrecy is not necessary as the government argued, or does it show that in fact it's fairly narrow because you are able to speak in general about the receipt of these NSLs?").

51. *See In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1073-74 (N.D. Cal. 2013).

52. John Doe, Inc. v. Mukasey, 549 F.3d 861, 883-85 (2d Cir. 2008).

53. *Id.*

54. *Id.* at 885.

disclosure prohibitions, the solution would become untenable. Widespread adoption of the procedure would overwhelm the courts and inhibit the current scale of NSL usage. According to the government's own estimate, the FBI "would not be able to function" if it had to review a large percentage of the NSLs it issues.[55]

Perhaps for this reason, the government consistently has emphasized in briefs and oral arguments that the class of speakers whom NSL gags suppress is miniscule,[56] despite the thousands of gags issued each year.[57] Government counsel claimed during oral argument in the Ninth Circuit in October 2014, "overwhelmingly the recipients do not wish to speak in the way that is involved here. They have not said, no, no, no, we want to constantly say we got this NSL, we got this NSL then we got another one. That's not what they—they've said they want."[58] Similarly, the government argued in the district court that "only a handful of recipients have provided the Government with notice that they intend to challenge the nondisclosure requirement,"[59] and previously in the Second Circuit that "there is no reason to believe that most recipients of NSLs wish to disclose that fact to anyone."[60]

Transparency reports cast doubt on the government's assertions and raise the question of how to measure the number of NSL gag recipients who wish to speak. In the government's view, the *Mukasey* process itself serves as a measurement tool. Accordingly, a reciprocal notice procedure that runs smoothly can show that the number of gag recipients who wish to speak is small. A reciprocal notice procedure overwhelmed to the point of dysfunction would show the opposite.

Yet the *Mukasey* process may be a poorly calibrated meter. It assumes that a system that runs smoothly also serves NSL recipients adequately. This could be wrong. The reciprocal notice procedure itself might produce inertia, intimidation, and costs that deter some would-be-speakers from disputing their gags. Since the default presumption under reciprocal notice is no judicial review, recipients must self-nominate to challenge the government. A lack of resources to

---

55. Oral Argument, *supra* note 40, at 20:34 ("The Bureau would not be able to function if it had to look at every single NSL issued over the years, thousands and thousands of them, every year, and it had to look at every single one and determine whether confidentiality still had to stay.").

56. *See*, *e.g.*, Brief for Defendants-Appellants at 39, *Doe*, 549 F.3d at 874 (No. 07-4943-cv).

57. In 2013, the White House reported that the FBI issued approximately sixty NSLs each day on average. President's Review Grp. on Intelligence & Commc'ns Techs., *Liberty and Security in a Changing World*, WHITE HOUSE (Dec. 12, 2013), http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [http://perma.cc/W5PE-MLCU].

58. Oral Argument, *supra* note 40, at 21:05.

59. Government's Opening Brief at 14, *In re* Nat'l Sec. Letter, No. 13-15957 (9th Cir. 2014).

60. *Doe,* 549 F.3d at 879 (quoting Appellants' Brief at 33).

hire an attorney—or fear of reprisal—could stop some from taking this step, especially given that the gags themselves prevent a safety-in-numbers association. Anyone who considers initiating a challenge will be unable to find like-minded NSL recipients and could wrongly imagine that he or she is alone in his or her views, or might feel vulnerable identifying himself or herself to the government, and will be unable to seek support from family, friends, or the public.[61] In this case, the *Mukasey* measure would generate artificially low readings of the number of suppressed speakers. This measure would count only those with the initiative and courage to deploy reciprocal notice and ignore those who wish to speak but not to volunteer to hold the government accountable in court.

Transparency reports offer an alternate metric. The volume of transparency reports suggests the government may be underestimating. Critically, the reports need not yield substantially more precise results than the *Mukasey* measure in order to challenge the government's current arguments in favor of its NSL gag authority. The mere existence of an alternate and divergent metric creates ambiguity concerning the government's claims.

C. Legal Implications of the Transparency Report Measure

That the number of would-be-speakers suppressed by NSL gags may be greater than the government argues reframes the legal issues that NSLs raise. To be sure, the idea that protection from government censorship might turn on the number of speakers who wish to communicate is anathema to First Amendment principles and doctrine.[62] But if it becomes clear that NSL gags stifle a large class of speakers, this could alter legal outcomes in other ways.

The possibility of a large, if previously unrecognized, class of NSL recipients who wish to speak could cause courts to lose confidence in the long-term practical viability of the reciprocal notice procedure. They might require its modification or revert to the Second Circuit's initial finding that, absent the reciprocal notice procedure, NSL gag orders are unconstitutional.[63]

Moreover, courts might reconsider past findings that NSL gag orders are not "typical prior restraint[s]."[64] The Second Circuit held that the NSL nondisclosure requirement is "not a typical example of [a prior restraint] for it is

---

61. *See, e.g.*, *My National Security Letter Gag Order*, WASH. POST, Mar. 23, 2007, http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html [http://perma.cc/W3VL-TX5U].

62. *See, e.g.*, Eugene Volokh, *Freedom of the Press as an Industry, or for the Press as a Technology? From the Framing to Today*, 160 U. PA. L. REV. 459, 506 (2012) ("[T]he Court's decisions since 1931 generally take the all-speakers-equal view.").

63. *Doe*, 549 F.3d at 883-85.

64. *Id.* at 877.

not a restraint imposed on those who customarily wish to exercise rights of free expression."[65] More recently, Judge Illston ruled that NSL gags "may not be a 'classic prior restraint.'"[66] A flood of transparency reports could sway courts to identify NSL gags as prior restraints that trigger full *Freedman* or *Nebraska Press* protections and the *Pentagon Papers* presumption of unconstitutionality.[67]

Finally, the prospect of a substantial class of gagged would-be-speakers might nudge courts towards finding unconstitutional overbreadth. Judge Illston held that because NSL gags ban speech about both the content of an NSL and the mere fact of its receipt, even in situations in which blocking only the former would adequately serve the government's national security interest, the gags are "impermissibly overbroad and not narrowly tailored."[68] The Ninth Circuit panel currently considering her decision may be more sympathetic to her finding in a world of mushrooming transparency reports.

IV. WARRANT CANARIES AND NSL RECIPIENTS WHO ARE SPEAKING CONSTANTLY

In another move to take control, Google, Apple, rsync.net, Rise Up, CloudFlare, and other technology companies have adopted a clever strategy to test the potency of NSL gags—warrant canaries.[69] A warrant canary is a regularly published statement that the speaker has not received an NSL or other secret surveillance order.[70] If the canary disappears, observers may infer that the government has delivered an order.[71] To prevent this from happening, the government might attempt to force a canary-publishing NSL recipient to keep issuing a false canary, or to lie.[72]

---

65. *Id*. at 876.

66. *In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1071 (N.D. Cal. 2013) (quoting *Doe*, 549 F.3d at 878).

67. *Cf. id*. (following a finding that NSL gags are not classic prior restraints with a holding that they do "not need to satisfy the extraordinarily rigorous *Pentagon Papers* test").

68. *Id*. at 1076.

69. For an excellent overview of companies that have adopted canaries, see Naomi Gilens, The NSA Has Not Been Here: Warrant Canaries as Tools for Transparency in the Wake of the Snowden Disclosures app. 15-16 (Apr. 2014) (unpublished manuscript), http://ssrn.com/abstract=2498150 [http://perma.cc/KG2Y-962H].

70. *See* Opsahl, *supra* note 8; *see also* Zack Whittaker, *Apple Omits 'Warrant Canary' from Latest Transparency Reports; Patriot Act Data Demands Likely Made*, ZDNET (Sept. 18, 2014, 12:15 PM PDT), http://www.zdnet.com/apple-omits-warrant-canary-from-latest-transparency-report-suggesting-patriot-act-data-demands-made-7000033840 [http://perma.cc/TN3Q-92DV].

71. Opsahl, *supra* note 8.

72. *See, e.g.*, Kaufman, *supra* note 7.

This section explores the potential impact of warrant canary adoption. It finds that canaries rebut the government's consistent assertion that NSL gags merely stifle speech about information the government itself has provided. Canaries create a system of constant speech, which NSL gags must then interrupt. The interruption silences an expression that pre-existed government involvement. Canaries also raise the intriguing question of whether the government can compel a lie consistent with the First Amendment. Compelled false canaries should trigger strict scrutiny review. As a result, canaries could either limit otherwise permissible NSL gags or become a moot issue, depending on whether or not courts begin to identify the gags as traditional prior restraints.

A. An Introduction to Warrant Canaries

On September 18, 2014, Apple stopped publishing a statement that previously it had issued regularly.[73] The statement announced that the company had received no surveillance orders under Section 215 of the USA Patriot Act.[74] Attentive observers theorized that Apple could have received a Section 215 order.[75] While this specific dead canary was probably a false alarm caused by a change in Apple's reporting format,[76] the uproar it generated shows that dead canaries can transmit information to observers.

Companies may publish canaries to provide as much information to the public as legally permissible; to express a commitment to privacy and transparency in clear and regular form; or to inspire public debate through protest. Canaries grant transparency mechanisms to young companies and new capability service providers, which were excluded from the government-approved bulk disclosure agreement.[77] From a public policy perspective, canaries may offer evidence to verify or challenge government statements about the extent of government surveillance practices.

---

73. *See* Whittaker, *supra* note 70.

74. *See* Cyrus Farivar, *Apple takes strong privacy stance in new report, publishes rare "warrant canary"*, ARS TECHNICA (Nov. 5, 2013, 5:52 PM), http://arstechnica.com/tech-policy/2013/11/apple-takes-strong-privacy-stance-in-new-report-publishes-rare-warrant-canary [http://perma.cc/XU3Y-GTD4].

75. *See, e.g.*, Jeff John Roberts, *Apple's "Warranty Canary" Disappears, Suggesting New Patriot Act Demands*, GIGAOM (Sept. 18, 2014, 8:17 AM), https://gigaom.com/2014/09/18/apples-warrant-canary-disappears-suggesting-new-patriot-act-demands [http://perma.cc/M6US-BYDM]; Whittaker, *supra* note 70.

76. In this particular instance, the disappearance of Apple's canary caused significant confusion, as some observers theorized that Apple had merely updated the format of its transparency report and that the change in format did not signal receipt of a Section 215 order. *See* @csoghoian, TWITTER (Sept. 18, 2014, 10:53 AM), https://twitter.com/csoghoian/status/512660812268204032 [http://perma.cc/DN9R-NDAG].

77. Letter from James M. Cole, *supra* note 41, at 3.

Additionally, canaries offer all companies the capacity to deliver more specific, granular, or targeted information than the current government disclosure guidelines permit. For instance, canaries can reveal the jump from zero surveillance orders to at least one surveillance order. This may be particularly informative for parties that are contractually responsible for the security of privileged information, such as doctors or lawyers. Canaries could also inform audiences of compliance with a surveillance order separately from notice of its receipt.

B. Canaries and the Continuity of Speech That NSL Gags Stifle

Canaries enable prospective gag recipients to speak constantly, before any NSLs issue. This temporal aspect challenges a second of the government's arguments for its NSL gag authority: that the gags merely prevent speech about information the government itself has provided as part of a covert investigation. In the government's words, an NSL gag "arises not to suppress a preexisting desire to speak, but only as a result of government interaction with an NSL recipient."[78] Based on this assertion, the government claims that recipients have no First Amendment rights to challenge the gag.[79] Canaries expose the alternative view that NSL gags silence communications that predate any interaction with the government.

C. Canaries and the First Amendment Status of Compelled Lies

Finally, warrant canaries raise the specter of a new legal issue: can the government compel a lie?[80] If the government served a canary-publishing company with a secret surveillance order, could it then force the recipient to continue to publish what would have become a false—or zombie—canary? The issue of compelled lies is now live. A Twitter lawsuit against the government seeking the right to publish a canary in the first place, filed on October 7, 2014, is a preliminary step towards resolving the issue.[81]

---

78. John Doe, Inc. v. Mukasey, 549 F.3d 861, 874 (2d Cir. 2008).

79. Government's Opening Brief at 35, *In re* Nat'l Sec. Letter, No. 13-15957 (9th Cir. 2014) ("There is no First Amendment right to disclose information learned through participation in a secret government investigation.").

80. *See, e.g.*, Kaufman, *supra* note 7; Ben Johnson, *A Canary in the Coal Mine . . . and in Your Mac*, MARKETPLACE, http://www.marketplace.org/topics/tech/canary-coal-mine-and-your-mac [http://perma.cc/7E86-N4DJ]; Gilens, *supra* note 69.

81. Ellen Nakashima, *Twitter Sues U.S. Government Over Limits on Ability To Disclose Surveillance Orders*, WASH. POST, Oct. 7, 2014, http://www.washingtonpost.com/world/national-security/twitter-sues-us-government-over-limits-on-ability-to-disclose-surveillance-orders/2014/10/07/5cc39ba0-4dd4-11e4-babe-e91da079cb8a_story.html [http://perma.cc/S77V-9AJJ].

Mandating a canary should provoke strict scrutiny. If the government were to force an NSL recipient to publish a false canary, it would do so precisely to further the canary's expressive purpose (and not in a way incidental to this purpose). Outside the commercial speech context, when the government forces true statements for their expressive purpose, strict scrutiny review applies.[82] Hence *a fortiori*, forced lies should trigger the strict scrutiny test of narrow tailoring to a compelling government interest.

Therefore, if technology companies fail in their ongoing challenges to convince courts that NSL gag orders are classic prior restraints, they could turn instead to defending their rights to use canaries. Requiring false canaries probably would trigger strict scrutiny, while NSL gags alone might not. Hence, canaries could establish limits to otherwise permissible gags.

Even if they faced the same level of scrutiny, First Amendment challenges to compelled lies might be stronger than challenges to compelled silence. The optical differences between forced action and inaction may inspire in judges additional antipathy for the former, potentially leading them to engage in a more searching examination of the interests that the government claims are compelling.[83]

The government may also find it difficult to prove that compelled publication of a false canary is narrowly tailored. In prior negotiations, it has permitted some companies to report the number of surveillance orders they receive in bands of 250.[84] Why not allow canary-publishing recipients to do the same? In other words, forcing recipients to issue zombie canaries could fail a narrow tailoring test because there is a less restrictive alternative that the government already employs.[85] To be sure, the government might respond that the bulk transparency reporting guidelines do not achieve the government's compelling interest when those reports would reveal a jump from zero to one surveillance orders. Even so, the narrow tailoring of false canaries would be disputable in ways that NSL gags are not.

---

82. *See, e.g.*, Leslie Gielow Jacobs, *Pledges, Parades, and Mandatory Payments*, 52 RUTGERS L. REV. 123, 183 (1999) ("Where the government acts to manipulate the marketplace of ideas, strict scrutiny applies unless the compelled expression falls into the narrow category of factual disclosures imposed to enhance consumer information . . . .").

83. *Cf.* Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55 (1964) (identifying an "unwillingness to subject those suspected of crime to the cruel trilemma of self-accusation, perjury, or contempt"). *But see* Akhil Reed Amar & Renee B. Lettow, *Fifth Amendment First Principles: The Self-Incrimination Clause*, 93 MICH. L. REV. 857, 890 (1995) ("But our justice system has no such scruples about compelling self-damaging answers from a civil litigant . . . .").

84. Letter from James M. Cole, *supra* note 41, at 3.

85. *See, e.g.*, Burwell v. Hobby Lobby Stores, Inc., 134 S. Ct. 2751, 2759 (2014) (holding that government regulations that impose a substantial burden on religious exercise must be "the least restrictive means of serving a compelling government interest").

A finding that NSL gags are classic prior restraints would render the false canary issue moot. If courts find the gags to be unconstitutional prior restraints, the government would face a larger constitutional hurdle to impose the gag in the first place than to compel a lie to maintain its efficacy after the fact. If instead the government successfully argues that NSL gags are constitutional prior restraints, then compelled false canaries should likewise be permissible. The gags would have survived the "most serious and the least tolerable" presumption against their legality.[86] False canaries might only raise a lesser challenge. Further, courts sufficiently sympathetic to the NSLs to declare them constitutional prior restraints would then be less likely to restrain them based on a novel compelled lies claim.

V. DISCLOSURE BY DESIGN AND NSL RECIPIENTS WHO WILL SPEAK IN THE FUTURE

Courts, lawyers, and legal scholars have focused thus far on how NSL gag orders affect linguistic communications and predominantly have overlooked a gag's relationship to alternative means for expression.[87] Alternative methods that NSL recipients could use to disclose receipt of surveillance orders include privacy-protective infrastructure designed to notify users if their data suffers a security breach, or what I call "disclosure by design." Disclosure by design is similar to a technologically implemented canary; a potential speaker designs a system that would expose the receipt of a covert surveillance order to a target interpretive community.

This Part details existing and hypothetical examples to elucidate the concept of disclosure by design. Whereas transparency reports challenge government claims about who *wants* to speak, and canaries challenge government claims about who already *is* speaking, with disclosure by design, speakers establish their intent today about what they *will* say in the future. To create an effective NSL gag, the government would have to prohibit a systems design ex ante.

---

86. 'n. v. Stuart, 427 U.S. 539, 559 (1976).

87. *See, e.g.*, Letter from Jonathon H. Levy, Att'y, U.S. Dep't of Justice, to Molly C. Dwyer, Clerk of Court, U.S. Court of Appeals for the 9th Circuit (Nov. 6, 2014), http://cdn.ca9.uscourts.gov/datastore/general/2014/11/12/13-15957%20Letter.pdf [http://perma.cc/6HNK-PHJL] (confirming that NSL gags limit recipients' ability to engage in public discussion); Brief of NSL Recipients Who Had Challenged Their NSL's as Amici Curiae in Support of Petitioner-Appellant at 11-14, *Under Seal v. Holder*, Nos. 13-15957, 13-16731 (9th Cir. Apr. 2, 2014) (arguing that NSL gags prevent recipients from lobbying the government for change); Oral Argument, *supra* note 40, at 30:45 ("And there's many things that a provider might want to say in addition to the particular number of NSLs they've received in an annual period . . . . They may want to say, like, there's been an increased number, there's really been an upswing this year.").

Disclosure by design challenges the efficacy of the government's current NSL gags and, additionally, government arguments that the gags prohibit merely information the government itself has provided. From a policy perspective, disclosure by design might not only reflect a larger class of would-be-speakers than the government has claimed are suppressed by NSL gags, but could also serve to expand that class.

A. An Introduction to Disclosure by Design

Disclosure by design is an emergent phenomenon. Journalists and activists have already proposed partially automated canary services that would send regular prompts to post a manual message, "No secret orders yet."[88] Others have suggested a "warrant canary metatag" built into web browsers.[89] Tamper-evident intrusion detection systems might serve a similar function.

For instance, tripwires could notify users if anyone accesses their data. To comply with an NSL order for user information, a communications service provider would have two choices: It could access the data and trip the wire, notifying the user. Alternatively, it first could remove the tripwire entirely and then access the data. The user would not receive notice. However, even in the second instance, a notice control could be established in advance. The user could hire a third party service to request data regularly and test whether the wire trips. If the tripwire fails, then the party could infer compliance with a covert surveillance order.[90] Of course, this system would be only as trustworthy as the communications service provider that runs it. But the same is true of linguistic canaries.

Automated notice systems also directly could reveal secret government data collection. On November 20, 2014, Amnesty International released Detekt, a tool that notifies users if their computers are compromised by known surveillance spyware that some governments have used to target journalists and human rights activists.[91] Similarly, a "trap canary" could identify uniquely content in a pool of user data and lace it with links to a fake URL designed to

88. Cory Doctorow has described such a system: "[T]he service sits there, quietly sending a random number to you at your specified interval, which you sign and send back as a 'No secret orders yet' message." Cory Doctorow, *How To Foil NSA Sabotage: Use a Dead Man's Switch*, GUARDIAN, Sept. 9, 2013, http://www.theguardian.com/technology/2013/sep/09/nsa-sabotage-dead-mans-switch [http://perma.cc/4PDX-5GM7].

89. timothy, *Time For a Warrant Canary Metatag?*, SLASHDOT, http://tech.slashdot.org/story/13/11/17/1411215/time-for-a-warrant-canary-metatag [http://perma.cc/P922-RB8Z].

90. chii, HACKER NEWS (June 13, 2013), https://news.ycombinator.com/item?id=5873694 [http://perma.cc/8LE4-RU7K].

91. *Detekt: New Tool Against Government Surveillance – Questions and Answers*, AMNESTY INT'L (Nov. 20, 2014), http://www.amnesty.org/en/news/detekt-new-tool-against-government-surveillance-questions-and-answers-2014-11-20 [http://perma.cc/M3ZV-TSWX].

collect information from visitors. If a government intelligence analyst tried the link, it would alert the user to the security breach.[92] To be sure, sophisticated government analysts may be hard to "trap," but any obstacles would raise the cost of enforcing NSL gags.

Nor must disclosure by design be automated fully or highly engineered. It could be possible obliquely to disclose receipt of an NSL through a technological change that carries symbolic meaning for an interpretive community. For instance, a design could communicate the idea—accurately or inaccurately—that a system has no capacity to store information that could be delivered to the government or strips the designer of the power to access information and thus bars its delivery to an investigator.[93] If this communication suddenly disappears, then audiences could interpret it as a dead canary.

For example, on April 16, 2014, Ladar Levison, founder of the pro-privacy email service Lavabit, was held in contempt of court for delaying compliance with a series of government orders for customer records.[94] Those orders came with nondisclosure mandates.[95] Yet just weeks after Levison received the orders, journalists deciphered and published information, if speculative, about their existence.[96]

---

92. Roger A. Grimes, *Beyond Honeypots: It Takes a Honeytoken To Catch a Thief*, INFOWORLD: SECURITY ADVISER (Apr. 16, 2013), http://www.infoworld.com/article/2614310/security/beyond-honeypots—it-takes-a-honeytoken-to-catch-a-thief.html [http://perma.cc/77G3-WKU2].

93. *See*, *e.g.*, Lorenzo Franceschi-Bicchierai, *Wickr: Can the Snapchat for Grown-Ups Save You from Spies?*, MASHABLE (Mar. 4, 2013), http://mashable.com/2013/03/04/wickr [http://perma.cc/KSM9-2J5P].

94. *In re* Under Seal, 749 F.3d 276, 293 (4th Cir. 2014).

95. As Lavabit's appellant brief describes, "The government forbade Lavabit from telling anyone that it had compromised its security in this way: not its customers, not its business partners, and not the relevant cryptographic authorities." Brief of Appellant at 19, *In re* Grand Jury Proceedings, No. 13-4625, 2013 WL 5574549 (4th Cir.).

96. Journalist Kevin Poulsen at *Wired Magazine* hypothesized that Lavabit had received either an NSL or a search or eavesdropping warrant. Kevin Poulsen, *Edward Snowden's Email Provider Shuts Down Amid Secret Court Battle*, WIRED (Aug. 8, 2013) http://archive.wired.com/threatlevel/2013/08/lavabit-snowden [http://perma.cc/WH6M-6UA9]. Journalist Amy Davidson at *The New Yorker* repeated this claim in quotation. Amy Davidson, *The N.S.A. and Its Targets: Lavabit Shuts Down*, NEW YORKER: DAILY COMMENT (Aug. 8, 2013), http://www.newyorker.com/news/amy-davidson/the-n-s-a-and-its-targets-lavabit-shuts-down [http://perma.cc/J2H4-SWSC]. Glenn Greenwald writing for *The Guardian* reiterated the idea by analogy: "Just as is true for people who receive National Security Letters under the Patriot Act, Lavabit has been told that they would face serious criminal sanctions if they publicly discuss what is being done to their company." Glenn Greenwald, *Email Service Used by Snowden Shuts Itself Down, Warns Against Using US-Based Companies*, GUARDIAN: COMMENT IS FREE, Aug. 9, 2013, http://www.theguardian.com/commentisfree/2013/aug/09/lavabit-shutdown-snowden-silicon-valley [http://perma.cc/PBJ5-877T].

The journalists were tipped off when Levison terminated his technological system. In his own words, Levison had engineered and advertised a system that was supposed to be "secure against . . . secret monitoring that the government was proposing to do."[97] After receiving covert government orders for user information, Levison shut down his servers. Then he posted in explanation, "the first amendment [sic] is supposed to guarantee me the freedom to speak out in situations like this. Unfortunately, Congress has passed laws that say otherwise."[98] Observers deciphered the message. "Reading between the lines," wrote journalist Kevin Poulsen, "it's reasonable to assume Levison has been fighting either a National Security Letter seeking customer information—which comes by default with a gag order—or a full-blown search or eavesdropping warrant."[99]

The information Levison transmitted lacked granularity. Observers could not specify the government surveillance authority under which he received a demand for information.[100] Yet however circuitous Levison's speech—journalist Glenn Greenwald called it "hostage-message-sounding missives"[101]—to primed interpretive eyes, Levison's technological act plus linguistic message communicated receipt of a secret government surveillance order.

Similarly, the founder of the private messenger service Wickr recently said of its design, the "architecture eliminates backdoors; if someone was to come to us with a subpoena, we have nothing to give them."[102] Like Apple's iPhone 6, if Wickr's claim were both trustworthy and suddenly withdrawn, users might infer that the government had forced Wickr to breach its own security. In short, users might infer that Wickr had received a covert surveillance order.

Now consider the Wickr scenario again, this time without any linguistic expressions. Wickr need not tell people directly that it had dropped its initial security guarantee. If the design actually does what Wickr claims, it could produce the same effect simply by disclosing its full infrastructure for public au-

97. Brief of Appellant, *supra* note 95, at 19 ("The government insisted that all of those parties be affirmatively misled into believing that the system remained secure against exactly the kind of secret monitoring that the government was proposing to do.").

98. Poulsen, *supra* note 96.

99. *Id.* Security blogger Bruce Schneier echoed the idea by inference: "Could you imagine what would happen if Mark Zuckerberg or Larry Page decided to shut down Facebook or Google rather than answer National Security Letters?" Bruce Schneier, *Lavabit E-Mail Service Shut Down*, SCHNEIER ON SEC. (Aug. 9, 2013), https://www.schneier.com/blog/archives/2013/08/lavabit_e-mail.html [http://perma.cc/V2BX-345M].

100. CBS News columnist Declan McCullagh posited a federal court order over an NSL, "because [NSLs] are limited in scope and don't apply to prospective surveillance, meaning a shutdown wouldn't accomplish anything." Declan McCullah, GOOGLE+ (Aug. 8, 2013) https://plus.google.com/+DeclanMcCullagh/posts/EujgUYbrEwv [http://perma.cc/UJ8R-7KM8].

101. Greenwald, *supra* note 96.

102. *See* Franceschi-Bicchierai, *supra* note 93.

dit.[103] Sophisticated audiences could review the technical system and decipher for themselves that "the architecture eliminates backdoors" and collects no information that Wickr could deliver in response to a subpoena. Like transparency reports and canaries, the technical guarantees of a design could be more or less granular and potentially provide user-specific, or even content-specific, security guarantees.

Were the government to force Wickr to breach its own security, Wickr would have to alter its design. The minute the design changes to become less secure, audiences could interpret the adjustment as a dead canary. Wickr need only disclose its before-and-after designs to enable sophisticated audiences to infer compliance from the changed architecture. Unless the government began to require communications service providers to keep their designs secret ex ante, any alteration would tip audiences off that something was amiss.

The above examples show that engineers may be able to design around NSL gags. While the legal consequences and technical feasibility of innovative privacy-protective technologies remain speculative, their development and growing adoption is not.[104]

B. The Disclosure by Design Echo Effect

Disclosure by design produces an echo effect; designers speak today about what they want their systems to say tomorrow. Thus, operative NSL gags would have to bar the creation of innovative infrastructure well in advance of any speech about NSLs. As a result, it would be even more difficult for the government to claim that expressions emanating from an automatic design, planned in the past, are communicating information that the speaker has just learned from the government. Again, the government has argued that the speech suppressed by NSLs deserves less First Amendment protection because this speech concerns only information the speaker acquired from a secret government investigation.[105] Yet, to prevent disclosure by design, the government might have to gag expressions that occur months or even years before the speaker receives an NSL.

When speech and non-expressive conduct intertwine, the government ordinarily may regulate a non-expressive aspect of the conduct. In *United States v.*

---

103. Note that currently, Wickr does not publically release its source code. *See id.* ("But Wickr also has a 'proprietary algorithm,' secret to everybody except the app developers and some trusted reviewers. Wickr doesn't have open source code.").

104. *See, e.g.*, Joris V.J. van Hoboken & Ira S. Rubinstein, *Privacy and Security in the Cloud: Some Realism About Technical Solutions to Transnational Surveillance in the Post-Snowden Era*, 66 ME. L. REV. 488, 510-14 (2014) (describing the development of privacy-protecting technology as it relates to storing information in the cloud).

105. Doe v. Mukasey, 549 F.3d 861, 874 (2d Cir. 2008).

O'Brien, the Court held that government regulation of conduct may be permissible despite incidental restrictions on expression "if it furthers an important or substantial governmental interest . . . unrelated to the suppression of free expression."[106] But in the case of disclosure by design, the opposite is true. Were the government to attempt to prohibit technology because it violates an NSL gag order, it would be regulating the conduct precisely in order to suppress its expressive capacity. In this scenario, *O'Brien* would provide the government with no protection from strict scrutiny review.[107]

C. Policy and Predictions for Disclosure by Design

Communications service providers, on the whole, may be more likely to adopt disclosure by design infrastructure than to publish granular transparency reports or canaries. If this happens, then disclosure by design not only will reveal the existence of a broad class of speakers who are suppressed by NSL gags, but also will help to produce and expand this class. Once again, such expansion could render infeasible the government's current *Mukasey* procedure for issuing NSL gags. Moreover, to embed disclosure into design could raise the cost and consequence of enforcing the gags. Communications built into infrastructure may have a greater chance of flying under the radar altogether. If courts find that NSL gags reach infrastructures of communication, then the gags' possible interference with innovation and industry could prove politically untenable.

CONCLUSION

This Essay suggests that a critical subject for future debate regarding the government's NSL gag authority will be extrajudicial solutions that telecommunications providers can adopt unilaterally. The Essay has shown that NSL recipients already are using transparency reports and warrant canaries to reframe the government's claims about its NSL gag authority. Moreover, and critically, in the long-term the Essay predicts that communications service providers are likely to adopt privacy-protective design capable of notifying users when their data suffer a security breach. It may be only a matter of time before disclosure by design undermines the efficacy of the government's NSL authority and renders obsolete the legal challenges to NSL gags that are currently underway in the courts.

---

106. United States v. O'Brien, 391 U.S. 367, 377 (1968).

107. *Id.* at 376-77.

Rebecca Wexler is a member of the Yale Law School J.D. Class of 2016 and a student fellow of the Information Society Project. *The author is grateful to Jack Balkin for his thoughtful comments on the* Mukasey *reciprocal notice procedure, and on constant and compelled speech; for helpful insights from Kurt Opsahl about the regulation of technological systems; and to Noah Messing, BJ Ard, Gautam Bhatia, and Kiel Brennan-Marquez for their generous feedback on earlier drafts. The author benefited greatly from participating in discussions at the Warrant Canary Workshop hosted by the Technology Law & Policy Clinic at NYU School of Law on November 3, 2014. She also thanks Bert Ma and the editors of the* Yale Law Journal *for their excellent editorial work.*

Preferred Citation: Rebecca Wexler, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, 124 YALE L.J. F. 158 (2014), http://www.yalelawjournal.org/forum/warrant-canaries-and-disclosure-by-design.