Harvard Journal of Law & Technology
Volume 28, Number 2 Spring 2015

THE NSA HAS NOT BEEN HERE: WARRANT CANARIES AS TOOLS FOR TRANSPARENCY IN THE WAKE OF THE SNOWDEN DISCLOSURES

*Naomi Gilens**

TABLE OF CONTENTS

I. INTRODUCTION

In 2005, Americans learned that the FBI employed the PATRIOT Act to coerce information from libraries regarding patrons' reading materials and Internet use. These demands were accompanied by nondisclosure orders threatening criminal sanctions should a library

* J.D., Harvard Law School, 2016. Thank you to Professor Jonathan Zittrain for advising the paper that inspired this Note, and to Alex Abdo, Brian Hauss, Brett Kaufman, Kurt Opsahl, Christopher Soghoian, and Patrick Toomey for their invaluable comments and insight on earlier drafts. In addition, I would like to thank the organizers and attendees of the Warrant Canary Workshop hosted by the Technology Law & Policy Clinic at the NYU School of Law on November 3, 2014. Finally, my deepest thanks to the wonderful team of editors at JOLT.

inform anyone of the surveillance.[1] In response to the controversial program, librarian Jessamyn West noted that although the library could not alert anyone when it received a request, it remained free to truthfully inform the public that it had *not* yet received one.[2] Seizing on this loophole, West designed a sign for libraries to hang that became the prototypical warrant canary: "The FBI has not been here (watch very closely for the removal of this sign)."[3] Like a canary in a coal mine, the presence of the sign would reassure the public, and its removal would signal to those watching closely that all was no longer well.[4]

Following West's lead, the file-transfer program rsync.net adopted a similar tactic in 2006 by posting weekly declarations on its website stating that it had not yet received any government orders for subscriber information.[5] Until the summer of 2013, West's signs and rsync.net's weekly updates remained isolated experiments — conceptually interesting, but of little practical import.

This all changed after June 2013, when Edward Snowden's disclosures confronted the public with detailed accounts of the National Security Agency's surveillance programs.[6] Those revelations

---

1. *See* Cory Doctorow, *How to Foil NSA Sabotage: Use a Dead Man's Switch*, THE GUARDIAN (Oct. 3, 2014, 9:01 AM EDT), http://www.theguardian.com/technology/2013/sep/09/nsa-sabotage-dead-mans-switch; Eric Lichtblau, *F.B.I., Using Patriot Act, Demands Library's Records*, N.Y. TIMES (Aug. 25, 2005), http://www.nytimes.com/2005/08/26/politics/26patriot.html?_r=0; Jessamyn West, *The FBI, and Whether They've Been Here or Not*, LIBRARIAN.NET (Sept. 9, 2013), http://www.librarian.net/stax/4182/the-fbi-and-whether-theyve-been-here-or-not/.

2. Doctorow, *supra* note 1.

3. *Id*. While West's sign is the first known implementation of the warrant canary concept, the idea originated earlier in cypherpunk circles (advocates for the use of cryptography in electronic communications in order to maintain privacy and anonymity). *See* Steve Schear *Re: ISP Utility to Cypherpunks?*, YAHOO GROUPS (Oct. 31, 2002, 11:44 AM), https://groups.yahoo.com/neo/groups/cypherpunks-lne-archive/conversations/topics/5869.

4. *See* Nadia Kayyali, *EFF Joins Coalition to Launch Canarywatch.org*, ELEC. FRONTIER FOUND. (Feb. 2, 2015), https://www.eff.org/deeplinks/2015/01/eff-joins-coalition-launch-canarywatchorg (The origin of the term warrant canary stems from the use of canaries in coalmines to warn the miners of the presence of carbon monoxide. For just as the canaries would become sick and die from the carbon monoxide poisoning, "the canaries on web pages 'die' when they are exposed to something toxic — like a secret FISA court order.").

5. *Rsync.net Warrant Canary*, RSYNC.NET (Feb. 16, 2015), http://www.rsync.net/resources/notices/canary.txt; *see also* John Kozubik, *The Warrant Canary in 2010 and Beyond,* KOZUBIK.COM (Aug. 6, 2010, 3:36 PM), http://blog.kozubik.com/john_kozubik/2010/08/the-warrant-canary-in-2010-and-beyond.html.

6. *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (June 6, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Glenn Greenwald, Ewen MacAskill, and Laura Poitras, *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, THE GUARDIAN (June 11, 2013), http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. See also the ACLU's searchable archive of documents disclosed both by the media and by the government since June 2013, *The NSA Archive*, AM. CIVIL LIBERTIES UNION, https://www.aclu.org/nsa-documents-search (last visited May 9, 2015).

launched a national debate about how the United States government interprets and applies its surveillance powers.[7] Information released about the government's collection of user data from communications providers also generated a strong public demand for companies to become more transparent with information regarding how user information is shared with the government.[8]

Prior to Snowden's unveilings, companies that published transparency reports generally released information only about law enforcement requests connected to criminal investigations, as the nondisclosure orders accompanying national security requests prohibited the companies from sharing information about these demands.[9] In response to increasing customer concern in the wake of the Snowden disclosures, companies fought for the right to publish information on these surveillance requests, or National Security Letters ("NSLs"). They ultimately received permission from the government to publish national security statistics, but only when aggregated with data on criminal investigation orders they had also received.[10]

---

7. *See, e.g.*, President Barack Obama, Remarks on Changes to the NSA at the Justice Department (Jan. 17, 2014), (transcript *available at* http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html) (condemning the "sensational way in which [the Snowden] disclosures have come out" but recognizing that as a result, "we have to make some important decisions about how to protect ourselves and sustain our leadership in the world while upholding the civil liberties and privacy protections our ideals and our Constitution require").

8. Technology companies have responded to the growing public pressure with vocal calls for reform. *See, e.g.*, *Global Government Surveillance Reform*, REFORM GOV'T SURVEILLANCE, https://www.reformgovernmentsurveillance.com (last visited May 9, 2015) (statement by AOL, Apple, Dropbox, Facebook, Google, LinkedIn, Microsoft, Twitter, and Yahoo calling for reforms to "[ensure] that government law enforcement and intelligence efforts are rule-bound, narrowly tailored, transparent, and subject to oversight").

9. *See, e.g.*, Carrie Cordero, *An Update on the Status of FISA Transparency Reporting*, LAWFARE: HARD NAT'L SEC. CHOICES (Apr. 23, 2014, 1:21 PM), http://www.lawfareblog.com/2014/04/an-update-on-the-status-of-fisa-transparency-reporting/. A number of statutes authorize non-disclosure orders accompanying national security requests made under certain circumstances. *E.g.* 18 U.S.C. § 2705(b) (2012) (prohibiting companies that receive a surveillance order under the Electronic Communications and Privacy Act from "notify[ing] any other person of the existence of the warrant, subpoena, or court order"); 50 U.S.C. § 1861(d) (2012) (prohibiting companies that receive an order under Section 215 of the Patriot Act from "disclos[ing] to any other person," with specific exceptions, "that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to [the Section 215 order]").

10. *See* Ted Ullyot, *Facebook Releases Data, Including All National Security Requests*, FACEBOOK NEWSROOM (June 14, 2013), http://newsroom.fb.com/news/2013/06/facebook-releases-data-including-all-national-security-requests/ (announcing that the government had granted Facebook permission to "include in a transparency report all U.S. national security-related requests (including FISA as well as NSLs) — which until now, no company has been permitted to do," but noting that "[a]s of today, the government will only authorize us to communicate about these numbers in aggregate, and as a range").

Given this concession's limited scope, Google, Facebook, Yahoo, and Microsoft sought permission to disclose more detailed information about national security requests received, such as the aggregate number of user accounts affected and the statutory authority for these orders.[11] When the government refused, the companies filed a lawsuit challenging the prohibition.[12] A settlement agreement reached in January 2014 relaxed the nondisclosure restrictions,[13] but companies' freedom to share information with the public remains cabined by stringent limitations.[14] Under the terms of the settlement, companies are allowed to share the number of NSLs and Foreign Intelligence Surveillance Act ("FISA") orders they receive and the number of user accounts implicated, but only in bands of one thousand (or increments of 250 if the surveillance request categories are aggregated).[15] Furthermore, the settlement imposes a two-year delay on the disclosure of data relating to the first order that a company receives for information from a product or service not previously the subject of an order. The settlement also requires companies to wait six months before including a new request in their relevant statistics,[16] and permits companies to report on NSLs and FISA orders only once every six months.[17]

Technology companies and civil liberties advocates have widely criticized the settlement for not going far enough in curtailing government secrecy. Twitter, for example, commented that although

---

11. *See* Claire Cain Miller, *Tech Companies Escalate Pressure on Government To Publish National Security Request Data*, N.Y. TIMES: BITS BLOG (Sept. 9, 2013, 4:46 PM), http://bits.blogs.nytimes.com/2013/09/09/tech-companies-escalate-pressure-on-government-to-publish-national-security-request-data/; Hayley Tsukayama, *Google, Facebook Ask FISA for Permission To Release Information on Government Requests*, WASH. POST (Sept. 9, 2013), http://www.washingtonpost.com/business/technology/google-facebook-ask-fisa-for-permission-to-release-on-infomation-on-government-requests/2013/09/09/5c365a3a-195d-11e3-a628-7e6dde8f889d_story.html.

12. Court filings are available at *Public Filing — U.S. Foreign Intelligence Surveillance Court*, FOREIGN INTELLIGENCE SURVEILLANCE COURT ("FISC") (last visited May 9, 2015), http://www.fisc.uscourts.gov/public-filings; *see also* Miller, *supra* note 11; Tsukayama, *supra* note 11.

13. Letter from James M. Cole, Deputy Attorney Gen., to Colin Stretch, Vice President and Gen. Counsel, Facebook, et al. (Jan. 27, 2014), *available at* http://www.justice.gov/iso/opa/resources/366201412716018407143.pdf.

14. Craig Timberg and Adam Goldman, *U.S. To Allow Companies To Disclose More Details on Government Requests for Data*, WASH. POST (Jan. 27, 2014), http://www.washingtonpost.com/business/technology/us-to-allow-companies-to-disclose-more-details-on-government-requests-for-data/2014/01/27/3cc96226-8796-11e3-a5bd-844629433ba3_story.html; *see also* Mike Masnick, *Feds Reach Settlement With Internet Companies Allowing Them To Report Not Nearly Enough Details on Surveillance Efforts*, TECHDIRT (Jan. 27, 2014, 11:55 PM), http://www.techdirt.com/articles/20140127/17253826014/feds-reach-settlement-with-internet-companies-allowing-them-to-report-not-nearly-enough-details-surveillance-efforts.shtml.

15. Letter from James M. Cole, *supra* note 13.

16. *Id.*

17. *Id.*

the settlement "is a step in the right direction," the "ranges do not provide meaningful or sufficient transparency for the public."[18] Making the same point more vividly, Kevin Bankston, policy director of the New America Foundation's Open Technology Initiative, observed, "[a]sking the public and policymakers to try to judge the appropriateness of the government's surveillance practices based on a single, combined, rounded number is like asking a doctor to diagnose a patient's shadow: only the grossest and most obvious problem, if even that, will be ever be [sic] evident."[19]

In the face of continuing pressure on companies to disclose national security requests, Internet companies have increasingly adopted warrant canaries to inform the public about particular types of national security orders they receive.[20] Unsurprisingly, companies that provide encryption services and whose users prioritize information security have been early adopters of the tactic. For example, Silent Circle, a company that provides mobile encryption services for voice and text,[21] has taken a self-proclaimed "page from rsync.net's playbook" by publishing weekly canaries.[22] Other data security companies that have implemented regular canaries include Virtru,[23]

18. Jeremy Kessel, *Fighting for More #transparency*, TWITTER BLOG (Feb. 6, 2014, 2:58 PM), https://blog.twitter.com/2014/fighting-for-more-transparency.

19. Kevin Bankston, *quoted in* Tony Romm, *Obama Administration To Allow Facebook, Google, Others More NSA Transparency*, POLITICO (Jan. 27, 2014, 10:04 PM EST), http://www.politico.com/story/2014/01/barack-obama-administration-nsa-national-security-agency-tech-technology-transparency-eric-holder-james-clapper-102677.html.

20. Warrant canaries additionally function as a form of precommitment. Not only do they communicate to the public that the company has not received a national security order, but they also obligate the company to making any future orders known, thereby giving weight to what may otherwise be seen as rhetorical commitments to user privacy. *See* John A. Robertson, *"Paying the Alligator:" Precommitment in Law, Bioethics, and Constitutions*, 81 TEX. L. REV. 1729, 1731 (2003) (describing precommitment generally and noting that "what is distinctive about precommitment behavior is the intention to limit future options in some way for a present or future payoff").

21. *Our Story*, SILENT CIRCLE, https://silentcircle.com/ourstory (last visited May 9, 2015).

22. Lou Ruppert, *Our Transparency Report*, SILENT CIRCLE BLOG (Apr. 2, 2014), https://blog.silentcircle.com/tag/transparency-report; Silent Circle's Warrant Canary, SILENT CIRCLE (Feb. 19, 2015), https://canary.silentcircle.com ("[N]o warrants have been served, nor have any searches or seizures taken place . . . Special note should be taken if these messages ever cease being updated, or are removed from this page.").

23. *Virtru Transparency Report: December 2014*, VIRTRU (Dec. 2014), http://blog.virtru.com/virtru-reports/transparency-report-march-2014/.

Lookout,[24] and Wickr,[25] which provide secure email,[26] mobile cybersecurity,[27] and secure messaging[28] respectively.

Companies outside the information security sector have also adopted warrant canaries. Tumblr, for example, began incorporating canaries into its transparency reports in February 2013.[29] Pinterest followed soon after,[30] and reddit recently joined the trend, declaring that the company has not yet received an NSL or FISA order.[31] Furthermore, Twitter has filed for a declaratory judgment establishing its right to issue such a declaration, laying the groundwork to publish its own canary statement in the future.[32]

No company has yet removed a canary to indicate that the company has received a national security request accompanied by a nondisclosure order.[33] It is currently unclear whether the government,

---

24. *2013 Transparency Report: Government Requests*, LOOKOUT, https://www.lookout.com/transparency/report-2013 (last visited May 9, 2015).

25. Jennifer DeTrani, *Wickr Transparency Report*, WICKR 1 (Nov. 24, 2014), https://www.wickr.com/wp-content/uploads/2014/11/Transparency-Report-11.24.14.pdf.

26. *How It Works*, VIRTRU, https://www.virtru.com/how-it-works (last visited May 9, 2015).

27. LOOKOUT, https://www.lookout.com (last visited May 9, 2015).

28. *How Wickr Works*, WICKR, https://www.wickr.com/how-wickr-works/ (last visited May 9, 2015).

29. *Tumblr's Transparency Report 2013*, TUMBLR, http://transparency.tumblr.com/ (last visited May 9, 2015) ("As of the date of publication of this report, we have never received a National Security Letter, FISA order, or any other classified request for user information.").

30. *Quarterly Transparency Report Archive*, PINTEREST, https://help.pinterest.com/en/articles/transparency-report-archive (last visited May 9, 2015) (explaining that "National security request means any national security letters and orders issued under the Foreign Intelligence Surveillance Act," and listing the number of National Security requests as "0").

31. *Reddit Transparency Report, 2014*, REDDIT (Jan. 29, 2015), https://www.reddit.com/wiki/transparency/2014 ("As 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.").

32. *See* 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/.

33. Apple published a canary-like statement in its 2013 transparency report and subsequently reworded it. This prompted speculation that it had "removed" its canary. *Compare Report on Government Information Requests*, APPLE (Nov. 5, 2013), https://www.apple.com/pr/pdf/131105reportongovinforequests3.pdf ("Apple has never received an order under Section 215 of the USA Patriot Act") *with Report on Government Information Requests*, APPLE (Jan. 1–June 30, 2014), https://www.apple.com/privacy/docs/government-information-requests-20140630.pdf (replacing the canary with a statement that "Apple has not received any orders for bulk data"). Rather than signaling that Apple had in fact received a Section 215 request, a likely explanation is that Apple capitulated to government pressure to change its wording, such that it would not be considered a canary. *See* Cyrus Farivar, *No, Apple Probably Didn't Get New Secret Gov't Orders to Hand Over Data*, ARS TECHNICA (Sept. 18, 2014, 4:35 PM EDT), http://arstechnica.com/tech-policy/2014/09/no-apple-probably-didnt-get-new-secret-govt-orders-to-hand-over-data (quoting Mark Rumold, an attorney at the Electronic Frontier Foundation, as saying "[r]eporting that band does not mean that they received a Section 215 order, it just means that they changed their practice to conform with the [Department of Justice]'s guidance"); Mike Masnick, *Did Apple Keep or Remove Its Warrant Canary Concerning PATRIOT Act Requests?*, TECHDIRT (Sept. 18,

on serving such a request, could lawfully prevent a company from removing its canary. However, as a wide range of Internet companies rapidly increase their use of canaries, the legality of these declarations will become a critical concern to the entire industry, and companies thus will likely litigate this legality in the near future.

This Note seeks to establish a framework for thinking about the unanswered constitutional and practical questions that canaries raise. Part II examines the different, and at times conflicting, purposes that canaries can serve, explores how these objectives can be effected through various types of canaries, examines case studies of each, and contends that the most useful canaries are those that are broadly conceived to inform public debate. Part III argues that an order compelling a company to publish a false canary must, at a minimum, be subject to the strictest level of judicial scrutiny. Part IV advocates for a company to adopt a canary for the purpose of litigating its lawfulness, in order to establish that canaries are legitimate tools to promote transparency.

II. IMPLEMENTING WARRANT CANARIES: CONFLICTING PURPOSES, BEST PRACTICES

Warrant canaries are not inherently valuable; companies must carefully craft them to communicate important information to customers and to the public. To begin with, it is useful to clarify what canaries can and cannot do. Once a company chooses to publish a canary, it operates on a binary basis, providing observers with only a yes-or-no answer to the question of whether the government has requested a particular type of information from the company. A canary may specify whether a business has received surveillance orders under specific statutory authorities (e.g., "We have never received a National Security Letter or FISA order"), or it may indicate whether discrete products or services have been targeted ("We have never received a request for email content.").

Ideally, when a company metaphorically kills a canary — that is, ceases to publish it — the dead canary will indicate to the public that something is amiss. Even if observers do not know exactly what type of national security request a company may have received, they will be on notice of government surveillance.

For a canary to effectively convey this message, a business must ensure that it regularly publishes its warrant canary "in the same

---

2014, 2:35 PM), https://www.techdirt.com/articles/20140918/13363728563/did-apple-keep-remove-its-warrant-canary-concerning-patriot-act-requests.shtml (explaining that Apple may have been "pressured from the DOJ not to use the original warrant canary language").

place . . . us[ing] the same language."[34] If the public has to speculate as to the original intent of the company's statement and meaning of its subsequent disappearance, the canary will not be an effective method of communication, and will stimulate mere suspicion of government intervention. For instance, in 2014 Apple rephrased a canary-like statement in its transparency report. While the original statement read, "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;"[35] Apple's subsequent transparency report replaced this statement with an avowal that "Apple has not received any orders for bulk data" and moved this disclosure to a new section of the report as well.[36] This change prompted widespread speculation that Apple had received a Section 215 order. Yet, because Apple had not clearly indicated that it intended the original statement to act as a warrant canary, it was, and still is, not clear if the alteration of the transparency report's text was a signal to the public that Apple actually received a national security order.[37]

While the most basic goal of a canary is to convey such a message, there are three broad purposes for which a company may adopt a canary. First, what I term "performative canaries" are exercises in public relations meant to show that a company cares about user privacy; second, "granular canaries" provide useful notification to individual users when the government compromises the security of their personal data; and third, "public policy canaries" inform the community about how the government interprets and exercises its surveillance powers. Although canaries can advance more than one of these goals simultaneously, this Part discusses the three types of canaries discretely in order to assess their value and propose models that best fulfill their respective purposes.

A. Performative Canaries

For companies struggling to convince an increasingly wary public that they can keep customers' information out of the hands of the U.S. government,[38] a warrant canary can provide a relatively low-cost way

34. *See* Christopher Soghoian, TWITTER (Sept. 18, 2014, 10:57 AM), https://twitter.com/csoghoian/status/512661646171316224 ("There is a lesson to be learned here: once you post a warrant canary, it needs to stay in the same place and use the same language.").

35. *See Report on Government Information Requests*, APPLE (Nov. 5, 2013), *supra* note 33.

36. *See Report on Government Information Requests*, APPLE (Jan. 1–June 30, 2014), *supra* note 33.

37. *See* Farivar, *supra* note 33; *see also* Masnick, *supra* note 33.

38. *See, e.g.*, Amended Motion for Declaratory Judgment at 5, *In re* Amended Motion for Declaratory Judgment of Google Inc.'s First Amendment Right To Publish Information About FISA Orders (FISA Ct. 2013) (No. 13-03) (asserting that "Google's reputation and

of emphasizing a commitment to transparency. Companies adopting canaries for solely public relations purposes are likely to comply with a government order to continue publishing the canary — even after being served with a national security request — in order to preserve the public conception of their brand. Therefore, rather than drafting a canary that will effectively communicate useful information, these companies may adopt canaries designed to convey as little as possible. For example, the company may state that it has never received a national security order under a specific statutory authority that cannot apply to the corporation. Thus, the canary will act as a public relations tool that creates a façade of security — the company will appear to promote transparency, while avoiding a situation in which the company must either fight a government surveillance request, or lie to the public.

The language of Apple's original canary statement provides a useful case study to illustrate some of the issues performative canaries raise, although it is not solely performative and Apple has since reworded it.[39] In 2013, the company received much praise for publishing a statement declaring, "Apple has never received an order under Section 215 of the USA Patriot Act."[40] As far as publicly available information indicates, the government has relied upon Section 215 to gather information from telecommunications providers such as Verizon and AT&T, not from product design and manufacturing companies like Apple.[41] The fact that Apple, a company with undoubtedly huge stores of data with almost 350 million iCloud customers,[42] presumably has never received an order

business has been and continues to be harmed by . . . reports in the media, and Google's users are concerned by the allegations"). For discussions of the actual costs of Snowden's disclosures to U.S. companies, *see* Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), http://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html; Daniel Castro, *How Much Will PRISM Cost the U.S. Cloud Computing Industry?*, INFO. TECH. & INNOVATION FOUND. 3–4 (Aug. 2013), http://www2.itif.org/2013-cloud-computing-costs.pdf.

39. *See supra* notes 35–38 and accompanying text.

40. *See, e.g.*, Cyrus Farivar, *Apple Takes Strong Privacy Stance in New Report, Publishes Rare "Warrant Canary,"* ARS TECHNICA (Nov. 5, 2013, 5:52 PM EST), http://arstechnica.com/tech-policy/2013/11/apple-takes-strong-privacy-stance-in-new-report-publishes-rare-warrant-canary/; 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.

41. *See, e.g.*, Scott F. Mann, *Fact Sheet: Section 215 of the USA PATRIOT Act*, CTR. FOR STRATEGIC & INT'L STUDIES (Feb. 27, 2014), http://csis.org/publication/fact-sheet-section-215-usa-patriot-act ("This provision of the PATRIOT Act has been interpreted to permit the bulk collection of 'telephony metadata' or the mass collection of basic call-log information, from telecommunications companies.").

42. Brief for Apple Inc. as Amicus Curiae Supporting Providers' Motions for Declaratory Judgment at 12, *In re* Motions for Declaratory Judgment To Disclose Aggregate Data Regarding FISA Orders and Directives (FISA Ct. 2013) (Nos. Misc. 13-03, 13-04, 13-05,

under Section 215 suggests that the government has not interpreted the statute as giving it authorization to do so.[43] To the extent that the government has not interpreted Section 215 as an appropriate authority by which to retrieve records from Apple, the canary communicates little information of value. Used as such, canaries serve to protect a company's brand, but do little to promote meaningful transparency.

However, while I draw on Apple's transparency statement to illustrate the mechanisms of a performative canary, it was not necessarily entirely performative. A purely performative canary would consist of a statement that a company has never received an order under an authority that *could not* apply to it.[44] In this case, nothing in the text of Section 215 affirmatively precludes the government from directing it to companies such as Apple; rather, it seems that the government has not yet done so as a matter of praxis.[45] Although there is no reason to think that the government will change its practice and begin applying Section 215 to companies such as Apple in the future, it still remains a possibility. Therefore, it is conceivable that rather than receiving a national security order, Apple succumbed to government pressure to change the wording of its transparency report, such that the removal of the Section 215 reference made the statement a performative canary that would not require removal upon the future receipt of a national security order.[46]

B. Granular Canaries

A granular canary provides individual users with updates about the security of their personal information. At one extreme, a company adopting such a canary theoretically could send daily notifications to individual users, informing each that the company had not shared his

13-06, and 13-07) [hereinafter Apple FISC Brief], *available at* http://www.uscourts.gov/uscourts/courts/fisc/Misc-13-03-04-05-06-07-131105.pdf.

43. *Report on Government Information Requests*, APPLE (Nov. 5, 2013), *supra* note 33, at 5; *see also* Masnick, *supra* note 33. This assumes that Apple changed the phrasing of its canary as a result of government pressure — not because it had received an NSL.

44. For instance, if a restaurant review site posted a canary stating that it had not received a government request under 31 U.S.C. § 5311 (2012), this would be meaningless, as § 5311 requests financial information from financial institutions, and such a business would not fit the definition of a financial institution under 31 U.S.C. § 5312 (2012).

45. The text of Section 215 plainly allows for applications beyond telecommunications companies. 50 U.S.C. § 1861 (2012) (specifying that Section 215 can authorize orders for "library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records"); *see also* Harley Geiger, *Issue Brief: Bulk Collection of Records Under Section 215 of the PATRIOT Act*, CTR. FOR DEMOCRACY & TECH. (Feb. 10, 2014), https://cdt.org/issue-brief-bulk-collection-of-records-under-section-215-of-the-patriot-act/ ("Section 215 is broadly worded, covering all business records on Americans.").

46. *See* Farivar, *supra* note 33.

or her data. However, no company has taken the concept this far, nor is any company likely to do so. Such a practice would alert users who become targets of investigations and cause them to withdraw their business from the company, thereby jeopardizing legitimate inquiries into individuals who pose actual threats to national security.

Instead, this approach to canaries is most effective when operating at a level of granularity sufficient to alert users that a service is not as secure as they would otherwise assume, or that there is a possibility that the government has demanded their data. Instead of acting on a personal level, the canaries may provide discrete notifications about certain types of data retained by the company. For example, when encrypted email provider Lavabit announced that it would suspend operations rather than "become complicit in crimes against the American people,"[47] concern arose over the government's compulsion of companies to turn over encryption keys.[48] As a result, some encryption providers adopted canaries specifically declaring that they have never received nor complied with a request for encryption keys.[49] Killing one of these canaries would provide users with immediate notice that their encrypted communications may no longer be secure. Users then could act on that information to close their accounts and move their information to another provider.

Consumers value granular canaries because they provide useful information; however, these canaries have greater legal risk. As discussed below, all gag orders are subject to a First Amendment balancing test to ensure the restriction on speech is justified by a compelling government interest.[50] Granular canaries have the greatest potential to compromise legitimate national security investigations because they could alert the target of an investigation of the government's search, prompting that individual to cease use of the targeted service, and to attempt to erase his or her information

47. Public Letter from Ladar Levison, LAVABIT (Aug. 9, 2013), http://lavabit.com/.

48. For example, Silent Circle responded to the Lavabit shutdown by preemptively ceasing operations of its own email encryption service, explaining that although it had not yet received a national security demand for users' keys, it could see "the writing [on] the wall." Jon Callas, *To Our Customers*, SILENT CIRCLE BLOG (Aug. 9, 2013), https://blog.silentcircle.com/to-our-customers/; *see also* Joe Mullin, *Lavabit Founder, Under Gag Order, Speaks out About Shutdown Decision*, ARS TECHNICA (Aug. 13, 2013, 10:35 PM EDT), http://arstechnica.com/tech-policy/2013/08/lavabit-founder-under-gag-order-speaks-out-about-shut-down-decision/.

49. Among other canaries, for instance, Cloudflare has published a declaration that the company "has never turned over [its] SSL keys or [its] customers' SSL keys to anyone." *Cloudflare Transparency Report for the First Half of 2014*, CLOUDFLARE, http://www.cloudflare.com/transparency (last visited May 9, 2015). Virtru's canary is even more specific, stating that the company has never provided the government with user encryption keys under a dozen different surveillance authorities. *Virtru Transparency Report*, VIRTRU BLOG (Dec. 2014), http://blog.virtru.com/ transparency-report-december-2014/.

50. *See infra* Part III.A.1.

therefrom. Clearly, the government has a strong interest in preventing this outcome. Thus, courts are less likely to find that these canaries are legal and are more apt to uphold a gag order prohibiting their removal.[51] Ultimately, as will be discussed below, no matter how informative the canary is in theory, it is of no practical use if the government can compel a company to publish a fraudulent canary after serving that company with a surveillance request.

C. Public Policy Canaries

Public policy canaries provide little information of immediate use to customers, but paint a larger picture of how the government is currently interpreting and using its surveillance powers. For example, several large companies, including Tumblr, Pinterest, and reddit, have adopted canaries stating that they have not received an NSL or FISA order.[52] Such canaries fall outside the granular model because they offer little information of practical use to individual consumers. Given Tumblr's large customer base, for example, it is unlikely that a significant number of people would stop using the product upon learning that the company had received a FISA order.[53]

Although public policy canaries provide little practical notice to users about the security of their personal data, they differ from performative canaries because they can provide the public with important information about how the government is interpreting and applying its surveillance authorities. Therefore, while a performative canary will be vague to avoid its removal upon receipt of a NSL, companies draft a public policy canary to necessitate its deletion in such a situation — thereby informing the community that the government has exercised its surveillance powers. For instance, if Tumblr kills its canary, it will alert the public that the government has expanded its application of its Section 215 powers to companies beyond telecommunications providers. Without Tumblr's affirmative act, the public would be unaware of this extension of the government's surveillance authority. This awareness may prompt reporters to investigate, civil liberties groups to file Freedom of

---

51. *See infra* Part III.A.1.

52. *See, e.g.*, *Tumblr's Transparency Report*, *supra* note 29, at 12; *Quarterly Transparency Report Archive*, PINTEREST, *supra* note 30; *Reddit Transparency Report*, *supra* note 31.

53. Apple itself has argued that "[i]t is . . . simply not possible that disclosure of the aggregate figure [of national security requests received] could compromise an investigation or reveal to a user that the user has been targeted. . . ." Apple FISC Brief, *supra* note 42 at 12. The logic applies to canaries as well, especially given that canaries convey only limited information. Operating as they do on a yes-or-no binary, canaries cannot disclose aggregate numbers of orders; rather, they merely disclose the fact that at least one order has been issued.

Information Act requests, or citizens to call on their representatives to clarify the new development.[54]

By providing information to the public to support debate on government surveillance policies, these canaries are valuable resources to the community. Moreover, because they do not aid individuals in avoiding government surveillance, these canaries are largely insulated from the usefulness-lawfulness tradeoff: while they can help inform the public about government surveillance practices, thereby contributing to advocacy efforts and policy debates, they avoid giving individual customers reason to leave companies served with national security orders. Because they are less likely than granular canaries to actually disrupt law enforcement investigations, public policy canaries are more likely to survive a challenge in court. For this reason, companies searching for meaningful practices to promote transparency and encourage a sustained, informed public debate about government surveillance, are well-advised to adopt public policy warrant canaries.

III. THE FIRST AMENDMENT PROBLEM: CAN THE GOVERNMENT COMPEL COMPANIES TO LIE?

As canaries have not yet been tested in court, it is currently unclear whether and to what extent they are actually lawful. The First Amendment protects a company's right to truthfully tell the public that it has received zero national security orders because a restriction on such statements would be an unconstitutional prior restraint on speech. As such, the government claims that it does not seek to prevent companies that have "received no national security legal process at all" from saying so, but rather only to limit the speech of those companies "who have received such process."[55] Therefore, the determination of a warrant canary's legality depends upon whether the government may compel the company to continue publishing its canary, even after receiving a national security request. In other words, can the government force a company to lie to shareholders, customers, and the general public for security reasons? While courts

54. Although Apple's current canary may alert observers that government surveillance practices have changed, the company is so large that observers will not know in what manner they have expanded without further investigation. A more valuable public policy canary might include discrete statements for different services — for example, declaring that the company has never received a Section 215 order for customer data from iMessage, Apple Mail, or FaceTime. Doing so would also incorporate a granular element into the policy canary by providing users with practical information about the platforms that might be subject to government surveillance.

55. Reply Memorandum in Support of Defendants' Partial Motion to Dismiss at 2, Twitter v. Eric Holder, et al., No. 14-cv-4480 (N.D. Cal. Mar. 31, 2015).

have not yet resolved this critical question, the First Amendment requires courts to review compelled false speech — including the coerced production of a false canary — under the most exacting measure of strict scrutiny.

A. The Case Against Canaries

The claim that canaries are unlawful asserts that nondisclosure orders protect compelling national security interests, and the First Amendment does not protect speech that willfully exploits a legal loophole to frustrate those concerns. While the government does not currently prohibit companies from truthfully stating that they have never received a national security order, the removal of such a statement would alert the public of the company's receipt of a surveillance request. As such, courts may view the killing of a canary as an unlawful violation of a nondisclosure order.

1. Government Interest

First, the government has a clear and compelling interest in being able to enforce nondisclosure orders related to national security investigations.[56] Because such orders are subject to strict scrutiny when challenged in court,[57] any order that a canary frustrates will be one that the government must have already narrowly tailored to protect a compelling government interest in national security. As the government has argued, sharing information about these requests could "risk significant harm to national security by revealing the nature and scope of the Government's intelligence collection on a company-by-company basis throughout the country."[58]

The government security interests at issue in nondisclosure orders are exactly those implicated by warrant canaries, given that canaries are a ruse specifically intended to foil these orders. As such, whether the government is enforcing a gag order or compelling a company to publish a false canary, an advocate arguing that canaries are unlawful

---

56. *See* Haig v. Agee, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation.") (internal quotation marks omitted); Snepp v. United States, 444 U.S. 507, 509, n.3 (1980) ("The Government has a compelling interest in protecting . . . the secrecy of information important to our national security.").

57. *See, e.g.*, John Doe, Inc. v. Mukasey, 549 F.3d 861, 878 (2d Cir. 2008).

58. Response of the United States to Motions for Declaratory Judgments by Google, Inc., Microsoft Corporation, Yahoo! Inc., Facebook, Inc., and LinkedIn Corporation at 16, *In re* Motions for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives (FISA Ct. 2013) (Nos. Misc. 13-03, 13-04, 13-05, 13-06, and 13-07), *available at* http://www.uscourts.gov/uscourts/courts/fisc/motion-declaratory-judgement-131002.pdf.

will suggest that the interests at issue and the strict scrutiny calculus remain the same.

Courts generally treat an act that has the intention and effect of conveying a message as an expression of that message and, thus, as speech protected by the First Amendment.[59] Companies usually adopt warrant canaries with the intention of communicating the existence of national security requests when the government sends these orders, as observers who note the dead canary will understand the removal of the canary as the company's receipt of such a request. Therefore, by killing a canary, a company deliberately notifies the public that it has received an NSL or FISA order. Thus, canaries arguably violate nondisclosure orders that prohibit businesses from notifying any person about these requests.

2. Self-Inflicted Sanctions

Furthermore, the government may argue that First Amendment protection does not extend to warrant canaries because the only reason that the government would compel a company to lie is if that corporation willfully took affirmative steps to frustrate an impending nondisclosure order — in essence, the warrant canary concept is too clever by half. Although there may be a real First Amendment distinction between ordinary compelled speech and compelled false speech, here the government has not required any party to engage in false speech. Instead, companies have taken it upon themselves to exploit a legal loophole in order to communicate information that would otherwise be illegal. The company is essentially manufacturing a First Amendment harm in order to avoid impending nondisclosure obligations. The First Amendment is intended to safeguard our "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open,"[60] not to protect companies that use clever tactics to evade constitutional restrictions on speech.

B. The Case for Canaries

The argument supporting warrant canaries relies on two assumptions. First, the government cannot prohibit a company from truthfully telling the public that it has not received a national security

59. *Cf.* Texas v. Johnson, 491 U.S. 397, 404 (1989) ("In deciding whether particular conduct possesses sufficient communicative elements to bring the First Amendment into play, we have asked whether an intent to convey a particularized message was present, and whether the likelihood was great that the message would be understood by those who viewed it.") (internal quotation marks omitted).

60. New York Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

order. Second, compelling an affirmative lie is categorically different than requiring silence, and therefore subject to broader First Amendment protection. While the first is uncontested, the following will examine the second assumption — whether the government can compel false speech.

1. Content-Based Speech Regulations

For a warrant canary to be effective, the First Amendment must protect a private party from being compelled by the government to lie. Forcing a company to publish a fraudulent canary after receiving a national security order is a content-based speech regulation[61] — which is subject to the greatest protections of the First Amendment — because the speech discusses political affairs. As such, the compelled speech is subject to strict scrutiny, just as the original gag order.[62] However, forcing a company to publish a fraudulent canary is distinguishable from, and more suspect than, the original gag order for two reasons: it affirmatively compels speech, rather than merely prohibiting it, and the speech in question is a lie. Not only are the First Amendment intrusions greater in the warrant canary context than in the original gag order, but also the government interest in burdening the speech is smaller, given that a warrant canary only can communicate limited information.[63]

At a minimum, compelling a company to publish false canaries must be subject to strict scrutiny review because it is a content-based speech regulation.[64] Like nondisclosure orders, a request prohibiting a company from killing its canary restricts that company's freedom to speak or not to speak about NSLs and FISA orders.[65] To survive strict scrutiny, such content-based restrictions must be "narrowly tailored to promote a compelling Government interest."[66] The narrow tailoring requirement functions as a "means-ends" test whereby courts will strike down a speech regulation if the "means" are too broad or

61. Content-based speech regulations are those that "proscrib[e] speech . . . or even expressive conduct . . . because of disapproval of the ideas expressed." R. A. V. v. St. Paul, 505 U.S. 377, 382 (1992).

62. *See In re* Nat'l Sec. Letter, 930 F. Supp. 2d 1064, 1075 (N.D. Cal. 2013) ("[A]s content-based restrictions on speech, the NSL nondisclosure provisions must be narrowly tailored to serve a compelling governmental interest.").

63. This assumes that companies do not use granular canaries.

64. Content-based regulations are subject to strict scrutiny because they "are especially likely to be improper attempts to value some forms of speech over others, or are particularly susceptible to being used by the government to distort public debate." City of Ladue v. Gilleo, 512 U.S. 43, 60 (1994) (O'Connor, J., concurring).

65. United States v. Stevens, 559 U.S. 460, 468 (2010) (emphasizing that content-based restrictions are "presumptively invalid, and the Government bears the burden to rebut that presumption") (internal quotation marks omitted).

66. United States v. Playboy Entm't, 529 U.S. 803, 813 (2000).

otherwise burdensome to accomplish the "ends."[67] Although national security is clearly a compelling government interest, related speech restrictions are nonetheless subject to narrow tailoring,[68] and courts have not shied away from striking down nondisclosure orders that fail this requirement.[69]

2. Public Issues

In addition, nondisclosure orders demand strict scrutiny because they restrict speech about government surveillance, an issue of great public importance. The Supreme Court has emphasized that "there is practically universal agreement that a major purpose of [the First] Amendment [is] to protect the free discussion of governmental affairs."[70] Indeed, the Court has held that "speech concerning public affairs is more than self-expression; it is the essence of self-government."[71] Internet companies have emphatically asserted a desire to participate in the public debate over surveillance in America today.[72] Debate on critical "public issues occupies the highest rung of the hierarchy of First Amendment values, and is entitled to special protection."[73] Warrant canaries, like disclosure notices, inform the debate on the government's surveillance practices and national

67. *See, e.g.*, Sable Commc'ns of C.A. v. F.C.C., 492 U.S. 115, 126 (1989) (holding that the government may "regulate the content of constitutionally protected speech in order to promote a compelling interest if it chooses the least restrictive means to further the articulated interest"); *see generally* Eugene Volokh, *Freedom of Speech, Permissible Tailoring and Transcending Strict Scrutiny*, 144 U. Pa. L. Rev. 2417 (1999).

68. *See* John Doe, Inc. v. Mukasey, 549 F.3d 861, 878 (2d Cir. 2008) (noting that the government had "conceded that strict scrutiny is the applicable standard" of review for NSLs).

69. *See id.* at 883 (holding that nondisclosure orders accompanying NSLs did not survive strict scrutiny because they were not narrowly tailored).

70. Mills v. Alabama, 384 U.S. 214, 218 (1966).

71. Connick v. Myers, 461 U.S. 138, 145 (1983) (citation omitted).

72. *See, e.g.*, Jeremy Kessel, *Fighting for More #transparency*, TWITTER BLOG (Feb. 6, 2014, 2:58 PM), https://blog.twitter.com/2014/fighting-for-more-transparency ("We think that the government's restriction on our speech . . . violates our First Amendment right to free expression and open discussion of government affairs,"); Google's Amended Motion for Declaratory Judgment at 5, *In re* Amended Motion for Declaratory Judgment of Google Inc,'s First Amendment Right To Publish Information About FISA Orders (FISA Ct. 2013) (No. Misc. 13-03), *available at* http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-03%20Motion-1.pdf (arguing that matters of government surveillance "are matters of significant weight and importance, and transparency is critical to advancing public debate in a thoughtful and democratic manner"); Facebook's Motion for Declaratory Judgment at 7, *In re* Motion for Declaratory Judgment To Disclose Aggregate Data Regarding FISA Orders and Directives (FISA Ct. 2013) (No. Misc. 13-06), *available at* http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-06%20Motion-3.pdf (explaining that "Facebook seeks to contribute to [the] important debate" occurring over the government's use of its surveillance powers).

73. *See* Snyder v. Phelps, 562 U.S. ___, 131 S. Ct. 1207, 1211 (2011) (citation omitted).

security policies. As such, they should be entitled to the full extent of First Amendment protections.

3. Compelled Silence

Published canaries also are subject to at least the same level of scrutiny as nondisclosure orders, because compelled speech is subject to no lesser First Amendment protection than compelled silence.[74] The Court has emphasized that an "important manifestation of the principle of free speech is that one who chooses to speak may also decide 'what not to say.'"[75] This principle often arises in clashes between the First Amendment and public accommodations law. For example, in the landmark case *Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*, an Irish LGBT group excluded from a St. Patrick's Day parade sued the parade's private organizers, claiming that their exclusion violated a state law prohibiting discrimination on the basis of sexual orientation in places of public accommodation.[76] A unanimous Supreme Court held that the state could not use its public accommodations law to compel the parade organizers to express a message against their will.[77] This was particularly relevant because the parade organizers disagreed with the view that the state had attempted to compel them to express.[78] As the Supreme Court emphasized, forcing the parade organizers to include the LGBT group would have been to "compel affirmance of a belief with which the speaker disagrees."[79] Doing so would have violated the Constitution because the First Amendment "protects the right of individuals to hold a point of view different from the majority and to refuse to foster . . . an idea they find morally objectionable."[80] Indeed, the Supreme Court has expanded this principle beyond affirmances of belief, including statements of fact within its purview: the government "may not compel affirmance of a belief with which the speaker disagrees," including not only "expressions of value, opinion, or endorsement," but also "statements of fact."[81] As such, courts should

74. *See* Riley v. Nat'l Fed'n of the Blind of N.C., Inc., 487 U.S. 781, 797 (1988) (holding that the First Amendment protects "the decision of both what to say and what *not* to say"); Wooley v. Maynard, 430 U.S. 705, 714 (1977) (noting 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").

75. Hurley v. Irish-Am. Gay, Lesbian & Bisexual Grp. of Boston, 515 U.S. 557, 573 (1995) (citing Pacific Gas & Elec. Co. v. Public Utils. Comm'n of Cal., 475 U.S. 1, 16 (1986) (plurality opinion)).

76. *Id.* at 561.

77. *Id.* at 559, 581.

78. *See id.* at 562.

79. *Id.* at 573 (citing W. Va. Bd. of Educ. v. Barnette, 319 U.S. 624, 642 (1943)).

80. Wooley v. Maynard, 430 U.S. 705, 715 (1977).

81. *Hurley*, 515 U.S. at 573–74.

hold that compelled false speech requires an even more exacting strict scrutiny review than compelled speech or silence.

And, indeed, it is possible that compelled speech may be subject to an even stricter standard than compelled silence because it requires an affirmative act. In a concurring opinion in *Jackler v. Byrne*, a case granting First Amendment protection to a government employee's speech, Judge Robert Sack of the Second Circuit Court of Appeals suggested that "government compulsion to speak . . . may well be *more* strictly limited than government compulsion not to speak."[82] Such reasoning accords with the understanding that requiring an affirmative act is more burdensome than merely prohibiting an act.[83]

Furthermore, the act of compelling false speech is a more intrusive restriction on freedom of expression than even ordinary compelled speech or silence. Noting the inherent difference in scale between compelling speech that is true and compelling speech that is false, Judge Sack observed:

> "[I]t seems unlikely that Galileo's dispute with Church authorities about Copernican theory . . . would be as infamous had he been forbidden to assert . . . that the earth moves about the sun, rather than forced to state publicly and contrary to his conviction that the sun revolves around the earth."[84]

4. Strict Scrutiny

Whether or not compelled lies are subject to stricter scrutiny than compelled speech or compelled silence, canaries may receive greater First Amendment protection than nondisclosure orders because killing a canary communicates less information than does affirmatively notifying the public of a government order. As they operate on a yes/no binary, canaries cannot inform the public of the crucial details in the requests beyond the existence of that request. For example, canaries generally do not indicate the number of government orders received — rather, they merely indicate that the number is greater than zero.[85] Nor do they identify with specificity the users to which

82. Jackler v. Byrne, 658 F.3d 225, 246 (2d Cir. 2011) (Sack, J., concurring).

83. *Cf.* Cacchillo v. Insmed, Inc., 638 F.3d 401, 405–06 (2d Cir. 2011) (analogously holding that the burden to obtain an injunction "is even higher on a party . . . that seeks a mandatory preliminary injunction that alters the status quo by commanding some positive act, as opposed to a prohibitory injunction seeking only to maintain the status quo") (internal citations omitted).

84. *Jackler*, 658 F.3d at 246 (Sack, J., concurring).

85. Letter from James M. Cole, *supra* note 13.

the requests apply.[86] For these reasons, even where the government narrowly tailored a nondisclosure order to protect its compelling interests, forcing a company to publish a false canary would not protect national security interests to the same degree. As a result, compelling a false canary could fail strict scrutiny's "means-end" test even when a nondisclosure order survives.

5. Constitutional Avoidance

Ultimately, courts need not even reach the First Amendment question of whether the government can compel a false canary because no statute explicitly authorizes the government to do so. The canon of constitutional avoidance requires that courts interpret statutes to eliminate constitutional questions whenever possible.[87] As discussed above, interpreting the nondisclosure statutes to force false speech would raise a host of difficult First Amendment questions.[88] Because Congress did not explicitly intend for nondisclosure regulations to compel such speech,[89] courts should not interpret these statutes to authorize the publication of false canaries, in order to avoid problematic First Amendment issues.[90] Congress may, of course, choose to amend the statutes to authorize national security agencies to compel false speech in the future. Unless and until Congress does so, courts should not understand these statutes to authorize such a sweeping and constitutionally suspect power.

IV. MOVING THE LAW FORWARD: A VISION FOR LITIGATION

Like all content-based restrictions on speech, limits on warrant canaries must be subject to a "means-ends" strict scrutiny analysis.[91] Courts are unlikely to apply First Amendment protection to the hypothetical canary that provides personalized daily notices to individual user accounts, given the actual damage it could inflict on a

86. *See supra* Part II.B. (no company has yet employed a granular canary for individual users).

87. *See, e.g.*, Clark v. Martinez, 543 U.S. 371, 380–81 (2005) (noting that "when deciding which of two plausible statutory constructions to adopt . . . [i]f one of them would raise a multitude of constitutional problems, the other should prevail").

88. *See supra* Part III.B.1–4.

89. *See, e.g.*, 18 U.S.C. § 2705(b) (2012) (authorizing nondisclosure orders for Electronic Communications Privacy Act surveillance); 50 U.S.C. § 1861(d) (2012) (authorizing nondisclosure orders for Section 215 surveillance); while these statutory provisions prohibit speech about the receipt of a particular government order, they do not compel false speech.

90. *See* Rust v. Sullivan, 500 U.S. 173, 207 (1991) (invoking the canon of constitutional avoidance, "[i]t is both logical and eminently prudent to assume that when Congress intends to press the limits of constitutionality in its enactments, it will express that intent in explicit and unambiguous terms").

91. *See* Sable Commc'ns of Cal. v. F.C.C., 492 U.S. 115, 126 (1989).

legitimate investigation. On the other end of the spectrum, the First Amendment almost certainly protects canaries that do not inflict real harm on the government's national security interest, even where the nondisclosure orders that the canaries evade do survive strict scrutiny. Compelling a lie is categorically more intrusive than compelling either truthful speech or silence. As such, compelled false speech should be subject to the most exacting strict scrutiny to ensure that the government does not infringe on companies' First Amendment rights, except where doing so is necessary to meet a pressing national security issue.

Given that the question of compelled false speech is a novel one, the facts of the first case litigated are likely to prove critical to the development of the law in this area. A company with a commitment to transparency and an interest in furthering the national debate over government surveillance could greatly advance the law by adopting a canary carefully crafted to pose minimal threat to national security investigations. Subsequently, it should seek a declaratory judgment to obtain an advisory opinion on the canary's legality.

Three major factors would align in an ideal test canary: the scope of the canary, the size of the company, and the frequency of its publication cycle. First, the scope of the information communicated should be as general as possible, falling squarely within the public policy category and offering few, if any, granular details. An illustrative example is Electric Embers' canary, which declares, "[s]ince our beginnings in 2003, we have received and complied with 0 (zero) government requests for information."[92] This canary avoids specifying particular surveillance authorities or specific platforms or services that the requests may have targeted. As such, the scope of the canary gives no particular user any reason to think that he or she has become the target of a government investigation.

Second, the company bringing a test case should have a relatively large number of users, such that if the company establishes that it has received at least one request, this information would not provide a significant indication that the government targeted any given user. If a company like Apple or Google, with millions of global users,[93] removed a canary, an individual user is not likely to believe that the

92. *Privacy Policy*, ELEC. EMBERS, http://electricembers.coop/about-us/privacy-policy/ (last visited May 9, 2015).

93. *See* Keith Griffith & John Heggestuen, *Apple's Astronomical 800 Million iTunes Accounts Could Give It a Huge Advantage in Payments*, BUSINESS INSIDER (Apr. 24, 2014, 4:00 PM), http://www.businessinsider.com/apples-astronomical-800-million-itunes-accounts-could-give-it-a-huge-advantage-in-payments-2014-4; Adrian Covert, *Gmail at 10: How Google Dominated E-Mail*, CNN MONEY (Apr. 1, 2014, 7:01 AM EST), http://money.cnn.com/2014/04/01/technology/gmail/ (Gmail "boast[s] more than 500 million users").

government directed the warrant at his or her account. A company with only a few clients occupies the other extreme; even acknowledging it had received one request may give customers reason to think that they are intelligence targets, and prompt them to change their behavior accordingly. With more than 800 clients,[94] Electric Embers occupies a middle ground. Although killing its canary would probably not alert every customer that their data is no longer secure, a minority of particularly sensitive clients still might move their business. For this reason, an ideal company to bring a test case would have at least several thousand clients.

Finally, the company should publish a test canary infrequently so as to avoid giving users immediate notification of a law enforcement request. Observers have noted that if a canary published bi-annually "is ever challenged in court, the ample time will allow a judge to coolly and calmly review the constitutionality of any government attempt to compel [the company] to lie."[95] In contrast, killing a weekly canary would almost certainly implicate a current investigation and raise pressing national security concerns. A judge would be more likely to uphold the compelled publication of a false canary if doing otherwise would endanger an active, time-sensitive investigation.[96]

Should a large company seek a declaratory judgment condoning an infrequently updated public policy canary, the government would have minimal grounds on which to argue. There would be little evidence to support that the canary sufficiently jeopardizes the government's national security interest so as to justify compelling the company to lie. Even if the court cabins its ruling to the particular facts of the test case, even one opinion sanctioning the use of canaries would establish useful precedent for future litigation. Furthermore, it would encourage companies to continue adopting canaries as a strategy to promote transparency and public understanding of government surveillance practices.

V. CONCLUSION

Ultimately, the growing prevalence of warrant canaries reflects the disconnect between the government's pervasive surveillance programs and emphasis on secrecy, and the public's desire to meaningfully participate in a democratic discussion on national

94. *Who We Serve*, ELEC. EMBERS, http://electricembers.coop/about-us/who-we-serve/ (last visited May 9, 2015).

95. Glaser, *supra* note 40.

96. *See id.* (suggesting that "if the first challenge to a warrant canary comes before a court in a . . . rushed context, a rushed judge could make bad law").

security. The fact that some of America's largest corporations are using canaries as an end run around national security orders demonstrates that the government's regime of secrecy currently in place is no longer workable in light of the increasing public demand for transparency and accountability.

Warrant canaries can open a door for Internet companies to promote openness surrounding the government's security policies and participate in the public discussion of government surveillance powers. These are critical goals, and companies should be lauded for pursuing them with the limited tools at their disposal. Establishing that canaries are lawful is a small and meaningful step toward transparency, and the framework described in this Note may help a company push the law in that direction.

At their core, however, canaries operate on a technicality by exploiting a difference in the First Amendment's protection of compelled silence and coerced lies.[97] To the extent that courts may permit companies to communicate information through a warrant canary that they could not affirmatively communicate under a nondisclosure order, canaries highlight that the secrecy of the government's current surveillance practices is too constrictive. Ideally, companies should not have to exploit legal loopholes to surreptitiously communicate minimal information. Rather, the government and the courts should reexamine the need for restrictive nondisclosure orders, and subsequently adopt procedures to better accommodate the public's desire for information about the government's security practices. Democratizing decisions regarding government surveillance and adopting a policy of increased transparency would not only obviate the need for warrant canaries, but also advance the First Amendment's key objective — to enhance public discussion of these critical issues.

97. *See supra* Part III.B.1–3.