“THE FBI HAS NOT BEEN HERE [WATCH VERY CLOSELY FOR THE REMOVAL OF THIS SIGN]”: WARRANT CANARIES AND FIRST AMENDMENT PROTECTION FOR COMPELLED SPEECH

Wendy Everett*

INTRODUCTION

Suppose that you are a storeowner in a village where the police force declares they have the right to search any store without a warrant if they believe that the search is relevant to an ongoing investigation. They expect that they will rarely, if ever, use this power, but according to the declaration, the store may not let anyone else know about the search. Concerned about this broad search power and the requirement to keep silent about any searches, all the storeowners agree to post a note that their store has not been searched. The owners also agree to remove the sign if they are searched; signaling to the other villagers that a search occurred.

One night the police appear and search your store. The police further prevent you from removing the sign in your window that states you haven’t been searched. The next morning, confused and unsettled, you walk down the street, looking cynically at all the “no searches here” signs in the store windows.

This is the situation that faces companies on the receiving end of National Security Letters (“NSLs”) or requests issued under the Foreign Intelligence Surveillance Act1 (“FISA orders”).2 NSLs are issued to gather customer data for use in counterterrorism and other national security investigations.3 Requests issued under FISA are similar, but directed at foreign powers or their agents.4

* George Mason University School of Law, J.D. Candidate, May 2016; Production Editor, GEORGE MASON LAW REVIEW, 2015-2016; Wellesley College, B.A., Media Arts and Sciences, 1999. I would like to thank my friends and family for their constant love and support.


3 OFFICE OF THE INSPECTOR GEN., U.S. DEP’T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION’S USE OF NATIONAL SECURITY LETTERS: ASSESSMENT OF PROGRESS IN IMPLEMENTING RECOMMENDATIONS AND EXAMINATION OF USE IN 2007 THROUGH 2009, at 2-3 (2014), http://www.justice.gov/oig/reports/2014/s1408.pdf (“National security letters are written directives to produce records that the FBI issues to third parties such as telephone companies, Internet service providers, financial institutions, and consumer credit reporting agencies. . . . [E]ach NSL statute has special
In the last ten years, the increased use of cellphones, combined with the growth of cloud computing, resulted in the storage of more private information than ever on servers.\(^4\) Law enforcement agencies responded to this shift by making requests—customer account information, stored emails, and other data that used to be cumbersome or difficult for officers to access—under a variety of authorities.\(^6\) NSLs and FISA orders are not like the more familiar standard warrants or subpoenas because they differ in the type of judicial oversight, the information that can be accessed, and the secrecy they impose.\(^7\)

Concerned that the United States government’s requests for customer information were broader than the public understood, Internet Service Providers (“ISPs”) and other technology companies published transparency reports containing counts of the number of subpoenas, warrants, and other law enforcement requests they received.\(^8\) Along with these statistics, some included statements that they had not, to date, received any NSLs or FISA orders.\(^9\) Like the window signs of the storeowners, these statements are dubbed warrant canaries, as they will alert the public that the company was

---

\(^4\) **Susan Landau,** *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* 77-78 (2010).


\(^6\) See King & Raja, supra note 5, at 452 & n.159.


\(^9\) 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/ (“Apple has become one of the first big-name tech companies to use a novel legal tactic to indicate whether the government has requested user information in conjunction with a gag order. Known as a ‘warrant canary,’ this language is encapsulated on Apple’s fifth page of its new transparency report (PDF), which was published on Tuesday. . . . Warrant canaries work like this: a company publishes a notice saying that a warrant has not been served as of a particular date. Should that notice be taken down, users are to surmise that the company has indeed been served with one. The theory is that while a court can compel someone to not speak (a gag order), it cannot compel someone to lie. The only problem is that warrant canaries have yet to be fully tested in court.”).
served with a NSL or a FISA order if they disappear. Receiving a request would “trip” the warrant canary, and the company would surreptitiously alert the public by removing the canary line. A careful observer may therefore discover the companies served with NSLs by checking for disappearing canaries.

Disclosure of a NSL or FISA order through the use of a warrant canary can result in serious penalties. Because of this, the government, in seeking to protect investigations that might be compromised by disclosure of a NSL, can put serious pressure on companies attempting to remove their canary. The government maintains that the secrecy provisions in the statutes governing NSLs and FISA orders impose an obligation to prevent leaking any information about who has received these requests. As one recipient explained, this obligation of nondisclosure essentially forces someone under investigation to lie. Applying this to the storeowner scenario explored above, this would imply that any company with a canary must leave it up even after it is no longer true. An ISP in this situation, however, may

---

10 Id.; see also Nate Cardozo et al., Panel II: Balancing National Security and Transparency in Government Data Collection, 32 CARDozo ARTS & ENT. L.J. 813, 825 (2014) (“A warrant canary is a statement by a company or any kind of online service provider, that it has not received any of a particular kind of request. For instance, say I run a small server to provide email for my wife and myself. I could have a statement on my website that says I have received zero subpoenas, zero warrants, zero national security letters, and zero national security orders. That statement is true. I have not received any request for my data from the government. That’s a warrant canary.”).


12 18 U.S.C. § 1510(e) (2012) (“Whoever, having been notified of the applicable disclosure prohibitions or confidentiality requirements of [any of the five NSL statutes], knowingly and with the intent to obstruct an investigation or judicial proceeding violates such prohibitions or requirements applicable by law to such person shall be imprisoned for not more than five years, fined under this title, or both.”); see 50 U.S.C. § 1861(d)(1) (2012), amended by USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 102, 129 Stat. 268, 272 (prohibiting the disclosure of a FISA order but not specifying a penalty).

13 See, e.g., USA FREEDOM Act § 502, 129 Stat. at 283-88 (to be codified at 18 U.S.C. § 2709(c), 12 U.S.C. § 3414(c), 15 U.S.C. §§ 1681a(d), 1681v(c), and 50 U.S.C. § 3162(b)) (making uniform the NSL nondisclosure requirements for all five NSL statutes); Jack M. Balkin, Old-School/New-School Speech Regulation, 127 HARV. L. REV. 2296, 2330 n.148 (2014) (“A recipient may not disclose the fact or the contents of the NSL or the accompanying gag order to anyone (except an attorney representing the recipient) if a senior FBI official certifies that ‘otherwise there may result a danger to the national security of the United States, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person.’” (quoting 18 U.S.C. § 2709(c)(1) (2012))).

14 Editorial, My National Security Letter Gag Order, WASH. POST (Mar. 23, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/03/22/AR2007032201882.html [hereinafter Editorial, My Gag Order] (“Under the threat of criminal prosecution, I must hide all aspects of my involvement in the case—including the mere fact that I received an NSL—from my colleagues, my family and my friends. When I meet with my attorneys I cannot tell my girlfriend where I am going or where I have been. I hide any papers related to the case in a place where she will not look. When clients and friends ask me whether I am the one challenging the constitutionality of the NSL statute, I have no choice but to look them in the eye and lie.”).
raise a First Amendment defense, arguing that being forced to publish the canary compels it to make a statement it does not agree with.\textsuperscript{15}

The First Amendment protects speech rights and ensures the right to criticize the government.\textsuperscript{16} To receive First Amendment protections, however, the ISP would have to prove that there was a speech act to be protected.\textsuperscript{17} If the ISP regularly generates new transparency reports and includes a zero-count warrant canary in the report, they may argue that being required to continue to publish the canary after it is tripped is an act of compelled speech. They would prefer to delete the canary but fear government action for disclosing—through the deletion—the receipt of a NSL; therefore, they must publish the false canary even though they would prefer to remain silent.

Conversely, removing a previously unchanged canary, after it has tripped through the receipt of a NSL or FISA order by the service provider who publishes the canary, might not appear to be speech—this is the case where the canary is simply deleted. The nondisclosure provision of the NSL would seem to compel the company to do nothing, and so how could that be deserving of First Amendment protections?

Having a report with your name on it, with a statement you no longer agree with, however, is speech, and should be analyzed under \textit{Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston}\textsuperscript{18} because the expressive content contained in this report is perceived as attributable to you. The action the ISP would like to take, deleting the line, is restricted by the NSL nondisclosure provision (as it would communicate to a watcher that a NSL was received), and so it may be a prior restraint.

This Comment argues that the nondisclosure provisions with respect to warrant canaries are invalid under the First Amendment as content-based speech regulations. This is the case, in part, because as content-based speech restrictions, they should be judged under the highest standard of strict scrutiny.\textsuperscript{19} Further, this Comment shows that the canaries are not commercial speech, despite being published by commercial entities, and so are due the highest level of protection of strict scrutiny.\textsuperscript{20} Finally, this Comment shows that the nondisclosure provisions are invalid as prior re-

\textsuperscript{16} U.S. CONST. amend. I.
\textsuperscript{18} 515 U.S. 557 (1995).
straints, and therefore also due the highest level of protection of strict scrutiny.\footnote{See Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559 (1976); see also Lovell v. City of Griffin, 303 U.S. 444, 452 (1938).}

In demonstrating that nondisclosure provisions are invalid, Part I provides background information on transparency reports and warrant canaries as well as covering the essential characteristics of National Security Letters and FISA orders. Part II explains the nondisclosure provisions at the heart of the debate. Part III explores First Amendment doctrine as it relates to content-based speech restrictions, compelled speech protection, commercial speech, and prior restraints. Part III applies First Amendment jurisprudence to compelled publication of a warrant canary after the company receives a NSL or FISA order. Finally, Part IV argues that canaries should be analyzed under a strict scrutiny standard because their use informs the public by shedding light on the government’s use of electronic surveillance.

I. TRANSPARENCY REPORTS AND WARRANT CANARIES

concern over government access to customer data, and the increasing realization among consumers that there were few restrictions on the information governments could, and did, request from various service providers.

The ubiquity of mobile computing devices has accelerated the recent push to cloud storage for several reasons. As more people go online, use of new technologies such as email and search engines create new types of data for law enforcement to seek out for investigations, such as stored emails and lists of search terms. Law enforcement agencies adapted to the migration of online storage by expanding the number of subscriber information requests made to carriers and Internet companies. The development of transparency reports by technology companies as a response to recent disclosures of government surveillance of electronic communications is explored below.

A. NSA Prism Disclosures Lead to an Increase in Transparency Reports and Warrant Canaries

Disclosure of some of the National Security Agency’s (“NSA”) surveillance methods in 2013 increased consumer awareness for how little protection is given to data stored in the cloud. Transparency reports were first published as experiments in the 2000s and proliferated in response to these concerns.


31 See Timberg, supra note 29.


33 See LANDAU, supra note 4, at 220.


35 See Kaufman, supra note 15.

36 rsync.net is considered to be the first transparency report, and has maintained one online since about 2006. The rsync.net canary is interesting because, in addition to cryptographically signing their canary, they include recent news headlines so that a series of canary posts cannot be created ahead of time and posted. rsync.net Warrant Canary, RSYNC.NET, http://www.rsync.net/resources/notices/canary.txt (last visited Jan. 2, 2016).

37 See Kaufman, supra note 15.
Transparency reports can be multiple pages (e.g., Google38) or just a single page listing various types of subpoenas and warrant requests received.39 Incentives for the publication of these reports vary. Although the exact contacts and format vary, the transparency reports generally include the number of accounts affected, number of warrants, number of subpoenas received, and explanatory text.40 Most content in transparency reports presents no problems, as there are no restrictions on disclosing the number of subpoenas or warrants requests received. Other types of law enforcement requests, however, may not be disclosed to the public. Requests from the FBI, the NSLs, lack the judicial oversight of warrants.41 They additionally come with a nondisclosure provision, muzzling the recipient.42

Before the passage of the Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 201543 ("USA FREEDOM Act"), recipients of a NSL were not allowed to even share the fact that they received the order with anyone other than their attorney and staff members tasked with retrieving the requested information.44 On June 2, 2015, the USA FREEDOM Act was signed into law, granting some limited disclosure bands for companies seeking to include NSLs or FISA orders in their transparency reports.45 Under this new law, companies may disclose NSLs in bands of 0-249, or FISA orders in similar bands of 0-499, depending on the chosen methods.46

The nondisclosure provision thus still precludes companies from publishing the exact number of NSLs they have received.47 A similar nondisclosure requirement keeps recipients of FISA orders from including those

38 See, e.g., Google Transparency Report, supra note 22.
40 Kopstein, supra note 8.
45 USA FREEDOM Act, sec. 603, § 604, 129 Stat. at 295 (to be codified at 50 U.S.C. § 1874) (updating FISA’s title VI by adding a section 604, entitled “Public Reporting by Persons Subject to Orders,” which specifically includes both FISA orders and NSLs).
46 Id. This new section contains four options for reporting counts of NSLs and FISA orders. Id.
counts as well. Precluded from including the information customers were most interested in, companies sought a solution to their bind.

The answer came in the form of a simple message: a warrant canary. In 2002, a librarian in Vermont posted a sign with the short message, “The FBI has not been here [watch very closely for the removal of this sign].” This clever sign was one of the first warrant canaries, designed to alert the public to future government surveillance. Prevented from affirmatively publishing the number of NSLs or FISA orders they received, companies took an alternative track and began publishing canaries that they planned to remove after receiving a surveillance request with a nondisclosure provision. “Watch for the removal of this sign” became “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.” Similarly, concerns that the new band thresholds, which start at zero, would prevent a company that previously never received a NSL from removing a “zero only” warrant canary has led some companies to pre-emptively publish “zero based” warrant canaries during product launches.

49 See, e.g., 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.
50 Nadia Kayyali, EFF Joins Coalition to Launch Canarywatch.org, EFF (Feb. 2, 2015), https://www.eff.org/deeplinks/2015/01/eff-joins-coalition-launch-canarywatchorg (“Warrant canary’ is a colloquial term for a regularly published statement that an internet service provider (ISP) has not received legal process that it would be prohibited from saying it had received, such as a national security letter. The term ‘warrant canary’ is a reference to the canaries used to provide warnings in coalmines, which would become sick from carbon monoxide poisoning before the miners would—warning of the otherwise-invisible danger. Just like canaries in a coalmine, the canaries on web pages ‘die’ when they are exposed to something toxic—like a secret FISA court order.”).
51 Jessamyn West, The FBI, and Whether They’ve Been Here or Not, LIBRARIAN.NET (Sept. 9, 2013), http://www.librarian.net/tag/warrantcanary/.
54 Cory Doctorow, EFF’s New Certificate Authority Publishes an All-Zero, Pre-Release Transparency Report, BOINGBOING (July 3, 2015), http://boingboing.net/2015/07/03/effs-new-certificate-authori.html (“EFF, Mozilla and pals are launching Let’s Encrypt, an all-free certificate authority, in September—but they’ve released a transparency report months in advance.”).
2016] THE FBI HAS NOT BEEN HERE 385

B. Warrant Canaries Explored

The Washington Post calls warrant canaries “mostly a PR stunt,”\(^{55}\) published by companies fearful of losing business and wary of being paint-
ed as willing conspirators to the NSA and FBI, while others see them as a
vital tool for an increasingly wired democracy.\(^{56}\) Critics decry the lack of
pushback by companies to government requests for subscriber data.\(^{57}\) They
see a widespread trend of acquiescence to surveillance requests, feeding yet
more surveillance.\(^{58}\) For example, the number of NSLs issued is tied to the
nondisclosure provisions they carry.\(^{59}\)

After the popularity of transparency reports began spreading in the fall
of 2013, several companies pressured the Department of Justice (“DOJ”) into
allowing them to disclose more information about embargoed requests.\(^{60}\) Five technology companies won permission in January 2014 to
publish ranges of information about some categories of requests, and now
publish aggregate statistics on such law enforcement requests.\(^{61}\)

While Facebook, LinkedIn, and the other companies that entered into
the publication agreement with the DOJ may publish these declassified ag-
gregate counts,\(^{62}\) questions remain about warrant canaries embedded in the

---

\(^{55}\) Andrea Peterson, Here’s Why Tech Companies’ NSA ‘Transparency Reports’ are Mostly a PR
heres-why-tech-companies-nsa-transparency-reports-are-mostly-a-pr-stunt/.

\(^{56}\) See We Need to Know, CENTER FOR DEMOCRACY & TECH. (July 18, 2013), https://cdt.org/
insight/we-need-to-know/.

\(^{57}\) Christopher Soghoian, An End to Privacy Theater: Exposing and Discouraging Corporate

\(^{58}\) See id. at 193, 236-37.

\(^{59}\) Editorial, My Gag Order, supra note 14 (“The inspector general’s report makes clear that NSL
gag orders have had even more pernicious effects. Without the gag orders issued on recipients of the
letters, it is doubtful that the FBI would have been able to abuse the NSL power the way that it did.
Some recipients would have spoken out about perceived abuses, and the FBI’s actions would have been
subject to some degree of public scrutiny.”).

\(^{60}\) Miller, supra note 8 (describing the suits filed with the Foreign Intelligence Surveillance Court
by Yahoo and Facebook requesting permission to publish information about FISA orders).

to-disclose-more-data-on-surveillance-requests.html; Carrie Cordero, An Update on the Status of FISA
status-fisa-transparency-reporting; 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.

\(^{62}\) The DOJ letter allows for two options for publication of requests. Under Option One, providers
may report aggregate data about 7 categories:

1. Criminal process, subject to no restrictions.
2. The number of NSLs received, reported in bands of 1000 starting with 0-999.
3. The number of customer accounts affected by NSLs, reported in bands of 1000 starting
   with 0-999.
transparency reports. Twitter, who was not part of the DOJ aggregate count agreement, filed suit in the District Court for the Northern District of California seeking declaratory judgment to publish a detailed transparency report. That ruling is currently pending. A key issue in the case is the right to publish a transparency report containing a warrant canary, in the form of a sentence, stating that the company received zero NSLs, instead of the 0-249 range allowed by the DOJ. With the passage of the USA FREEDOM Act, both sides filed briefs on the effect of the new bands of counts allowed and whether they would permit Twitter’s proposed transparency report format.

4. The number of FISA orders for content, reported in bands of 1000 starting with 0-999.
5. The number of customer selectors targeted under FISA content orders, in bands of 1000 starting with 0-999.
6. The number of FISA orders for non-content, reported in bands of 1000 starting with 0-999.
7. The number of customer selectors targeted under FISA non-content orders, in bands of 1000 starting with 0-999.

A provider may publish the FISA and NSL numbers every six months. For FISA information, there will be a six-month delay between the publication date and the period covered by the report. For example, a report published on July 1, 2015, will reflect the FISA data for the period ending December 31, 2014. In addition, there 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 (whether developed or acquired) for which the company has not previously received such an order, and that is designated by the government as a ‘New Capability Order.’

Letter from James M. Cole, Deputy Attorney Gen., U.S. Dep’t of Justice, to Gen. Counsels at Facebook, Google, LinkedIn, Microsoft, and Yahoo 2-3 (Jan. 27, 2014) (footnote omitted), http://www.washingtonpost.com/national/security/Graphics/dagletter.pdf. Under Option Two, a provider may report aggregate data for only 3 categories:

1. Criminal process, subject to no restrictions.
2. The total number of all national security process received, including all NSL and FISA orders, reported as a single number in the following bands: 0-249 and thereafter in bands of 250.
3. The total number of customer selectors targeted under all national security process, including all NSLs and FISA orders, reported as a single number in the following bands, 0-249, and thereafter in bands of 250.

Id. at 3. The USA FREEDOM Act (passed on June 2, 2015) preserved these bands with minor changes by amending FISA, expanding the transparency report publication options for companies. USA FREEDOM Act of 2015, Pub. L. No. 114-23, sec. 603, § 604, 129 Stat. 268, 295-97. Somewhat confusingly, section 603 of the USA FREEDOM Act adds a new section 604 to the end of FISA’s Title VI, which will eventually be codified at 50 U.S.C. § 1874. Id.

64 The court recently ordered Twitter to amend their complaint due to the enactment of the USA FREEDOM Act. Order Denying Motion to Dismiss as Moot and, on the Court’s Own Motion, Ordering Filing of Amended Complaint in Light of Recent Legislation, Twitter, Inc. v. Lynch, No. 14-cv-04480-YGR (N.D. Cal. Oct. 14, 2015).
66 Supplemental Brief Regarding the USA FREEDOM Act at 1, Twitter, Inc. v. Lynch, No. 14-cv-4480 (N.D. Cal. July 17, 2015) (arguing that Twitter’s challenges are now moot while also stating that Twitter’s transparency report would not be allowed under the USA FREEDOM Act); Twitter’s Opening Supplemental Brief on Effect of Recent Legislation at 6, Twitter, Inc. v. Lynch, No. 14-cv-4480 (N.D. Cal. Oct. 7, 2014).
If a company never received a NSL or a FISA order, what does it gain by publishing a warrant canary? Should it push for protections for a canary that may never go off, or for speech it initiated by publishing the canary? In their amicus brief supporting Twitter, Freedom of the Press Foundation argued that the software companies were uniquely positioned to contribute to the debate on electronic surveillance measures, as both suppliers of electronic communications and as recipients of NSLs.67

Apple recently removed or moved and reworded its warrant canary, prompting debate about whether Apple received a NSL or FISA order.68 Scenarios like this prompt speculation about whether companies could be compelled to leave up a canary after being served with a NSL. It is currently unknown whether Apple changed the wording in the report of their own volition, or if the report is meant to signify that they did, in fact, receive a NSL.69

What each of these transparency reports has in common is an effort to educate the public on the range of data requests made by the government under various authorities, ranging from the more familiar warrants to NSLs and FISA orders. NSLs and FISA orders are meant to serve different needs of the law enforcement and intelligent communities, but their nondisclosure provisions are similar.70

II. NATIONAL SECURITY LETTERS AND FISA ORDERS

The Fourth Amendment protects Americans from unreasonable searches and seizures by preventing law enforcement officials from issuing general warrants when investigating crimes.71 Although originally written to cover physical searches of people, their homes, and possessions, courts have also applied Fourth Amendment protections to searches and seizures

---

67 Brief of Amicus Curiae Freedom of the Press Found. in Support of Plaintiff’s Opposition to Defendants’ Partial Motion to Dismiss at 2, Twitter, Inc. v. Holder, No. 14-cv-04480-YGR (N.D. Cal. Feb. 17, 2015) (“Because of the uniquely dual role that technology companies play with respect to government surveillance—at once custodians of Americans’ private data and recipients of government requests for that data—these companies have a critical perspective on the issue.”).


69 Iain Thomson, Apple’s Warrant Canary Riddle: Cock-Up, Conspiracy, or Anti-Google Point-Scooring, REGISTER (Sept. 20, 2014, 3:34 AM), http://www.theregister.co.uk/2014/09/20/apples_warrant_canary_is_either_cockup_conspiracy_or_the_antigoogle_selling_point/.


71 U.S. CONST. amend. IV; Thomas Y. Davies, Recovering the Original Fourth Amendment, 98 MICH. L. REV. 547, 551 (1999).
of electronic communications.\textsuperscript{72} It is beyond the scope of this Comment to present a full explanation of this body of law, but some background will help explain the use of NSLs and FISA orders by law enforcement officials.

Part II.A explains the Fourth Amendment and statutes that govern collection of this data in criminal and intelligence investigations. Part II.B discusses NSLs and FISA orders. Finally, Part II.C covers the statutory basis for the nondisclosure provisions of these authorities.

A. The Fourth Amendment and the Content-Metadata Distinction

Distinctions stemming from the very early days of Fourth Amendment case law hold that there is a difference between the contents of communication, such as the body of a letter, and information about that letter, such as address information of the sender and receiver.\textsuperscript{73} The address information is generally viewed as metadata, thereby deserving of less protection than the contents of communications.\textsuperscript{74} Therefore, while traditional warrants, supported by probable cause and judicial approval, were required to see the content of a sealed letter, only a subpoena supported by lesser standards was required to see address information.\textsuperscript{75} When applied to electronic communications, this means that the body of an email message is considered content, while information such as the “to:” and “from:” fields, as well as other message headers, are considered metadata.\textsuperscript{76}

In addition to the Fourth Amendment, the Electronic Communications Privacy Act of 1986\textsuperscript{77} ("ECPA") protects communication data in transit and when stored, such as in email messages.\textsuperscript{78} The ECPA contains a number of


\textsuperscript{73} Matthew J. Tokson, The Content/Envelope Distinction in Internet Law, 50 WM. & MARY L. REV. 2105, 2112 (2009).

\textsuperscript{74} See id.

\textsuperscript{75} See id. at 2112, 2122.

\textsuperscript{76} Metadata is any information about a message, as opposed to text of the body of the message, which is considered content. Metadata includes information such as the sender’s name and address, the recipient’s name and address, the time the message was sent, the place it was sent from, the place it was sent to, and any information collected on way points along the way, such as email headers logging the email servers which processed the message. A Guardian Guide to Metadata, GUARDIAN (June 12, 2013, 11:52 AM), http://www.theguardian.com/technology/interactive/2013/jun/12/what-is-metadata-nsa-surveillance.


\textsuperscript{78} See Nathaniel Gleicher, Neither a Customer Nor a Subscriber Be: Regulating the Release of User Information on the World Wide Web, 118 YALE L.J. 1945, 1946 (2009) ("The Electronic Communications Privacy Act of 1986 (ECPA) contains two parts: Title I, the Wiretap Act, which covers wire, oral, and electronic communications in transit; and Title II, the Stored Communications Act (SCA), which covers communications in electronic storage. Because electronic communications are stored in, and travel across, the computers of third parties, their protection under the Fourth Amendment is at best
provisions describing law enforcement access to email or stored content.\textsuperscript{79} Most law enforcement requests for electronic communications data are fairly limited and include particularity requirements and other minimization limitations.\textsuperscript{80} Some FISA orders, however, are quite broad. A single FISA order grants the requesting government agency access to a large amount of metadata, such as phone numbers called for hundreds or thousands of customers of a company.\textsuperscript{81} Although there is only a single request made to the electronic communications provider, the amount of data disclosed to the government in response to that request can be vastly more than that delivered under several NSL requests or warrants.\textsuperscript{82} This Comment focuses primarily on the nondisclosure provisions of both types of requests, and therefore must necessarily gloss over most of the differences between NSLs and the various types of FISA orders. This next Section does, however, present a very high level summary of the characteristics of each request in order.

**B. National Security Letters and FISA orders**

Law enforcement agencies use NSLs and FISA orders for criminal or national security investigations to gather content and metadata from various service providers.\textsuperscript{83} While they are issued under different statutory authorities and grant access to different types of information, they each come with nondisclosure provisions that prevent recipients from speaking about them or letting the targets know about the requests.\textsuperscript{84}

The broadness of FISA orders, even though such requests must be approved by a Foreign Intelligence Surveillance Court ("FISC") judge, are a
cause for concern for many. Although NSLs do not allow access to as much information, critics decry the lack of any judicial oversight, as they are issued directly by the administering agency. Indeed, at least one DOJ Inspector General report notes that when the FBI is unable to get a FISA order authorized by a FISC judge, they instead issue a NSL, because those do not require judicial oversight.

1. National Security Letters

Congress created the first NSL as part of the Right to Financial Privacy Act of 1978 (“RFPA”), expanding law enforcement access to financial records. It gave the FBI access to certain information held by banks for use in criminal or national security investigations. Four NSL statutes, granting access to various types of records, existed by the 2000s. Section 505 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (“USA PATRIOT Act”) updated three of these existing NSL authorities, and section 358(g) added an additional one to the Fair Credit Reporting Act.
Since NSLs are designed to be an investigative tool for use by the FBI in national security investigations, they are intended to be limited in their use to espionage or terrorism cases, and are issued by the agency after a certification that the records sought are for use in national security investigations. Critics refer to NSLs as FBI’s “extra-judicial backdoor into investigations” due to the lack of judicial oversight. Rather than convincing a judge that there is probable cause to issue a warrant, NSLs may be issued directly by the FBI, and have a lower standard. Furthermore, nondisclosure provisions generally do not have a set expiration. This concerns critics and judges reviewing cases involving NSLs, but the government has moved to make potential changes to the time that nondisclosure orders stand.

Currently five NSL sections provide the FBI access to various types of information. As noted above, each provision comes with a nondisclosure requirement that makes it a felony for recipients to let anyone know that they were served with a NSL. Under the USA FREEDOM Act, the nondisclosure may be challenged in court. The nondisclosure provisions should be applied only in instances where the FBI or other issuing agency can certify that disclosing the NSL may result in danger to U.S. national security, interference with an investigation or diplomatic relations, or danger to the life of any person.


96 See LANDAU, supra note 4, at 192.

97 DOYLE, supra note 44, at 2; 1 KRIS & WILSON, supra note 81, § 20:8, at 745, 747.


99 See Michael J. Glennon, National Security and Double Government, 5 HARV. NAT’L SEC. J. 1, 6-8 (2014).


103 18 U.S.C. § 3511(b) (2012), amended by USA FREEDOM Act § 502(g), 129 Stat. at 288. The USA FREEDOM ACT removed the requirement that courts must accept as “conclusive” administration officials’ good-faith certification that nondisclosure was required. USA FREEDOM Act § 502(g), 129 Stat. at 289.

104 USA FREEDOM Act § 502(a)-(e), 129 Stat. at 283-88 (updating the nondisclosure language for all five NSL statutes).
2. Foreign Intelligence Surveillance Court Orders

FISA authorizes other government data requests that come with nondisclosure provisions.\textsuperscript{105} FISA grants access to communications data for use in investigating foreign agents.\textsuperscript{106} Both “traditional” FISA under Title I as well as the subsequently passed Sections 215 and 702 entitle law enforcement to collect a variety of subscriber data, including content and metadata for stored communications, data in transit, and “tangible goods.”\textsuperscript{107} The passage of the USA FREEDOM Act modified these authorities, removing the provisions for bulk collection, but left some FISA orders intact.\textsuperscript{108} A FISC judge approves requests after reviewing targets and procedures meant to minimize the amount of data collected to avoid unnecessary or overly broad data collection.\textsuperscript{109} Once approved, FBI agents can use the court orders to access metadata or content and perform electronic surveillance.\textsuperscript{110}

Section 702 was created as part of the FISA Amendments Act of 2008\textsuperscript{111} (“FAA”). It allows for targeted collection of content for targets outside the United States and is accompanied by a nondisclosure provision.\textsuperscript{112} Law enforcement agencies can use Section 702 to request “foreign intelligence information” from electronic service providers on persons believed not to be citizens of the United States and also located outside the United States.\textsuperscript{113} Information collected under the Section 702 program is subject to minimization procedures to restrict the actual information received by

\textsuperscript{105}See Nieland, supra note 86, at 1207 & n.37.

\textsuperscript{106}1 KRIS & WILSON, supra note 81, § 4:2, at 117.

\textsuperscript{107}See id. § 4:2, at 119; Laura K. Donohue, Bulk Metadata Collection: Statutory and Constitutional Considerations, 37 HARV. J.L. & PUB. POL’Y 757, 764 (2014) (“Initially focused on electronic surveillance, FISA expanded over time to incorporate physical searches, pen registers and trap and trace, and searches of business records and tangible goods.”).

\textsuperscript{108}H.R. 2048, The USA FREEDOM Act, HOUSE JUDICIARY COMMITTEE, http://judiciary.house.gov/index.cfm/usa-freedom-act (last visited Jan. 4, 2016) (“[The Act] prohibits bulk collection of ALL records under Section 215 of the PATRIOT Act, the FISA pen register authority, and national security letter statutes. . . . [It also creates] new procedures for the emergency use of Section 215 but requires the government to destroy the information it collects if a FISA court order is denied.”).

\textsuperscript{109}Steven G. Bradbury, Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702, LAWFARE RES. PAPER SERIES, Sept. 1, 2013, at 1, 2.

\textsuperscript{110}See 1 KRIS & WILSON, supra note 81, § 4:3.


\textsuperscript{112}50 U.S.C. § 1881a(a); 50 U.S.C. § 1861(d)(1), amended by USA FREEDOM Act § 102(b), 129 Stat. at 272; Bradbury, supra note 109, at 10.

agents working on a case. However, Section 702 allows access to the contents of emails or other communication, not just the addressing information and other metadata, and the collected data is stored for long periods by law enforcement agencies.

C. Nondisclosure Provisions

Nondisclosure requirements in NSLs and FISA orders stem from the need to protect sources, methods, and ongoing investigations as well as to prevent targets from realizing they are under surveillance. The risk to ongoing investigations is predicated on the worry that a target under surveillance will figure out that he is a target if he realizes that one of his service providers received one of these law enforcement requests. This disclosure suppression is similar to the “sneak and peek” warrants used when investigators fear that disclosure of a search will adversely affect an ongoing investigation. A further concern is that targets will deduce methodologies used by the government and alter their behavior to avoid them, thus endangering future investigations by closing off these data sources.

While electronic surveillance in criminal investigation wiretaps, such as those under the Wiretap Act, are eventually disclosed to the suspect at the close of the investigation, there is no such provision for FISA surveillance. Investigators fear that if an ISP or other company announces they received a NSL, suspects using that service provider will be tipped off.

114 Id. at 6-8.
115 Id. at 112.
116 See 1 KIRS & WILSON, supra note 81, § 20:1.
118 ACLU v. U.S. Dep’t of Justice, 265 F. Supp. 2d 20, 23-24 (D.D.C. 2003) (“Finally, the Patriot Act expanded the government’s information-gathering powers in at least one other way unrelated to FISA. Section 213 provides explicit authority for federal law enforcement officers to use so-called ‘sneak-and-peek’ warrants. Such warrants allow agents to conduct searches secretly (whether physically or virtually), to observe or copy evidence, and to depart the location searched, generally without taking any tangible evidence or leaving notice of their presence.”); see also ADMIN. OFFICE OF THE U.S. COURTS, REPORT OF THE DIRECTOR OF THE ADMINISTRATIVE OFFICE OF THE UNITED STATES COURTS ON APPLICATIONS FOR DELAYED-NOTICE SEARCH WARRANTS AND EXTENSIONS 1 (2014), http://www.uscourts.gov/file/18430/download (providing data on the number of applications under the Patriot Act for warrants and extensions of warrants authorizing delayed notice, and the number of those granted or denied in the fiscal year ending September 30, 2014).
121 1 KIRS & WILSON, supra note 81, § 29:2.
the provider is small enough, a disappearing canary might enable a suspect to realize that he or she is the likely target, or the suspect might stop using that provider and switch to another with an un-tripped canary.

To prevent either of these situations, it might appear that the investigators should simply issue NSLs and FISA orders to all possible service providers; however, the statutory requirements under which they are issued prohibit this type of broad use. With FISA orders for instance, senior DOJ officials and Directors of National Intelligence must certify that the significant purpose is to obtain foreign intelligence information under the FAA with procedures in place to limit targeting to persons reasonably believed to be located outside the United States. Additionally, for U.S. persons located abroad, there must be a judicial finding of probable cause that the target is an agent of a foreign power. These restrictions mean that blanketing service providers as a way of avoiding tipping off a suspect is not a lawful solution, and they increase the likelihood that a service provider might be required to leave intact a canary.

At this point it is unclear whether a provider that published a warrant canary with the text “We have received no NSLs” might be required to convert it to a USA FREEDOM-compliant warrant canary stating “We have received 0-249 NSLs.” Could a provider who really has received no NSLs be compelled to convert its canary to a USA FREEDOM compliant one? If a provider with a “traditional” canary does receive a NSL request, could it be compelled to convert it USA FREEDOM compliant one? Would doing so effectively act to trip the canary? Or could they be compelled to leave up their original, “We have received no NSLs” canary, because to change it would disclose the receipt of a NSL—something akin to disclosing a NSL count of one. That solitary disclosure might violate the requirement to disclose only “in bands of 250 starting with 0-249” or “in bands of 1000 starting with 0-999”

As seen, although NSLs and FISA orders allow access to various types of customer data, they have similar nondisclosure protections meant to ensure that law enforcement and intelligence investigations are not disrupted or impacted by the targets determining that they were subject to an investigation. While the ISPs and technology companies processing these requests cannot publicly disclose when they receive one, the warrant canaries deployed in the transparency reports of some corporations may hint as to the extent of the use of these orders. The next Part covers some of the rele-

---

124 Id.; see also 1 KRIS & WILSON, supra note 81, § 17:3.
125 50 U.S.C. § 1881b(b)-(c) (2012); see also 1 KRIS & WILSON, supra note 81, § 16:17.
127 See supra notes 116-119 and accompanying text.
vant First Amendment protections available to providers publishing zero-count warrant canaries.

III. FIRST AMENDMENT PROTECTIONS

The First Amendment of the United States Constitution prohibits Congress from making any laws abridging the freedom of speech or of the press.128 The right to free speech is an underpinning of United States democracy, allowing for the free flow of information, including criticism of the government. American courts place a high value on speech disapproving of the government, finding that speech critical of government actions is at the core of the type of speech protected by the First Amendment.129 Protections granted by the First Amendment extend beyond simply shielding spoken views and opinions; there is a “right to speak freely and the right to refrain from speaking at all,”130 as compelled speech protections preserve the right to be silent rather than speak a message one disagrees with. This prohibition against compelled speech stems from the understanding that the First Amendment provides for freedom of mind, and that few things are so abhorrent to the freedom of mind as being compelled to say something that one does not agree with.131

Restrictions on speech based on its content also come under close scrutiny by the courts.132 In contrast, content-neutral restrictions that place time, place, or manner restrictions on all speech generally receive only intermediate scrutiny.133

128 U.S. CONST. amend. I (“Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ”).
129 See Gentile v. State Bar of Nev., 501 U.S. 1030, 1034 (1991); Landmark Comm’ns, Inc. v. Virginia, 435 U.S. 829, 838 (1978) (“Whatever differences may exist about interpretations of the First Amendment, there is practically universal agreement that a major purpose of that Amendment was to protect the free discussion of governmental affairs.” (quoting Mills v. Alabama, 384 U.S. 214, 218 (1966))).
131 See id.
132 Caroline Mala Corbin, Compelled Disclosures, 65 ALA. L. REV. 1277, 1283 (2014).
A. Content-Neutral Speech Restrictions vs. Content-Based Speech Restrictions

Most First Amendment cases involve expressions the government would like to control in some way. The government is able to regulate speech based on time, place, or manner so long as it is content-neutral. Since this latter type of restriction is a content-based restriction, it comes under strict scrutiny by courts. Content-based restrictions that preclude speech on one topic are generally upheld only when there is a compelling reason for the restriction.

The key to differentiating between content-neutral and content-based restrictions is whether the restriction varies by the message being conveyed. Furthermore, the courts weigh dissenting speech in deciding whether government disagreement with the message conveyed is at play. Although content-neutral regulations are not free from scrutiny, they are subject to less searching by the courts, particularly if alternatives are available.

Restrictions concerning the “nature of a place” and regulating all speech, regardless of content, based on “time, place, and manner,” are valid content-neutral restrictions. When such a content-neutral regulation is narrowly tailored to promote a specific government interest, leaves open alternatives, and may be justified regardless of the content of the speech it happens to affect, then it may be upheld. For example, in Ward v. Rock Against Racism, the Court upheld municipal noise regulations that restricted musical performances in a New York City’s Central Park, finding

135 Grayned, 408 U.S. at 115.
137 Id. at 321-22.
143 Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (“[E]ven in a public forum the government may impose reasonable restrictions on the time, place, or manner of protected speech, provided the restrictions ‘are justified without reference to the content of the regulated speech, that they are narrowly tailored to serve a significant governmental interest, and that they leave open ample alternative channels for communication of the information.’” (quoting Clark, 468 U.S. at 293)).
that the regulation was narrowly tailored and served a content-neutral purpose by restricting all excessive noise levels.\textsuperscript{145} The restriction left open alternatives by allowing concerts that did not exceed the noise level regulations.\textsuperscript{146}

If a court finds that a speech restriction is content-based, it must apply strict scrutiny to the restriction in deciding its constitutionality.\textsuperscript{147} The restriction is constitutional only if it is narrowly tailored to advance an overriding government interest.\textsuperscript{148} That interest must be balanced against the free speech interests of the person speaking.\textsuperscript{149} When the restriction regulates political speech at the core of First Amendment protections, the court should apply exacting scrutiny to the regulation at hand.\textsuperscript{150} In \textit{Boos v. Barry},\textsuperscript{151} for example, restrictions on picketing near embassies in Washington, D.C. were found unconstitutional on their face.\textsuperscript{152} The Court held that restrictions targeted to protests against foreign governments are content-based restrictions.\textsuperscript{153} \textit{Boos} illustrates that if a content-based restriction is not narrowly tailored to serve a compelling state interest, then it is facially unconstitutional.\textsuperscript{154}

B. Constitutional Protections for Compelled Speech

Compelled speech cases invert the standard First Amendment dynamic, because instead of seeking the right to say something, the plaintiff desires to stay silent.\textsuperscript{155} In these cases, the speaker is compelled to make a statement or express support for a position he disagrees with. Because this is a violation of the freedom to speak without restriction, the regulations are inspected to see to what extent they interfere with the speaker’s First Amendment rights.\textsuperscript{156} When speakers are coerced into making statements

\begin{itemize}
  \item \textsuperscript{145} \textit{Id.} at 785, 802-03.
  \item \textsuperscript{146} \textit{Id.} at 802-03.
  \item \textsuperscript{147} \textit{Boos v. Barry}, 485 U.S. 312, 320-22 (1988).
  \item \textsuperscript{148} \textit{McIntyre v. Ohio Elections Comm’n}, 514 U.S. 334, 347 (1995) (applying the standard to core political speech).
  \item \textsuperscript{149} Christopher M. Schultz, \textit{Content-Based Restrictions on Free Expression: Reevaluating the High Versus Low Value Speech Distinction}, 41 \textit{ARIZ. L. REV.} 573, 576-78 (1999).
  \item \textsuperscript{150} \textit{McIntyre}, 514 U.S at 347 (citing First Nat’l Bank v. Bellotti, 435 U.S. 765, 786 (1978)).
  \item \textsuperscript{151} 485 U.S. 312 (1988).
  \item \textsuperscript{152} \textit{Id.} at 334 (“We conclude that the display clause of § 22-1115 is unconstitutional on its face. It is a content-based restriction on political speech in a public forum, and it is not narrowly tailored to serve a compelling state interest.”).
  \item \textsuperscript{153} \textit{Id.} at 321.
  \item \textsuperscript{154} \textit{Id.} at 334.
  \item \textsuperscript{155} Corbin, supra note 132, at 1282 (referring to \textit{West Virginia State Board of Education v. Barnett}, 319 U.S. 624 (1943), as a “paradigmatic example of unconstitutional compelled speech”).
  \item \textsuperscript{156} See generally id. (analyzing the modern, compelled-speech doctrine).
\end{itemize}
they do not agree with, there is a presumption that they are constitutionally invalid, like content-based restrictions.157

Instances where the government tries to compel statements are fewer than cases where support or association is compelled.158 Preventing a company from removing a canary compels the company to make a statement with which it does not agree. Further, that statement, informing debate on the scale and scope of surveillance requests, is of a type often valued highly under the First Amendment, as speech informing political debate.159 The canary is speech relevant to a political debate because, by showing which providers have been served with NSLs and FISA orders, it allows the public to realize the extent of law enforcement use of these authorities as the canaries disappear; the canaries are a way to fight the ability of the government to “distort the discourse” through misrepresentation.160

Supreme Court cases on compelled speech have largely concentrated on the First Amendment’s protection of freedom of mind and the importance of informed discourse to our society.161 Freedom of the press and the freedom to speak are so important because a democratic society depends on an informed populace. When a citizen is forced by the government to say something that he does not agree with, courts carefully inspect the reason for this compulsion, applying generally high standards of scrutiny and a searching inquiry into why the speech was compelled.162

First Amendment prohibitions of compelled speech protect democracy by allowing citizens to access information free from the distortion of government compulsion.163 In Pacific Gas and Electric Co. v. Public Utilities Commission of California,164 the Court was especially concerned about

157 Id. at 1283 (“The default rule is that as a content-based regulation, compelled speech must pass strict scrutiny.”).
159 Corbin, supra note 132, at 1295 (“The government could also distort the discourse by misrepresenting the true views of speakers. For example, if the government forces speakers to convey an opinion they disagree with, and if an audience believes that the message is the private speakers’ rather than the government’s, the audience may erroneously conclude that the message is more widespread than it really is.”).
160 Id.
162 See, e.g., Pac. Gas & Elec. Co. v. Public Utils. Comm’n, 475 U.S. 1, 16-17 (1986) (plurality opinion); Wooley, 430 U.S. at 716-17 (“Even were we to credit the State’s reasons and “even though the governmental purpose be legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved. The breadth of legislative abridgment must be viewed in the light of less drastic means for achieving the same basic purpose,” (quoting Shelton v. Tucker, 364 U.S. 479, 488 (1960))).
164 475 U.S. 1 (1986).
compelled speech that might distort public discourse.\textsuperscript{165} The Supreme Court held that compelled speech is antithetical to the free flow of information protected by the First Amendment.\textsuperscript{166} \textit{Pacific Gas} further protected the speaker’s right to remain silent, even when that speaker is a corporation.\textsuperscript{167} Canaries should then receive similar protections, as they illuminate the public discourse on government surveillance. As \textit{Pacific Gas} shows, the corporate identity of the speaker does not mean that the protections offered by the First Amendment are any less than those due to an individual.\textsuperscript{168}

The Court also recognized the fundamental personal right to refrain from expressing views one does not agree with in \textit{Wooley v. Maynard},\textsuperscript{169} and reiterated it twenty-some years later in \textit{Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston, Inc.} \textit{Wooley} is a paradigmatic compelled speech case concerning a motorist who objected, on religious grounds, to the “Live Free or Die” message on his New Hampshire license plate.\textsuperscript{170} The Supreme Court started its analysis with the First Amendment’s protection of the freedom of thought, including “both the right to speak freely and the right to refrain from speaking at all.”\textsuperscript{171} The right to refrain from giving voice to an opinion one did not share was tied to the important right of “individual freedom of mind,”\textsuperscript{172} covering facts as well as opinions.\textsuperscript{173} The Court again summed up the importance of protection against compelled speech in \textit{Hurley} by stating that “the principle of free speech is that one who chooses to speak may also decide what not to say.”\textsuperscript{174}

The content of the compelled speech also matters to the Court a great deal. In \textit{Riley v. National Federation of the Blind of North Carolina, Inc.},\textsuperscript{175} the Court held that mandating statements a speaker did not agree with could not help but alter the content of the speech.\textsuperscript{176} It then followed that this was a content-based regulation of speech, and therefore deserved a higher level of scrutiny.\textsuperscript{177} In \textit{West Virginia State Board of Education v. Barnette},\textsuperscript{178} the

\begin{itemize}
  \item \textsuperscript{165} See id. at 16.
  \item \textsuperscript{166} \textit{Id.} (citing Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 559 (1985)).
  \item \textsuperscript{167} \textit{Id.} (“Were the government freely able to compel corporate speakers to propound political messages with which they disagree, this protection would be empty, for the government could require speakers to affirm in one breath that which they deny in the next.”).
  \item \textsuperscript{168} \textit{Id.}
  \item \textsuperscript{169} 430 U.S. 705 (1977).
  \item \textsuperscript{170} \textit{Id.} at 715.
  \item \textsuperscript{171} \textit{Id.} at 714 (citing W. Va. State Bd. of Educ. v. Barnette, 319 U.S. 624, 633-34 (1943)).
  \item \textsuperscript{172} \textit{Id.} (quoting \textit{Barnette}, 319 U.S. at 637) (internal quotation marks omitted).
  \item \textsuperscript{175} 487 U.S. 781 (1988).
  \item \textsuperscript{176} \textit{Id.} at 795 (citing Miami Herald Publ’g Co. v. Tornillo, 418 U.S. 241, 256 (1974)).
  \item \textsuperscript{177} See id.
  \item \textsuperscript{178} 319 U.S. 624 (1943).
\end{itemize}
Court decided again that coercing acceptance of an idea, such as requiring students to pledge allegiance to the flag, went beyond the limitations of the Constitution.\textsuperscript{179} Later, in \textit{Thomas v. Collins},\textsuperscript{180} Justice Jackson referenced \textit{Barnette} in his concurrence stating that the First Amendment prevented a public authority from “assuming a guardianship of the public mind” through regulation of speech.\textsuperscript{181}

The Court has expanded the right to free and unrestricted thought through these cases. It also developed an extensive jurisprudence covering the right to refuse to say anything that one does not agree with.\textsuperscript{182} This area of First Amendment jurisprudence covers cases where speech is attributed to the plaintiff, involves association, or concerns access.\textsuperscript{183} In deciding compelled speech cases, the Court takes into consideration whether the statement was made by the plaintiff or if the plaintiff was merely granting access to the public to make its own statements.\textsuperscript{184}

This distinction is illustrated in two cases. In \textit{PruneYard Shopping Center v. Robins},\textsuperscript{185} the public could pass out leaflets without having it appear that the shopping center owner was behind the speech.\textsuperscript{186} In \textit{Hurley}, however, the Court allowed a parade organizer to exclude a gay and lesbian group from a parade.\textsuperscript{187} Marching in a parade, as opposed to passing out leaflets in a shopping center, appears more like a form of endorsement.\textsuperscript{188} Treating the parade organizer as an endorser of all messages carried by the parade participants impinges on the organizer’s right to proffer only messages he agrees with. He is compelled to speak a message he does not agree with, in such a way that the public perceives it as being one he agrees with. Contrast this with the shopping center owner in \textit{PruneYard} objecting to the public passing out information at his store.\textsuperscript{189} If the owner did not agree with the messages being passed out, he was free to pass out his own literature promoting his own point of view.

The common thread through many of these compelled speech cases is that the Court generally views compelled speech as a type of content-based speech restriction, and is suspicious of speech that clouds public debate on

\textsuperscript{179} Id. at 641.
\textsuperscript{180} 323 U.S. 516 (1945).
\textsuperscript{181} Id. at 545 (Jackson, J., concurring).
\textsuperscript{184} Id. at 467-68.
\textsuperscript{185} 447 U.S. 74 (1980).
\textsuperscript{186} Id. at 87.
\textsuperscript{187} \textit{Hurley}, 515 U.S. at 573.
\textsuperscript{188} See id. at 576-77; Greene, supra note 183, at 468.
\textsuperscript{189} Greene, supra note 183, at 468.
issues of public policy. Therefore, there is a general presumption that compelled speech is constitutionally invalid, like content-based restrictions.\textsuperscript{190}

C. \textit{Prior Restraints}

Prior restraints are similar to content-based speech restrictions, falling under strict scrutiny as speech regulations predicated on the nature of what is spoken, rather than when or where.\textsuperscript{191} They are regulations based on blocking speech before it occurs, and therefore interfere with First Amendment rights to speak freely. These speech restrictions regulate speech by requiring court approval before making a statement.\textsuperscript{192} These injunctions are in conflict with the liberty of speech granted by the First Amendment, and are thus subject to close inspection. Because of the stifling effect of prior restraints, they are seen as more restrictive than a system of subsequent punishment.\textsuperscript{193}

In \textit{Near v. Minnesota ex rel. Olson},\textsuperscript{194} the Court established a presumption against prior restraints.\textsuperscript{195} While it did not grant total immunity,\textsuperscript{196} there is a presumption that these restrictions are in conflict with the aims of the First Amendment.\textsuperscript{197} Because of this, they have been characterized as coming with a heavy presumption against constitutional validity,\textsuperscript{198} and the government therefore must bear the burden of justifying the restraint.\textsuperscript{199} Found to be “the most serious and the least tolerable infringement on First

\begin{flushright}


\textsuperscript{192} \textit{Id}. at 654.


\textsuperscript{194} 283 U.S. 697 (1931).

\textsuperscript{195} \textit{Id}. at 707; Emerson, \textit{supra} note 191, at 653.

\textsuperscript{196} National security concerns are one restriction recognized by the Court. \textit{Near}, 283 U.S. at 716 (“When a nation is at war many things that might be said in time of peace are such a hindrance to its effort that their utterance will not be endured so long as men fight and that no Court could regard them as protected by any constitutional right.” (quoting Schenck v. United States, 249 U.S. 47, 52 (1919))).

\textsuperscript{197} See \textit{id}. at 716-17 (“The exceptional nature of its limitations places in a strong light the general conception that liberty of the press, historically considered and taken up by the Federal Constitution, has meant, principally although not exclusively, immunity from previous restraints or censorship. . . . That liberty was especially cherished for the immunity it afforded from previous restraint of the publication of censure of public officers and charges of official misconduct.”).


\end{flushright}
Amendment rights,” they cast a chilling effect that can dampen and distort the vibrant discourse the First Amendment seeks to protect.

Although national security concerns are one of the justifications for prior restraint recognized by the Court, the Pentagon Papers case shows that it is not a foregone conclusion that national security concerns will merit this level of restriction. While the Pentagon Papers case is a “high-water mark” in protection of First Amendment rights against national security concerns, courts engaged in strict scrutiny of a prior restraint must balance the government’s interest against the restraint. The Court engaged in such a balancing with the Pentagon Papers in *New York Times Co. v. United States* when two newspapers fought to publish contents of classified studies on the Vietnam War. The newspapers won a victory for free speech when the Court found the prior restraint unconstitutional and “bearing a heavy presumption against its constitutional validity.” This strict test for prior restraints comes with the thumb on the scales of unconstitutionality, because the muzzling effect is considered especially detrimental to the functioning of a democratic society.

Not all analysis of prior restraints is strict. In some cases, prior restraints are upheld because they protect important government functions—such as grand jury proceedings or Judicial Review Councils (“JRC”), such as in *Kamasinski v. Judicial Review Council*. *Kamasinski* upheld a prior restraint.

---

202 This is a common shorthand for the landmark case *New York Times Co. v. United States*, 403 U.S. 713 (1971) (per curiam). See, e.g., Redish, supra note 201, at 69.
203 *N.Y. Times Co.*, 403 U.S. at 719 (Black, J., concurring) (“To find that the President has ‘inherent power’ to halt the publication of news by resort to the courts would wipe out the First Amendment and destroy the fundamental liberty and security of the very people the Government hopes to make ‘secure.’ No one can read the history of the adoption of the First Amendment without being convinced beyond any doubt that it was injunctions like those sought here that Madison and his collaborators intended to outlaw in this Nation for all time.”).
206 403 U.S. 713 (1971) (per curiam).
207 Id. at 714.
209 See *Thomas v. Collins*, 323 U.S. 516, 543 (1945) (“The restraint is not small when it is considered what was restrained. . . . There is some modicum of freedom of thought, speech and assembly which all citizens of the Republic may exercise throughout its length and breadth, which no State, nor all together, nor the Nation itself, can prohibit, restrain or impede.”).
210 See *Haig v. Agee*, 453 U.S. 280, 307-09 (1981) (noting that “no governmental interest is more compelling” than national security and that the partly content-based restriction on the respondent was the only option available to the government).
211 44 F.3d 106 (2d Cir. 1994).
restraint because the plaintiff’s interest in disclosing information gained from a JRC was outweighed by the state’s interest in carrying out confidential JRC investigations. Confidentiality in these proceedings promotes important interests and efficient investigation of potential misconduct, but these restrictions are time-bound, and valid only so long as the investigation remains active.

1. Nondisclosure Provisions as Prior Restraints

The nondisclosure provisions of NSLs were litigated as prior restraints on speech several times. In *Doe v. Gonzales*, although the court vacated the district court’s decision and remanded the case to consider changes to 18 U.S.C. § 2709(c), Justice Cardamone wrote a concurrence addressing the First Amendment ramifications of § 2709(c), the ECPA’s NSL nondisclosure rule. He addressed the problem of balancing the government’s national security concerns, particularly protecting its investigative processes, against the speech restriction in § 2709. The plaintiffs were especially concerned by the nondisclosure provision because the investigations were seen as “permanent and unending.” They argued that only allowing the NSL recipients to disclose a § 2709 request after the close of the investigation would be tantamount to preventing them from ever sharing that information.

Justice Cardamone wrote of the difficulty of the “shroud of secrecy in perpetuity” that he sees as “antithetical to democratic concepts” and the First Amendment. He quoted *New York Times Co.*, where Justice Black explained, “The word ‘security’ is a broad, vague generality whose contours should not be invoked to abrogate the fundamental law embodied in the First Amendment.” Further quoting Justice Black’s admonition that “guarding of military and diplomatic secrets at the expense of informed representative government provides no real security for our Republic.”

---

212 Id. at 111-12.
213 See id. at 112.
214 Id.
215 449 F.3d 415 (2d Cir. 2006) (per curiam).
216 Id. at 421 (Cardamone, J., concurring).
217 Id. at 422.
218 Id.
219 Id. at 421-22.
220 Id. at 422.
221 *Doe*, 449 F.3d at 423 (Cardamone, J., concurring) (quoting *N.Y. Times Co. v. United States*, 403 U.S. 713, 719 (1971) (Black, J., concurring)) (internal quotation marks omitted).
222 Id. (quoting *N.Y. Times Co.*, 403 U.S. at 719 (Black, J., concurring)) (internal quotation marks omitted).
Justice Cardamone recognized that casting civil liberties by the wayside in pursuit of counterterrorism investigations would lead to a hollow victory.

Would breaking a single nondisclosure order, NSL- or FISA-based, threaten the sources and methods they are designed to protect? The DOJ has relied on the argument that the nondisclosure orders are meant to protect classified information, and so they decline to provide much concrete information about the impact of disclosure on their investigations.\(^{223}\) FISA restrictions on ISPs (or software companies or other providers) are upheld because the FISC issues a nondisclosure order to protect classified information.\(^{224}\) That this information is classified likely means that it is important to some ongoing investigation, and therefore is the type of information that courts might protect against a First Amendment challenge. If the DOJ can show that the nondisclosure orders are serving the compelling government interest of national security, that they are the least restrictive means of achieving that protection, and that they are narrowly tailored to that aim, the courts might allow the restrictions to stand based on the importance of national security interests.

Courts have weighed whether the compelling interest in national security is strong enough to overcome the high bar of strict scrutiny’s least restrictive and narrowly tailored tests several times. Relevant to NSLs, the question of the constitutionality of the ECPA’s § 2709 provision came to courts in In re National Security Letter\(^{225}\) and the revisiting of Doe in 2008—the renamed John Doe, Inc. v. Mukasey.\(^{226}\) In the John Doe, Inc. case, the NSL recipient once again challenged the nondisclosure requirement, arguing that it was a prior restraint.\(^{227}\) The court distinguished it from some earlier prior restraint cases that regulated public speakers or movie distributors, but also rejected analogies to grand jury proceedings or judicial misconduct cases like Kamasinski, where prior restraints had been upheld.\(^{228}\) The court differentiated the prior restraint at hand from grand jury secrecy by noting that NSL provisions are imposed by statute, while in a grand jury hearing, “interests in secrecy arise from the nature of the proceeding.”\(^{229}\) The court characterized the district court as having noted that the nondisclosure restriction strikes at “the core of the First Amendment” by restraining political criticism.\(^{230}\) The court ruled that § 2709’s nondisclosure requirements should be subject to a meaningful, post-issuance judicial

\(^{223}\) See Reply Memorandum in Further Support of Defendants’ Partial Motion to Dismiss at 6-7, Twitter, Inc. v. Holder, No. 14-cv-4480 (N.D. Cal. Mar. 31, 2015).

\(^{224}\) See id. at 12-13.


\(^{226}\) 549 F.3d 861 (2d Cir. 2008).

\(^{227}\) Id. at 866.

\(^{228}\) Id. at 876.

\(^{229}\) Id. at 877.

\(^{230}\) Id. at 870.
review.\textsuperscript{231} The court held this was wholly lacking with the law’s requirement that courts must accept as “conclusive” government officials’ good-faith certification of the need for a nondisclosure order under 18 U.S.C. § 3511—\textsuperscript{232}a rule added with the passage of the USA PATRIOT Improvement and Reauthorization Act of 2005.\textsuperscript{233}

Since the later-passed USA FREEDOM Act allows publication in bands of counts of NSLs, it is not clear whether earlier rulings that the NSL non-disclosure provisions are prior restraint still stand.\textsuperscript{234} But as noted in Part II, instead of the original flat prohibition on any disclosure, recipients of NSLs may now discuss the letters with an attorney and may more meaningfully challenge the nondisclosure provisions in a court.\textsuperscript{235} Some other questions remain. If a provider launches a new service with a zero-count warrant canary, as Electronic Frontier Foundation’s (“EFF”)\textsuperscript{236} new certificate authority\textsuperscript{237} has done,\textsuperscript{238} must they launch with a transparency report that states that they have received 0-249 NSLs? Or may the provider, as EFF has done, publish a transparency report listing “0” as the count for all data request types?\textsuperscript{239}

\textsuperscript{231} Id. at 882 .

\textsuperscript{232} John Doe, Inc., 549 F.3d at 882 (“There is not meaningful judicial review of the decision of the Executive Branch to prohibit speech if the position of the Executive Branch that speech would be harmful is “conclusive” on a reviewing court, absent only a demonstration of bad faith.”). Congress later replaced the entire subsection containing the language to which the John Doe, Inc. court objected. 18 U.S.C. § 3511(b) (2012), amended by USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 502(g), 129 Stat. 268, 288-89.

\textsuperscript{233} Pub. L. No. 109-177, § 115, 120 Stat. 192, 211-13; see also DOYLE, supra note 44, at 5.

\textsuperscript{234} See supra Part II.B.1.

\textsuperscript{235} The new language in the 2015 USA FREEDOM Act significantly departed from the original language of the USA PATRIOT Act’s 2008 reauthorization. \textit{Compare} USA FREEDOM Act § 502(g), 129 Stat. at 289 (instructing district courts under § 3511(b)(1)(C) and § 3511(b)(3) to issue a nondisclosure order only if the “court determines that there is reason to believe” that it is necessary and then to include in the order “conditions appropriate to the circumstances”), \textit{with} USA PATRIOT Improvement and Reauthorization Act § 115, 120 Stat. at 212 (requiring courts under § 3511(b)(2) to accept “as conclusive” any good-faith certification by administration officials that disclosure would endanger national security or meet any other qualifying condition).

\textsuperscript{236} \textit{About EFF, ELECTRONIC FRONTIER FOUND.}, https://www.eff.org/about (last visited Jan. 5, 2016).


\textsuperscript{239} Mike Masnick, \textit{Let’s Encrypt Releases Transparency Report—All Zeroes Across The Board}, TECHDIRT (July 2, 2015, 6:18 PM), https://www.techdirt.com/articles/20150702/17014131521/lets-encrypt-releases-transparency-report-all-zeroes-across-board.shtml (“This is actually pretty important
the count for all data types, and then receives a NSL, may it still un-publish the zero count for that data type, even though the 0-249 options now exists? Alternatively, may it update their zero count to the “0-249” count now that the zero count is inaccurate? Either one of these actions would be enough to tip off a careful monitor that the provider received at least one NSL.

Prohibiting a company that is not subject to any NSLs or FISA orders from releasing a zero-count warrant canary, however, blocks speech before it occurs without a narrowly-tailored compelling government interest to outweigh the burden. Such a restraint would fail to be narrowly tailored because it would apply to all companies that wanted to publish words to the affect of “we have received zero NSLs,” regardless of whether they had or might foreseeably be served with one. Similarly, the restraint fails to protect a compelling government interest, because none of these companies have information that has been requested in a particular investigation. The restraint would therefore be to protect more broadly-drawn, fuzzy goals of protecting information requested from other providers, a type of vague government goal that courts are likely to find hard to uphold.

In re National Security Letter concerned an unnamed company that received a NSL requesting subscriber information. The company brought suit challenging the nondisclosure provision in the Northern District of California. The plaintiff argued that the nondisclosure provision, § 2709(c), was a prior restraint and a content-based speech restriction that could only be upheld if it was preventing “direct, immediate, and irreparable damage” to the country. Going a step further than the Second Circuit in John Doe, Inc., the district court found that § 2709(c), as a prior restraint, was unconstitutional. The court also held that the nondisclosure provision was a restriction on speech about government conduct, one that should be narrowly tailored to serve a compelling government interest. The government appealed, and the Ninth Circuit recently vacated the district court’s decision and remanded to reconsider the plaintiff’s challenge in light of the changes for a variety of reasons. First, it clearly acts as something of a warrant canary. And by posting this now, before launch and before there’s even been a chance for the government to request information, Let’s Encrypt is actually able to say “0.”

241 Id.
242 Id. at 1071 (quoting N.Y. Times Co. v. United States, 403 U.S. 713, 730 (1971) (Stewart, J., concurring)) (internal quotation marks omitted).
243 Id. at 1081.
244 See, e.g., id. Twitter also recently filed suit seeking to publish clearer transparency reports, also arguing that they are prior restraint of speech. Meghan Graham, Twitter is Suing the US Government in an Effort to Reveal Surveillance Information, JUST SECURITY (Oct. 8, 2014, 4:39 PM) http://justsecurity.org/16126/twitter-suing-government-effort-reveal-surveillance-information/; Lee, supra note 63.
to § 2709 and § 3511 effected by the USA FREEDOM Act.\textsuperscript{245} As of the publication of this Comment, the follow-on litigation is still pending. National security interests are certainly among the most compelling government interests, and disclosure of sources and methods might cripple future investigations. Protecting critical debate, however, is also a vital government interest in a democracy.

D. Commercial Speech Protections

Not all speech receives the same level of protection under the First Amendment. One category of speech generally held to be deserving of less protection is commercial speech.\textsuperscript{246} While corporations have the right to “discussion, debate, and the dissemination of information and ideas that the First Amendment seeks to foster,”\textsuperscript{247} some of their speech will not be of the type the First Amendment primarily seeks to protect.\textsuperscript{248} But areas of lower protection are only created as carve-outs from the general presumption that all speech deserves equal First Amendment protection.\textsuperscript{249}

Commercial speech is defined narrowly as speech proposing a commercial transaction.\textsuperscript{250} After recognizing that some commercial speech should receive First Amendment protections in \textit{Virginia State Board of Pharmacy v. Virginia Citizens Consumer Council, Inc.},\textsuperscript{251} the Supreme Court developed a four-part test for commercial speech in \textit{Central Hudson Gas & Electric Corp. v. Public Service Commission of New York}\textsuperscript{252} to


\textsuperscript{249} Geoffrey R. Stone, \textit{Content Regulation and the First Amendment}, 25 WM. & MARY L. REV. 189, 194 (1983) (arguing that the Court “creates areas of nonprotection only after it affirmatively finds that a particular class of speech does not sufficiently further the underlying purposes of the first amendment”).


\textsuperscript{251} 425 U.S. 748 (1976).

\textsuperscript{252} 447 U.S. 557 (1980).
weigh the protection for the speech despite its commercial nature.253 First, the Court decides if the speech is lawful or misleading, as either classification will disqualify it from First Amendment protection.254 If the commercial speech seeking protection is not false, deceptive, and does not relate to illegal acts, then the government interest is weighed.255 Speech restrictions in service of a substantial government interest are allowed, but only if they directly advance that interest and the restriction is not overbroad.256 The Court has thus upheld protection for many kinds of commercial speech, especially if the speech aims to inform or enlighten consumers.257

The Court pays special attention to cases where commercial speech bans seek to advance non-speech related policy goals, as they can hide government policies from the public.258 The dangers of restricting truthful commercial speech259 worry the Court because these restrictions are generally aimed at hiding government policies that could only be put in place while restricting speech.260 Justice Thomas, for instance, has concurred in judgments based on the Central Hudson test, but objected to its use in products labeling or similar cases because he believes it may be used to keep consumers ignorant.261

Courts have also recognized that there is not always a clear dividing line between commercial and noncommercial speech. In Riley, the commercial speech was “inextricably intertwined” with protected speech, and thus was treated as a whole that would be subject to exacting scrutiny.262 When corporations engage in speech critical of government programs, their speech is not the same as when they seek to sell products or promote their services; speech critical of government programs is closer to the heart of the type of speech necessary for a democracy that the First Amendment sought

253 Id. at 566; Kozinski & Banner, supra note 250, at 631.
254 Cent. Hudson, 447 U.S. at 566 (“In commercial speech cases, then, a four-part analysis has developed. At the outset, we must determine whether the expression is protected by the First Amendment. For commercial speech to come within that provision, it at least must concern lawful activity and not be misleading. Next, we ask whether the asserted governmental interest is substantial. If both inquiries yield positive answers, we must determine whether the regulation directly advances the governmental interest asserted, and whether it is not more extensive than is necessary to serve that interest.”).
256 Id.
259 Id. at 502.
260 Id. at 503 (“In this way, these commercial speech bans not only hinder consumer choice, but also impede debate over central issues of public policy.”).
to protect. Similarly, speech by commercial entities that touches on public policy issues is treated differently than speech aimed primarily at making a sale.\textsuperscript{263} The Court has moved from rigid rules classifying all speech by commercial entities as low in value to the more nuanced view today, a view that takes policy concerns into consideration.\textsuperscript{264}

Each of these areas of First Amendment jurisprudence will come into play when courts consider warrant canaries. Communications providers might classify them as a prior restraint, due to the speech restriction of the nondisclosure provision, or commercial speech. The next Part explores how these First Amendment protections apply to warrant canaries.

IV. FIRST AMENDMENT PROTECTIONS FOR WARRANT CANARIES

When courts take up consideration of whether a company may take down its canary, they must weigh national security concerns against First Amendment protections for freedom of speech. When canaries act as criticism of government policies, they sometimes move beyond commercial speech into a protected zone of core First Amendment speech entitled to greater protection, especially where society has a “strong interest in the free flow of commercial information.”\textsuperscript{265}

Compelling a corporation to leave a canary up leads it to make an affirmative statement that it does not wish to make. Part IV.A considers how a canary becomes a type of compelled speech and argues that it is strikingly similar to the compelled speech found unconstitutional in Wooley.\textsuperscript{266} Part IV.B explores how government objections to removing canaries are content-based speech restrictions, as the message of the canary is the source of the government’s speech restriction. Finally, Part IV.C addresses how restricting a company from removing a canary is a prior restraint. For these reasons, compelled publication of the canaries must be analyzed under strict scrutiny as protected First Amendment speech.

A. Coercing a Company to Keep Up a Canary is Compelled Speech

Once a company with a warrant canary receives a law enforcement request that it believes trips its canary, it should not be coerced into publishing a false canary. Publication of a canary is an act of speech; therefore publication of a canary coerced by the government, in order to hide a NSL

\textsuperscript{263} See Kozinski & Banner, supra note 250, at 634-35.


or FISA order, is compelled speech. The First Amendment offers protections from compelled speech, especially when the government attempts to elicit a direct statement from the speaker.\(^{267}\)

The compelled publication of a canary is most like *Wooley*, and the same sort of analysis should be applied. In *Wooley*, the Court protected a New Hampshire resident from having to proclaim, via his state-issued license plate, a statement he did not agree with.\(^{268}\) The Court in *Wooley* was especially uncomfortable with the invasion of “the sphere of intellect” the First Amendment was meant to protect.\(^{269}\) Like the motorist who did not want his license plate to carry the message “Live Free or Die,” an ISP served with a NSL can object to publishing a canary that is no longer truthful.

The issues raised by compelling the publication of a false canary are similar to the ones discussed in *Thomas*. That is, the public should be concerned about authorities that seek to “assum[e] a guardianship of the public mind,” and frame the debate on their terms.\(^{270}\)

If a service provider wishes to launch with a zero-count canary, they should be free to do so, as there are not, at that point, any active government investigations that would be implicated by the provider’s canary. If such a provider is served with a NSL, however, and wishes to take down their canary, can they be compelled to leave it up under the new disclosure rules announced in the USA FREEDOM Act?

The bands envisioned in that Act presume that a provider wishes to signal that it was served with a NSL, thus engaging in protected speech about government surveillance. The government’s position might be that there is no compelled speech at play, as a service provider may either publish nothing (and therefore follow the nondisclosure order through total silence) or publish the allowable bands; this set of choices allows a speaker to say what they wish without violating the law. Removing a zero-count canary would signal to observers that the service provider received at least one request, likely violating the zero based bands of disclosure. However, the provider may be caught in a catch-22 bind if it converts its original zero-count warrant canary to a new zero-based-band canary; observers may deduce that the provider has now been served with at least one NSL.

Coercion to make an affirmative statement one does not agree with is deeply unsettling. In *Barnette*, the Court protected a citizen from being compelled “to utter what is not in his mind.”\(^{271}\) Similarly, a service provider required to publish a tripped canary is being compelled to publish to the

---

\(^{267}\) See id. at 714-15.

\(^{268}\) Id. at 715.


\(^{271}\) *Barnette*, 319 U.S. at 634.
world something that “is not in [its] mind.” Like the small town with the “no searches here” signs, the provider will see deception in every canary still up. The government’s ability to control the debate by stifling the free flow of information about the extent of these programs is troubling. By compelling the parties they seek information from to stay silent, the government distorts the public debate in a way that should be deeply disturbing to those who value dissent and democratic ideals.

A question arises concerning whether the freedom to refrain from speaking extends to the right to create a situation by speaking and then silencing oneself. The provider should have the right to publish the canary in the first place, lest he be bound by a prior restraint on his speech. However, while the original publication may be protected by the First Amendment’s prior restraint doctrine, may he seek refuge in the compelled speech doctrine for being required to repeat speech he willingly made originally? After all, Wooley envisioned a situation where the government elicited a direct statement from the speaker without the speaker’s complicity in the creation of that speech. But the service provider publishing a canary is no such third party with speech pushed onto him by the government without his involvement. This Comment argues that the speaker should not be forced to waive his protection against speech restrictions in the future. The speaker is not merely being required to imply support for a cause or association with a group; he is required to profess a factual statement he no longer agrees with.

As in Pacific Gas, where a corporation’s right to remain silent rather than “propound [a] political message[] with which [it] disagree[s]” was upheld, a service provider’s compelled canary publication might distort the political discourse. The Court in Pacific Gas feared that even in the face of a legitimate government purpose for compelling speech, the broad trampling of personal liberties could not be allowed. Protecting sources and methods by hiding those service providers that have received a NSL is a legitimate and substantial interest, but it must still be balanced against the right to speak, or not speak, one’s mind.

The distinction between PruneYard and Hurley is particularly relevant for analysis of a canary, as the autonomy of the speaker is at issue in the same way that the parade organizers’ autonomy as speakers was threatened. The PruneYard and Hurley cases were decided differently because of the public’s perception of who the speaker is. While the shopping center owner in PruneYard has the ability to publicize his own views if he does not agree with those leafleting at his store, a software company compelled

---

272 Id.
273 Wooley, 430 U.S. at 713.
275 See id. at 17-18.
276 Greene, supra note 183, at 468.
to leave up a canary cannot speak in opposition to the message it is forced to carry. It is more like the parade organizer in Hurley, compelled to carry a message he objects to, while the public will implicitly assumes he agrees with it.

B. Requiring a Canary to Stay on a Website is a Content-Based Restriction of Speech

In addition to meriting a higher standard of review despite roots in commercial speech, canaries are due more scrutiny as content-based restrictions. Rather than a regulation based on less problematic grounds such as a time, place, or manner restriction,277 canaries are regulated solely on the content of their message. Regulation of speech based on the content of the message, rather than time or place, is granted the highest level of scrutiny by the courts.278

When the government opposes a change to a zero-count canary, it makes a content-based objection. While the government on one hand appears to have few complaints about the publication of warrant canaries that have not gone off—rsync.net, for one, has been publishing their warrant canary with seemingly no interruption for several years—they have objected to other potential canaries.279 Therefore, it might at first appear unclear whether the government’s objection to the removal of a sentence from a website is a content-based restriction or a content-neutral one. Consider, though, that the government would not object to the removal of a company’s lunch menu from their website. Therefore, it seems plain that this is a content-based restriction, rather than the time, place or manner restrictions allowed under content-neutral regulation of speech.280

In other words, the text of the warrant canary is specific content. The government would not seek to impose the publication of nonsense; they care about the message a disappearing canary would carry. Control of a

---

277 Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 771 (1976) (“There is no claim, for example, that the prohibition on prescription drug price advertising is a mere time, place, and manner restriction. We have often approved restrictions of that kind provided that they are justified without reference to the content of the regulated speech, that they serve a significant governmental interest, and that in so doing they leave open ample alternative channels for communication of the information.”).


280 Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (stating that the government may impose time, place and manner restrictions that are content neutral).
canary’s presence is not a regulation independent of the specific content of the speech at issue. Although control of a canary is meant to promote a specific government interest, that of national security, it does not leave open alternatives, as required under Ward v. Rock Against Racism.281

Given this distinction, it appears that the courts should follow the standard test of strict scrutiny for content-based restrictions, as put forth in Riley.282 There the Supreme Court held that compelled speech was “subject to exacting First Amendment scrutiny” because of the content-based nature of the speech restriction.283 The level of scrutiny afforded content-based speech restrictions284 has long been established and continues to be the standard used by cases today.285

C. Transparency Reports and Canaries Are Not Mere Commercial Speech

As noted previously, commercial speech can be narrowly construed as speech proposing a commercial transaction,286 which canaries do not do. Even if one cynically derides transparency reports as a form of advertising, by presenting this data, the companies are contributing to an ongoing public debate about the adaptation of the Fourth Amendment to online communications and the bounds of computer-assisted government surveillance. Transparency reports, and the canaries within them, are more than proposals to buy a product.

Counts of warrants and subpoenas bear on the public debate about the Fourth Amendment, but canaries go beyond that to illuminate a part of the government’s surveillance program shrouded in mystery. As perhaps the only way the public at large can learn when and where these requests are made on their behalf, canaries are part of a public debate about the bounds of government behavior.287

281 Id.
283 Id. at 798.
285 See McCullen v. Coakley, 134 S. Ct. 2518, 2529 (2014) (“In particular, the guiding First Amendment principle that the ‘government has no power to restrict expression because of its message, its ideas, its subject matter, or its content’ applies with full force in a traditional public forum. As a general rule, in such a forum the government may not ‘selectively . . . shield the public from some kinds of speech on the ground that they are more offensive than others.’” (citation omitted) (quoting Erznoznik v. Jacksonville, 422 U.S. 205, 209 (1975); Police Dep’t v. Mosley, 408 U.S. 92, 95 (1972))).
287 N.Y. Times Co. v. United States, 403 U.S. 713, 728 (1971) (Stewart, J., concurring) (discussing that an important restraint upon executive power is an informed citizenry, which is a product of a free and informed press).
Brad Smith, Microsoft’s General Counsel and Executive Vice President of Legal and Corporate affairs, recently spoke on government surveillance and articulated the criticism of surveillance that these companies engage in:

[T]he one asset that the US has which is even stronger than our military might is our moral authority. And this decline in trust has not only effected people’s trust in American technology products. It has affected people’s willingness to trust the leadership of the United States. If we are going to win the war on terror. If we are going to keep the public safe. If we are going to improve American competitiveness, we need Congress to stay on the path it’s set.288

Although the speech might be commercial in nature, if it articulates government criticism of the amount and scope of warrantless wiretapping and surveillance, it deserves strong First Amendment protections.289 The “enlightened citizenry” is protected not just by a robust press, but by companies engaging in the dialog through transparency reports, acting as an “effective restraint upon executive policy.”290

Warrant canaries, in this way, transcend their commercial nature by showing the extent of government surveillance. If the government is allowed to restrict their removal, the public loses a chance learn the scope of customer data requested in investigations. Without understanding the scale of these programs, it is harder to debate their effectiveness and more difficult to weigh whether our society is willing to trade off security gains against the intrusion.291

There have been calls for more data illuminating the scale and scope of government surveillance and data requests to ISPs and technology companies.292 This data, which canaries can provide, is like the publically in-

289 N.Y. Times Co., 403 U.S. at 728 (Stewart, J., concurring) (“In the absence of the governmental checks and balances present in other areas of our national life, the only effective restraint upon executive policy and power in the areas of national defense and international affairs may lie in an enlightened citizenry—in an informed and critical public opinion which alone can here protect the values of democratic government. For this reason, it is perhaps here that a press that is alert, aware, and free most vitally serves the basic purpose of the First Amendment. For without an informed and free press there cannot be an enlightened people.”).
290 Id.
291 Julian Sanchez, Can We Do Without National Security Letters?, JUST SECURITY (Jan. 9, 2014, 8:15 AM), http://justsecurity.org/5351/national-security-letters/ (“[I]t seems at least as plausible to suppose that when communications and financial records can be vacuumed up subject to a vague and permissive standard with little in the way of external checks, investigators will tend to err on the side of overcollection.”).
292 Soghoian, supra note 57, at 230-31 (explaining the difficulties in understanding the number of requests to companies).
formative aspect of the advertising considered valuable in *Virginia Pharmacy*, valuable because it informed the population, much as canaries do. As in *Virginia Pharmacy*, where the Court broke new ground and first found that commercial speech was entitled to First Amendment protections, based on the value of the free flow of information in our society, the information conveyed by warrant canaries is not mere information about a commercial transaction.

Warrant canaries are meant to win back consumer trust. Warrant canaries also foster debate and remind the public about nondisclosure orders that accompany surveillance orders. Warrant canaries serve a valuable role in the public discourse, but this value needs to be weighed against the substantial government interest in prosecuting criminal acts and pursuing counterterrorism investigations.

As in *Riley*, where the commercial speech was inextricably intertwined with protected speech, transparency reports and canaries can extend beyond their commercial roots. The nature of the speech as a complete body must be taken into consideration, especially when, as in *Riley*, we are considering the effect of publication of a compelled statement within it. The key characteristic of the speech in *Riley* was that the speech was coerced, and the so-

---

294 Id. at 762.
295 Id. at 762-63.
296 Kopstein, supra note 8 (noting the recent growth of distrust in American technology companies).
298 Critics have paid close attention to NSL canaries in particular because of concerns about the lack of judicial oversight. See *National Security Letters*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/national-security-letters (last visited Jan. 6, 2016) (“These letters served on communications service providers like phone companies and ISPs allow the FBI to secretly demand data about ordinary American citizens’ private communications and Internet activity without any meaningful oversight or prior judicial review.”); *About Apple’s Dead Warrant Canary*, EMPTYWHEEL (Sept. 18, 2014), https://www.emptywheel.net/2014/09/18/about-apples-dead-warrant-canary/.
299 Roberts, supra note 68.
cial goals could be met by other, less restrictive means. The compelled nature of the speech in *Riley* meant that the Court used a heightened scrutiny factor, while most commercial speech cases use only an intermediate scrutiny standard. *Riley* therefore applied a heightened standard to the speech at hand due to these factors, and so should courts when considering requiring the continued publication of a tripped canary.

1. Applying the *Central Hudson* Test

Even if the courts decide that canaries should be analyzed as commercial speech, the *Central Hudson* test shows that they should receive protection. The *Central Hudson* test was developed by the Supreme Court to analyze commercial speech cases. It is used when the speech is primarily proposing a commercial transaction. The *Central Hudson* test grants intermediate scrutiny. If warrant canaries are seen more as a service provider’s advertising than as criticism of government surveillance, they would be entitled some protection because commercial speech is not entirely without First Amendment protections.

Applying the *Central Hudson* test to the use of warrant canaries shows that they are entitled to protection. The first factor is whether the speech is illegal or misleading, but although it is technically misleading to have a zero-count canary up after receiving a NSL, that technicality should be disregarded. Without the nondisclosure provision blocking the removal of a tripped canary, the ISP would speak truthfully by taking down their tripped canary. The government should therefore not be able to take advantage of the misleading factor by requiring a lie, and then wielding the *Central Hud-
son test’s misleading prong. Any ISP who publishes a warrant canary that is later tripped by receipt of a NSL should not be caught in a paradox of a misleading situation it did not create.

If the restriction is not found to be misleading, then the next prong of Central Hudson requires that restrictions directly support a substantial government interest.\textsuperscript{310} When weighing speech restrictions, whether commercial or not, courts consider national security concerns to be especially vital.\textsuperscript{311} Here the government interest promoted by the nondisclosure provisions of NSLs and FISA orders, which canaries evade, stems from the need to protect sources and methods, as well as to prevent targets from realizing they are under surveillance.\textsuperscript{312} Investigators fear that if an ISP or other company announces they received a NSL, suspects using that service provider will be tipped off, and might flee to another provider with an un-tripped canary.\textsuperscript{313}

How should a court balance these national security concerns with the free flow of information? When the government seeks to prevent an ISP from removing a warrant canary, they are unfairly suppressing the free speech rights of the ISP, and distorting the public discussion about surveillance. Removing a warrant canary from a website will not “incite an immediate breach of the peace.” Instead, it will contribute only a small piece of information to the national debates on adapting the Fourth Amendment to electronic communications and the use of various statutory authorities by law enforcement to request information from providers.

The courts will then move to the next step of the Central Hudson analysis, where government “must assert a substantial interest to be achieved by [the] restriction[,]” directly advanced by that restriction and unable to be met in any other more limited way.\textsuperscript{315} The national security interest in forcing a canary to stay up is aimed primarily at protecting ongoing investigations as well as protecting broader law enforcement interests in hiding sources and methods.\textsuperscript{316} Under Central Hudson, there must be a close connection between the government interests protected by the regulation and the speech restricted by this regulation.\textsuperscript{317} Ongoing investigations might be more impaired by the removal of a canary at a small ISP with only a few customers. It seems unlikely, however, that the removal of a canary at a

\textsuperscript{311} See, e.g., Haig v. Agee, 453 U.S. 280, 307 (1981) (“[N]o governmental interest is more compelling than the security of the Nation.”).
\textsuperscript{312} See Sales, supra note 117, at 819-21.
\textsuperscript{313} See Editorial, Patriot Act Balancing Act, supra note 122.
\textsuperscript{314} Chaplinsky, 315 U.S. at 572.
\textsuperscript{315} Cent. Hudson, 447 U.S. at 564.
\textsuperscript{316} Sales, supra note 117, at 818.
\textsuperscript{317} Cent. Hudson, 447 U.S. at 565-66.
large webmail provider, such as Google or Yahoo, would tip off any particular customer under investigation.

The substantial government interest in the regulation, however, must be directly advanced by the regulation, and the regulation must not be overbroad.\textsuperscript{318} Although they do address the government’s interest in protecting its investigations and the impact of leaks, indefinite restrictions such as the nondisclosure provisions of NSLs and FISA orders are very broad. Compelling an ISP, for example, to leave up a warrant canary for many years would therefore likely run afoul of the restriction against overly broad or indefinite regulations.

D. \textit{Restricting the Removal of a Canary as a Prior Restraint}

Companies with zero-count canaries should not be forced to leave them up after receiving a NSL or FISA order. Prior restraints that block speech before it occurs, much as a provider might be blocked from changing a zero-count canary, come with a presumption of unconstitutionality.\textsuperscript{319} A company required to leave a zero-count canary untouched is harmed by a prior restraint that conflicts with the aims of the First Amendment.\textsuperscript{320} Prior restraints not only “chill[]” speech, but also “freeze[]” it before it is even communicated.\textsuperscript{321} Freezing the rights of service providers to discuss the spread of surveillance requests should be weighed carefully to see if the national security concerns are serious enough to balance this least tolerable infringement of speech. Blocking speakers from participating in discussions about a given topic, as is the result when providers must leave a zero-count canary untouched, is a prior restraint that seriously impinges the First Amendment rights of the service providers.\textsuperscript{322} Particularly when the affected speech is a tripped canary that might contribute to the national conversation on the extent of government surveillance, weighing the restraint should be done under strict scrutiny.

\textsuperscript{320} Near \textit{v.} Minnesota \textit{ex rel.} Olson, 283 U.S. 697, 713 (1931) (“[I]t is the chief purpose of the [liberty of the press] guaranty to prevent previous restraints upon publication.”).
\textsuperscript{321} Nebraska Press Ass’n \textit{v.} Stuart, 427 U.S. 539, 559 (1976).
\textsuperscript{322} “It hardly requires repetition that ‘[a]ny system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity,’ and that the State ‘carries a heavy burden of showing justification for the imposition of such a restraint.’” \textit{Capital Cities}, 463 U.S. at 1305 (quoting \textit{N.Y. Times Co.}, 403 U.S. at 714).
E. NSL Nondisclosure Provisions as Prior Restraints

The NSL nondisclosure cases, filed by plaintiffs who received government requests carrying nondisclosure provisions, have generally held that the government can regulate speech under certain circumstances, including the government’s police power.

However, in order to be upheld, a prior restraint must be narrowly tailored to uphold a significant government concern. In the district court case decided after the Second Circuit’s remand from the Doe v. Gonzales of 2006—also named Doe v. Gonzales, the district court held that nondisclosure orders were so far-reaching and the investigations underlying these search requests were so long-lived that the nondisclosure restriction was not narrowly tailored. Compelling a company to leave up a canary is similarly far-reaching, as it becomes speech the speaker does not agree with, and presents a lie to the world. The broad effects of this prior restraint muzzle the speaker and stifle speech critical of government surveillance methods.

Furthermore, while the USA FREEDOM Act restricts the reporting of the number of NSLs and FISA orders that companies receive to bands of 250 or 500, the government publishes numbers of NSLs across all providers, thus reserving for itself speech denied to others. When seeking the least restrictive means possible to protect the sources and methods at risk, can the government ban publication of a canary on a specific account, but not a canary that covers ten thousand? Does the use of wide bands make the restraints more or less restrictive? Indeed, if government is the only one allowed to speak on this issue, it can shape the debate.

V. COMPELLED PUBLICATION OF WARRANT CANARIES DESERVES STRICT SCRUTINY

Courts faced with the problem of whether a company can be compelled to leave untouched a canary must consider several factors. First, the court must decide if leaving the canary up is an act of compelled speech, and they must decide the level of protection under the First Amendment for that speech. National security concerns must be balanced with the First

325 Doe, 500 F. Supp. 2d at 422. The Second Circuit agreed with the district court on the matter of the government’s failure to narrowly tailor procedural standards. John Doe, Inc., 549 F.3d at 881.
326 See Brief of Amicus Curiae Freedom of the Press Found. in Support of Plaintiff’s Opposition to Defendants’ Partial Motion to Dismiss, supra note 67, at 16.
327 See id. at 5.
Amendment’s protection of speech critical of the government and with the freedom of the mind guaranteed by the First Amendment.  

The highest level of protection, strict scrutiny, should apply to cases litigating the removal of a tripped zero-count canary. Courts should decide that the removal of a tripped canary is speech. The courts should also carefully weigh the costs of continued publication of tripped zero-count canaries. Requiring these canaries to be published appears to be a form of compelled speech based on government pressure to publicize a particular message by a private party. The court will have to balance the national security concerns implicated by the modification of the canary to decide whether the compelling government interest strongly outweighs the speech rights of the speaker and his freedom of mind. When a company is prevented from taking down or otherwise modifying a canary, that restriction seriously interferes with the speaker’s First Amendment rights and ability to communicate his thoughts about a controversial government program. Although there is some information leakage when a canary is “tripped” or otherwise taken down, that information is general in nature, informing others merely that a particular provider may have been served with legal process for some consumer data. While this may disclose some sources and methods used by law enforcement, this must be weighed against the freedom of the mind guaranteed by the First Amendment.

Warrant canaries are protected speech, and therefore should be due strict scrutiny when weighed in court. If the government wishes to compel a company to leave up a canary, it must show that there is an overriding government interest that will be harmed by removing the canary. The government must also take steps to show that compelling publication of the canary directly protects the nation’s national security interests and that there is no less restrictive solution available.

Companies seeking to remove a canary should further have their requests reviewed under strict scrutiny as a content-based speech restriction. Restrictions based on “time, place, and manner” are valid content-neutral restrictions, but restrictions that affect only particular types of speech, based on their message, are not. If the government seeks to compel a canary to stay up, this is a content-based speech restriction. The canaries are not a time, place, and manner restriction because the government is not objecting to where they are published, or how, but rather the specific message they carry.

Furthermore, canaries are not due just intermediate scrutiny as commercial speech. In Riley, the Court recognized that some advertising speech could be “inextricably intertwined” with protected speech as to change the

328 Eyink, Note, supra note 2, at 496 (opining that national security concerns must be balanced with First Amendment protections when weighing nondisclosure provisions of NSLs).

329 Volokh, supra note 138, at 2422.

fundamental character of it.\textsuperscript{331} Canaries appear to be more than mere advertising; they are small pieces of a larger debate in this country about the use of electronic surveillance.

\textit{Ward} requires that courts ensure that regulations are justified “without reference to the content of the regulated speech” in determining if the restriction is content-neutral.\textsuperscript{332} That is not the case here; the content of the canary is the primary issue at hand in the controversy. The canary’s message, that the government has made a particular type of surveillance request of the company, is the one thing that the government objects to being published. \textit{Ward} also requires that the restriction leave open alternatives.\textsuperscript{333} Although the USA FREEDOM Act has introduced some new methods of publicizing the spread of NSLs and FISA orders through the bands, the fact remains that a company with a tripped zero count canary is likely to still face pushback if they remove it. Quite possibly, they will have no real alternative available, and will face pressure to leave the zero count canary untouched to hide the NSL or FISA order.

When a restriction is content-based, it is analyzed under more exacting scrutiny than a content-neutral restriction.\textsuperscript{334} Courts should apply strict scrutiny to the message the canaries convey, one that is relevant to the ongoing public debate about the extent of government surveillance.\textsuperscript{335}

Finally, as compelled speech that goes against the speaker’s freedom of mind, compelled publication of a tripped canary should be closely inspected by the courts. The First Amendment strives to protect our freedom of the mind; to prevent companies from being coerced to participate in a message they do not agree with.\textsuperscript{336} A company compelled to publish its canary has lost that freedom of the mind.

\textbf{CONCLUSION}

Deciding what to do when faced with a company that wants to remove a canary and a law enforcement agency that wants to protect its sources and

\textsuperscript{331} Riley v. Nat’l Fed’n of the Blind of N.C., Inc., 487 U.S. 781, 796 (1988) (“But even assuming, without deciding, that such speech in the abstract is indeed merely ‘commercial,’ we do not believe that the speech retains its commercial character when it is inextricably intertwined with otherwise fully protected speech. Our lodestars in deciding what level of scrutiny to apply to a compelled statement must be the nature of the speech taken as a whole and the effect of the compelled statement thereon. This is the teaching of \textit{Schaumburg} and \textit{Munson}, in which we refused to separate the component parts of charitable solicitations from the fully protected whole.”).


\textsuperscript{333} Id. (quoting Clark, 468 U.S. at 293).


\textsuperscript{335} See, e.g., Kopstein, \textit{supra} note 8.

\textsuperscript{336} Riley, 487 U.S. at 796-98.
methods will not be easy for any court. Although the USA FREEDOM Act
now allows more information to be published about requests by government
agencies, these surveillance programs remain largely shrouded in secrecy.

The ongoing use of these programs is subject to serious debate in the
United States, with some critics arguing that the programs are overused in
large part because of the secrecy provided by the nondisclosure restrictions.
Like the village signs that mysteriously never disappeared, a canary re-
quired to stay untouched after it has been tripped hides the use of NSLs and
FISA orders. When that occurs, the public loses valuable information in the
discussion about the scope of government surveillance programs. Canaries
are speech critical of government action because of the way they illuminate
the scale of these programs, and should therefore receive the protections of
the First Amendment.

A court weighing whether to compel a company to leave a canary un-
touched should use the discretion granted it by the USA FREEDOM Act and
apply exacting scrutiny to the particulars of the case before it. The First
Amendment protections for freedom of mind, and the importance of speech
critical of government actions, mean that the court should not compel a
company to leave a canary up without weighing the protected speech care-
fully against the risk to ongoing investigations.

codified at 50 U.S.C. § 1874). Section 603 of the Act updated FISA by adding a new section to FISA’s
Title VI—section 604, entitled “Public Reporting by Persons Subject to Orders,”—which contains four
options for reporting counts of NSLs and FISA orders. See id. at 295-96.
338 See id. § 502(g), 129 Stat. at 289 (instructing district courts under § 3511(b)(1)(C) and
§ 3511(b)(3) to issue orders only if the “court determines” they are necessary and if the orders include
“conditions appropriate to the circumstances”).