NO. 18-56669

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

WILLIAM P. BARR, Attorney General,

PETITIONER–APPELLEE,

v.

UNDER SEAL,

RESPONDENT–APPELLANT.

On Appeal from the United States District Court
District for Southern California (San Diego)
Case No. 3:18-cv-02269-BAS-MDD
The Honorable Cynthia A. Bashant, District Judge

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION AND AMERICAN CIVIL LIBERTIES UNION IN SUPPORT OF APPELLANT

Naomi Gilens
Patrick Toomey
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Email: ngilens@aclu.org
Telephone: (212) 549-2500

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94103
Email: jgranick@aclu.org
Telephone: (415) 343-0758

Andrew Crocker
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: andrew@eff.org
Telephone: (415) 436-9333

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, Amici Curiae Electronic Frontier Foundation and American Civil Liberties Union state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: April 29, 2019

By: /s/ *Andrew Crocker*
Andrew Crocker

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Legislative Materials

Other Authorities

STATEMENTS OF INTEREST[1]

This brief is filed pursuant to Fed. R. App. P. 29(a) with the consent of all parties.

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit public interest organization dedicated to protecting digital civil liberties and free expression. With more than 31,000 active donors, EFF represents technology users' interests in court cases and broader policy debates, and actively encourages and challenges the government and courts to support privacy and safeguard individual autonomy as emerging technologies become more prevalent in society. EFF represents the electronic communication service providers CREDO and Cloudflare in challenges to nondisclosure orders accompanying National Security Letters they received. *See In re Nat'l Sec. Letter*, 863 F.3d 1110, Nos. 16-16067, 16-16081, 16-16082 (9th Cir. 2017), *pet. for reh'g pending*.

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than 1.5 million members dedicated to the principles of liberty and equality embodied in the Constitution and our nation's civil rights laws. The ACLU has frequently appeared before the Supreme Court, this Court, and other federal and state courts in numerous cases implicating

[1] No counsel for a party authored this brief in whole or in part, and no person other than amici or their counsel has made any monetary contributions intended to fund the preparation or submission of this brief.

government surveillance and Americans' right to privacy, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and as amicus in *United States v. Jones*, 565 U.S. 400 (2012), and *United States v. Elmore*, 917 F.3d 1068 (9th Cir. 2019).

INTRODUCTION AND SUMMARY OF ARGUMENT

As applied by the lower court in this case, the National Security Letter ("NSL") statute permits the government to impose gag orders on electronic communication service providers of indefinite duration. Although a prior decision of this Court stated that an NSL gag "must terminate when it no longer serves" a compelling government interest in national security, in practice the FBI retains the ability to convert NSLs into *permanent* bans on speech. *See In re Nat'l Sec. Letter* (*In re NSL*), 863 F.3d 1110, 1126 (9th Cir. 2017), *pet. for reh'g pending*. These gag orders violate the First Amendment.

Amici write to make three points.

First, Appellant is by no means the only service provider subject to indefinite or permanent NSL gag orders. Undersigned counsel for amicus EFF represent two service providers, CREDO Mobile and Cloudflare, who have been subject to NSL nondisclosure orders since 2011 and 2013, respectively. Both providers are subject to indefinite, open-ended nondisclosure orders, and the FBI has determined that the CREDO gag order should be permanent. The NSLs issued to CREDO and Cloudflare illustrate how the FBI uses NSLs to prevent service providers from speaking fully about their experiences for years on end. These orders have significantly limited the exercise of the providers' First Amendment rights, including speaking truthfully to Congress about the FBI's use of NSLs and

publishing accurate transparency reports describing how many demands for user information they have received from law enforcement. Although the FBI narrowed the nondisclosure orders to these service providers during the course of litigation before this Court, the providers remain barred from notifying their customers that the FBI has demanded information about them via NSLs. These experiences are not unusual: the FBI has issued more than half a million NSLs since 2001, few of which appear to have been revisited to lift associated speech restrictions.

Second, indefinite gag orders significantly constrain critical public oversight of government surveillance demands. Even delayed disclosure of government surveillance serves important purposes. As numerous examples show, disclosure allows users to defend their privacy rights, allows the courts to fulfill their constitutional role in addressing the legality of executive action, and enables public debate concerning the proper scope of government surveillance.

Third, well-settled First Amendment law requires reversal of the district court's order that Appellant comply with the three NSLs' nondisclosure requirements "unless and until the Government informs it otherwise." ER 1. That order violates the First Amendment because it imposes a content-based restriction on Appellant's speech and fails to ensure that the restriction on Appellant's speech is limited in duration to only the time necessary for the government's interest in continued nondisclosure.

ARGUMENT

I. NSL NONDISCLOSURE ORDERS THAT VIOLATE THE FIRST AMENDMENT CONTINUE TO RESTRICT INTERNET SERVICE PROVIDERS.

Alone among the FBI's investigative tools, the National Security Letter statute allows the FBI to unilaterally impose nondisclosure orders on recipients, without ensuring that all such gag orders eventually dissolve. In its 2017 *In re NSL* decision, this Court acknowledged that the duration of NSL gags raised serious First Amendment concerns requiring the statute to meet strict scrutiny. *See* 863 F.3d at 1126–27. Noting that the FBI's internal procedures for reviewing NSLs failed to "resolve the duration issue entirely," the Court nevertheless affirmed the statute's facial constitutionality because it assumed that judicial review by district courts would ensure that NSL gags do "not remain in place longer than is necessary to serve the government's compelling interest." *Id*. at 1126.[2]

Here, however, the district court refused to narrowly tailor the nondisclosure order issued to Appellant. As Appellant's experience illustrates, this Court's

[2] As explained in a pending petition for rehearing and rehearing en banc in *In re NSL*, amici disagree with this Court's panel decision concluding that the NSL statute is facially constitutional, because it imposes prior restraints on speech, fails to include the safeguards necessary to prevent prior restraints on speech, and as a whole the statute allows the restriction of more speech than is necessary to serve the government's interests. Regardless of whether the *In re NSL* panel's opinion remains intact, amici agree with Appellant in this case that, by its own terms, *In re NSL* requires district courts to place finite limits on the duration of NSL nondisclosure orders.

directive to lower courts has not prevented the imposition of unconstitutional indefinite gag orders.

Many, if not the majority, of other NSL recipients labor under similarly unconstitutional indefinite nondisclosure orders. Although only a handful of NSL recipients are known to have challenged these demands, they are far from the only service providers subject to indefinite nondisclosure orders. Since 2001, the government has issued almost 500,000 NSLs and continues to issue more than 12,000 each year.[3] Although the government has at times suggested that the FBI's policy for reviewing NSL gag orders, known as "Termination Procedures," would apply to older NSLs, the procedures entirely exempt from review any NSL issued before November 2012 for which the underlying investigation has already closed—encompassing tens if not hundreds of thousands of NSLs. Without clear

[3] Department of Justice, Office of the Inspector General, *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 65 (2014), https://oig.justice.gov/reports/2014/s1408.pdf (graph showing NSLs issued 2003–11); President's Review Group on Intelligence & Communications Technologies, *Liberty and Security in a Changing World: Report and Recommendations from the President's Review Group on Intelligence and Communications Technologies* at 91–93 (2013) ("President's Review Group"), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf (number of NSLs issued in 2012); Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities Calendar Year 2017* at 26 (May 2, 2017), https://perma.cc/ZTD4-ZS75 (chart showing NSLs issued 2013-2017).

directives from this Court, the countless recipients of these NSLs will have limited recourse if they seek to have a court review a nondisclosure issued years before.

This includes two clients of amicus EFF, CREDO and Cloudflare, who are prohibited from speaking fully about the NSLs they received in 2011 and 2013, respectively.

A. NSL Nondisclosure Orders Issued to CREDO and Cloudflare Years Ago Still Prevent Them from Speaking Fully About Their Experiences Receiving and Challenging Them.

Despite years of legal challenges to the statutes that authorize NSL nondisclosure orders, CREDO and Cloudflare are still subject to indefinite orders that prohibit them from fully speaking about receiving NSLs more than eight and six years ago, respectively.

In each case, the NSL prohibited the provider from disclosing any information about the NSL to its affected customer, to most of its employees and staff, to the press, to members of the public, and to members of Congress. Shortly after receiving the letters, CREDO and Cloudflare filed petitions asking the same district court to set aside the NSLs, arguing that the statute was unconstitutional on its face and as applied. Those challenges included two different appeals to this Court. *See In re NSL*, 863 F.3d at 1119–21 (procedural history). Until 2017, the providers' identities remained under seal because the nondisclosure orders

prohibited them from even acknowledging that they had received the NSLs, much less that they were challenging them in court.

Days before oral argument in this Court, the government notified CREDO and Cloudflare that it was modifying the nondisclosure orders accompanying the NSL CREDO received in 2011 as well as the NSLs Cloudflare received in 2013. *See In re NSL*, 863 F.3d at 1120; *see also* Notice Concerning National Security Letter at Issue in No. 16-16067, Unsealing of Briefs, and Public Identification of the Appellants, *In re NSL*, No. 16-16067 (9th Cir. Mar. 20, 2017), ECF No. 77 ("March 2017 Notice"). The Notice stated that in light of the FBI's new Termination Procedures, the FBI was allowing CREDO to publicly disclose (1) the fact that it had received the 2011 CREDO NSL and (2) whether it provided information in response to the NSL. March 2017 Notice at 3. The Notice further stated that although the FBI had closed the underlying investigation that led to the 2011 CREDO NSL, the FBI was still prohibiting CREDO from speaking publicly about any other aspect of the NSL, including notifying the customer it targeted or providing any other information that could identify that customer. *Id*.

With respect to Cloudflare, the Notice stated that the company could identify itself as receiving both 2013 NSLs subject to its challenge. The FBI had lifted the nondisclosure order with respect to one of the NSLs and, although it allowed Cloudflare to state that it had received a second NSL, the FBI continued to require

the company "to refrain from disclosing any information concerning the NSL other than the fact" that it had received the second one. *Id*. at 4.

Thus the FBI still prohibits both CREDO and Cloudflare from speaking fully about the NSLs they received.

B. The FBI's Termination Procedures Permit It to Impose Indefinite and Potentially Permanent Gag Orders on CREDO and Cloudflare.

The FBI's review of the NSL nondisclosure orders issued to CREDO and Cloudflare in response to the 2015 amendments to the NSL statutes demonstrate that the FBI can enter indefinite and, in some cases, permanent, gag orders against providers. The USA FREEDOM Act of 2015 directed the Attorney General to adopt unspecified procedures providing for internal FBI review "at appropriate intervals" to determine whether gags issued under the revised statute are still supported. Pub. L. 114-23, § 502(f)(1)(A) ("USA FREEDOM"). Pursuant to procedures adopted on November 24, 2015, the FBI reviews NSL gags on (at most) two occasions: the third anniversary of the investigation that led to the NSL's issuance, and the closing of that investigation.[4] The FBI's application of its Termination Procedures to CREDO and Cloudflare expose the unconstitutional gaps in these procedures and the NSL statute. While this Court upheld those

[4] Federal Bureau of Investigation, *Termination Procedures for National Security Letter Nondisclosure Requirement* (Nov. 24, 2015), https://www.fbi.gov/file-repository/nsl-ndp-procedures.pdf/view.

Termination Procedures as applied to CREDO and Cloudflare, the companies' petitions for panel rehearing and rehearing en banc remain pending. *See* Pet., *In re NSL*, No. 16-16067 (9th Cir. Oct. 2, 2017), ECF No. 90. Moreover, one of the linchpins of the Court's analysis has not been borne out in practice since the opinion. Although this Court expected that district courts hearing challenges to NSL gag orders would "require the government to justify the continued necessity of nondisclosure on a periodic, ongoing basis," *In re NSL*, 863 F.3d at 1127, that has not come to pass.

CREDO has been subject to an NSL gag order since 2011, which appears to be permanent. This is because the FBI has closed the underlying case associated with the NSL it received in 2011. March 2017 Notice at 1. By their own terms, the FBI's Termination Procedures do not require the FBI to ever reconsider a nondisclosure order once an underlying investigation closes. Thus, the prohibition limiting what CREDO could say about the NSL—including not being able to notify the subscriber whose information the FBI requested—remains in effect. And neither the Termination Procedures nor the NSL statutes require the FBI to ever again reconsider the gag it has imposed on CREDO. *See* Oral Argument at 27:41, *In re NSL*, Nos. 16-16067 & 16-18082 (9th Cir. Mar. 22, 2017), https://youtu.be/ccS06CFkZ5M (counsel for government stating that an indefinite gag order is "possible").

Meanwhile, the nondisclosure order the FBI entered against Cloudflare in 2013 remains in place indefinitely. This is because the NSL Termination Procedures only require subsequent review of the gag order at the close of the FBI's investigation. *See In re NSLs,* No. 16-518 (JEB), 2016 WL 7017215, at *2 (D.D.C. July 25, 2016) (discussing "loopholes" in NSL Termination Procedures allowing indefinite gag orders). Cloudflare thus is in the same position as Appellant in this case inasmuch as the ability to fully exercise its First Amendment rights remains entirely dependent on executive determinations by the FBI.

II. DISCLOSURE IS ESSENTIAL TO PROTECT USERS AND THE PUBLIC FROM UNLAWFUL GOVERNMENT SEARCHES.

Indefinite gag orders are also at odds with users' privacy interests and the public's interest in ensuring that government surveillance demands are lawful. Even when disclosure is delayed, it serves vital purposes. Disclosure of NSLs by technology companies allows users to defend their privacy rights, helps ensure that courts have the chance to address the legality of novel surveillance tools, and permits the public to deliberate on the proper limits of government surveillance.

A. Disclosure of NSLs Is Critical to Protect Users' Privacy Rights.

Disclosure to impacted individuals is often essential to meaningful court review of new surveillance techniques or novel interpretations of existing surveillance laws. When it comes to NSLs, as with many other types of surveillance, disclosure by providers is critical because the government itself never

notifies individuals that their information has been seized—even in criminal cases. Indeed, the government refuses to disclose to criminal defendants when inculpatory evidence against them was derived from NSLs. *See, e.g.*, Gov't Resp. Br. at 8, *United States v. Thomas*, No. 15-cr-00171 (E.D. Pa. July 29, 2019), ECF No. 74 (arguing that with respect to NSLs "there is *no* requirement to provide a defendant with notice or discovery of the process used" (emphasis in original)). Accordingly, legal challenges to the government's interpretation and application of its NSL authority do not arise in criminal cases. Unless providers receiving NSLs are eventually allowed to disclose them, few individuals will be in a position to challenge the government's use of this surveillance technique, and the ability of courts to review the lawfulness of overbroad NSLs will be sharply circumscribed.[5]

[5] A similar story applies to another controversial subpoena authority: the Drug Enforcement Administration's ("DEA") use of administrative subpoenas as part of its "Hemisphere Project." Using this program, the DEA issues subpoenas to AT&T to access and analyze a vast pool of subscriber call data that includes location records. Scott Shane & Colin Moynihan, *Drug Agents Use Vast Phone Trove, Eclipsing N.S.A.'s*, N.Y. Times, (Sept. 1, 2013), http://nyti.ms/Nsuk3Z. Though the public learned of Hemisphere in 2013, the government has scrupulously sought to conceal the use of the program from courts, defense attorneys, and criminal defendants. *Id.* In particular, agents have been instructed that, to "[p]rotect[] [t]he [p]rogram," they must "never refer to Hemisphere in any official document." *See Synopsis of the Hemisphere Project*, N.Y. Times (Sept. 1, 2013), http://nyti.ms/1dOBj3F (slide presentation). Because no individual has received notice that he or she was subject to this surveillance, even in a criminal prosecution, no individual has yet been able to challenge the lawfulness of the program in court.

Disclosure also ensures that individuals whose information is seized or searched have an opportunity to defend their privacy from unwarranted and unlawful government intrusions, including by remedying unjustified invasions and seeking the return of property or information unlawfully held. In most instances, no one has a stronger interest in vindicating the user's privacy interests than the user. *See generally* S. Rep. 90-1097, 1968 U.S.C.C.A.N. 2112, 2194 (Pursuant to Title III's notice requirement, "all authorized interceptions must eventually become known at least to the subject," so that he "can then seek appropriate civil redress for example, under [18 U.S.C. § 2520], if he feels that his privacy has been unlawfully invaded."); Fed. R. Crim. P. 41(g). By preventing providers from disclosing the fact of the NSL to the user whose privacy interest was impacted, the government deprives users of any opportunity to assert their privacy rights and to seek court review. With no knowledge of an intrusion, the individual is unable to challenge it.

As a result, customers must rely on their service providers to stand up for their privacy rights in the face of secret surveillance demands. But there is no guarantee that a company receiving an NSL will decide to challenge it, even if the government's demand for information appears to go beyond what the law allows. A company's interests are diverse; it may have a number of matters before government regulators at a given time; litigation can be expensive, especially for

smaller companies; and the ultimate legal duty of a public company is to its shareholders.[6] As a result, companies may challenge government surveillance orders on behalf of their customers infrequently, if ever, even when they perceive those orders to be unlawful. That risk is especially high because these orders are secret.

The government's past misuse of NSLs shows how abuses can go unchallenged for years in the absence of disclosure. In 2005, Congress directed the Department of Justice ("DOJ") Office of the Inspector General ("OIG") to investigate and review the FBI's use of NSLs. *See* Department of Justice, Office of Inspector General, *A Review of the Federal Bureau of Investigation's Use of National Security Letters* (Mar. 2007) ("NSL Report"), https://perma.cc/LQ8X-C5PC. The Inspector General's investigation uncovered widespread misuse of the NSL authority, concluding that "the FBI used NSLs in violation of applicable NSL statutes, Attorney General Guidelines, and internal FBI policies." *Id.* at 125; *see also John Doe, Inc. v. Mukasey*, 549 F.3d 861, 880 (2d Cir. 2008) (citing the NSL Report's conclusions).

These problems have persisted. Despite explicit guidance from DOJ's Office of Legal Counsel, NSLs issued by the FBI as recently as 2016 include demands for

[6] *See, e.g.*, Stephen W. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 Harv. L. & Pol'y Rev. 313, 327–29 (2012) (discussing divergence between users and companies in incentives to challenge surveillance orders).

customer information beyond what the statute allows. *See* Dustin Volz, *FBI Request for Twitter Account May Have Overstepped Legal Guidelines*, Reuters, (Jan. 27, 2017) https://reut.rs/2PrbkEI; Department of Justice, Office of Legal Counsel, *Requests for Information Under the Electronic Communications Privacy Act* (Nov. 5, 2008), https://perma.cc/H7CG-GJWW. At the heart of these abuses is the FBI's effort to use NSLs to obtain new types of records as technology has advanced, including sensitive records of Internet activity, even though the NSL statute does not allow it. *See id.* Unfortunately, few companies appear to have challenged the improper NSLs they have received—and, as explained above, some of those who have pursued challenges remain mired in lengthy litigation, including some pending before this Court.

Against this backdrop, disclosure to individuals can play a critical role in clarifying the limits of the government's surveillance powers, especially in the face of new technologies. In a variety of cases where individuals have learned that the government used novel or secretive surveillance tools, those individuals have successfully challenged the lawfulness of that surveillance. *See, e.g.*, *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (collection of cell-site location information); *In re Grand Jury Subpoena*, 828 F.3d 1083 (9th Cir. 2016) (subpoena for personal emails); *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (bulk collection of phone records). For example, many law enforcement agencies use surveillance devices

known as "cell site simulators" or, more commonly, "Stingrays." These devices mimic cell phone towers, allowing law enforcement to collect information from any cell phone within range, including location information, and even the content of voice or text message conversations. *See* Stephanie K. Pell & Christopher Soghoian, *Your Secret Stingray's No Secret Anymore*, 28 Harv. J.L. & Tech. 1, 11 (Fall 2014). Though Stingray surveillance is widespread, for years the government carefully kept its use of these devices hidden from magistrate judges and courts, with prosecutors' offices even dropping cases rather than revealing their use of the device. *See, e.g.*, Daphne Duret, *Stingray: PBSO Deputies Use Secret Cellphone Catcher That Could Grab Your Call Logs, Texts*, Palm Beach Post (Aug. 24, 2018), https://www.palmbeachpost.com/news/20180827/stingray-pbso-deputies-use--secret-cellphone-catcher-that-could-grab-your-call-logs-texts.[7] However, in the rare cases where a defendant *has* learned that the government's evidence

[7] *See also, e.g.*, *Hearing Could Determine Penalties, Fines for Tacoma over Stingray Data*, Tacoma Weekly News (May 23, 2018), https://perma.cc/72SF-DZ9U ("TPD had for years hidden its use of this surveillance equipment from the public and from the courts."); Isiah Holmes, *Wisconsin Police Department Used Stingray Device, Despite Denials*, Pontiac Trib. (Nov. 6, 2017), https://perma.cc/WC7Z-2WUF; Justin Fenton, *Baltimore Police Used Secret Technology to Track Cellphones in Thousands of Cases*, Baltimore Sun (Apr. 9, 2015), https://perma.cc/8HH4-ZMDL ("The Baltimore Police Department has used an invasive and controversial cellphone tracking device thousands of times in recent years while following instructions from the FBI to withhold information about it from prosecutors and judges . . . .").

derived from Stingray surveillance, many courts have held that the warrantless use of Stingrays violates the Fourth Amendment.[8]

B. Disclosure of NSLs is Critical to Provide the Public With Information About How the Government Is Interpreting and Applying Its Surveillance Authorities.

Not only is disclosure necessary to allow individuals subject to government surveillance to defend their constitutional rights, but it is also essential to force the executive branch to account for its investigative methods to the public at large. If the public is unaware that the government is engaging in certain surveillance techniques, it cannot deliberate on those techniques and the resulting intrusions into individual privacy. There is a strong relationship between the scope of government electronic investigative techniques and the public's right to know: the more individuals' communications or data these techniques sweep up, the greater the public's interest in receiving notice about them.

[8] *See, e.g.*, *United States v. Lambis*, 197 F. Supp. 3d 606 (S.D.N.Y. 2016); *Commonwealth v. Almonor*, No. SJC-12499, 2019 WL 1769556 (Mass. Apr. 23, 2019); *State v. Andrews*, 134 A.3d 324 (Md. 2016); *Ferrari v. State*, 260 So. 3d 295 (Fl. Dist. Ct. App. 2018); *State v. Sylvestre*, 254 So. 3d 986 (Fl. Dist. Ct. App. 2018); *Jones v. United States*, 168 A.3d 703 (D.C. Ct. App. 2017); *see also United States v. Artis*, 919 F.3d 1123 (9th Cir. 2019) (assuming that use of Stingray required warrant, and noting that government assumes the same); *United States v. Ellis*, 270 F. Supp. 3d 1134 (N.D. Cal. 2017) (holding that Stingray surveillance is a Fourth Amendment search but declining to suppress evidence per exceptions to the exclusionary rule).

However, the government often tightly limits disclosure in the very instances where it has interpreted and applied its surveillance authorities the most expansively. Keeping its activities out of the public eye has allowed the government to build sprawling surveillance programs with virtually no public deliberation or oversight. When the public has become aware of how the government has been conducting surveillance in secret, the public, courts, and Congress have often sought to rein in the government's use of these techniques and recalibrate the balance between government surveillance and individual privacy.

1. National Security Letters

The government's prior use of NSLs illustrates this dynamic. Until 2005, recipients of NSLs were prohibited from disclosing to any person that the FBI had sought or obtained the requested information. 18 U.S.C. § 2709(c) (2001), *amended by* USA FREEDOM*,* § 501 (2015); NSL Report at 14, https://perma.cc/LQ8X-C5PC. During that period, the FBI's reports to Congress vastly understated how frequently the FBI used NSLs. *Id.* at 32–37.

But after the DOJ Inspector General revealed the FBI's systematic and extensive misuse of NSLs, courts, Congress, and the executive branch all took steps to curtail the FBI's indiscriminate use of them. First, the Second Circuit interpreted the NSL statutes, 18 U.S.C. §§ 2709, 3511, to permit gag orders only when senior FBI officials certify that disclosure may result in an enumerated harm

that is related to an authorized terrorism or intelligence investigation, and placed on the government the burden to show why disclosure of receipt of an NSL will risk an enumerated harm. *Mukasey*, 549 F.3d 883. In addition, the court held both statutes unconstitutional to the extent that they impose a nondisclosure requirement without placing on the government the burden of initiating judicial review of that requirement, and to the extent that, upon such review, a governmental official's certification that disclosure may endanger the national security of the United States or interfere with diplomatic relations is treated as conclusive. *Id.*

The Northern District of California subsequently held that the government's "pervasive use of nondisclosure orders, coupled with the government's failure to demonstrate that a blanket prohibition on recipients' ability to disclose the mere fact of receipt of an NSL is necessary to serve the compelling need of national security, creates too large a danger that speech is being unnecessarily restricted." *In re Nat'l Sec. Letter*, 930 F. Supp. 2d 1064, 1076 (N.D. Cal. 2013). The court enjoined the government from issuing NSLs or enforcing the nondisclosure provision. *Id.* at 1081.

Then, in 2013, responding to the OIG reports and congressional testimony, the President's Review Group recommended several limitations on the FBI's NSL authority to better protect the privacy and civil liberties of Americans. *See* President's Review Group. Noting that "nondisclosure orders . . . interfere with

individual freedom," the President's Review Group recommended a requirement for judicial approval prior to the issuance of an NSL absent "genuine emergency," and a requirement that nondisclosure orders should remain in effect for no longer than 180 days without judicial re-approval. *Id.* at 27, 92–93. In addition, the President's Review Group recommended that "[w]ith respect to authorities and programs whose existence is unclassified," including the NSL authorities, "there should be a strong presumption of transparency to enable the American people and their elected representatives independently to assess the merits of the programs for themselves." *Id.* at 26. "[T]o the greatest extent possible," the report continued, the government should report on its use of NSLs in order to "inform Congress and the public about the overall size and trends in a program," especially "major changes in the scale of a program." *Id.* at 128.

In the wake of these court cases and the report by the President's Review Group, Congress amended the NSL statutes in 2015. Among other changes, the amendments allowed for the government to modify or rescind nondisclosure orders after issuance, and no longer required recipients of gag orders who unsuccessfully challenged those orders to wait for a year before seeking further judicial relief. USA FREEDOM, § 502(a), (g), *codified at* 18 U.S.C. § 2709(c); *id.* § 3511(b). The amendments also required the Attorney General to adopt procedures requiring the

periodic review of gag orders "to assess whether the facts supporting nondisclosure continue to exist." *See* USA FREEDOM, § 502(f)(1)(A).

2. Exigent Letters

During the course of its investigation of the FBI's misuse of its NSL authority, the OIG discovered one especially troubling practice: the FBI had acquired call record information from telephone companies without any legal process whatsoever—a practice known as issuing "exigent letters." *See NSL Report* at 86–97. The FBI used exigent letters to obtain information by promising that the agent had already requested a grand jury subpoena or an NSL, but needed the information more urgently. The companies receiving the exigent letters were asked to turn over sensitive customer information in reliance on that representation. In many instances, though, no emergency existed, no grand jury subpoenas or NSLs had been requested before the documents were obtained, and the FBI could not substantiate that agents ever followed through with the proper process. *Id.* As a consequence of the FBI's use of exigent letters, the OIG concluded the FBI had circumvented the NSL statutes and violated National Security Investigation Guidelines and internal FBI policies. *Id.* at 93. When the issuance of the OIG's report brought the FBI's use of exigent letters to light, the FBI ceased the practice and took corrective steps. *See* Department of Justice, Office of the Inspector General, *A Review of the Federal Bureau of Investigation's*

Use of Exigent Letters and Other Informal Requests for Telephone Records at 190, 289 (Jan. 2010), https://oig.justice.gov/special/s1001r.pdf.

3. Other Secret Surveillance Programs

A number of other government surveillance activities that, for years, operated entirely in secret have been restricted or shut down once exposed to public scrutiny. For example, as discussed above, law enforcement, for years, sought to keep its use of Stingray devices secret from the public and the courts. *See supra*, note 7. As the government's widespread use of this secret surveillance technique has come to light, the public has strongly rejected it. At least sixteen states have now enacted legislation requiring law enforcement agencies to obtain a warrant before tracking cell phone location information in real time. *See, e.g.*, Cal. Penal Code § 1546 (2017); Colo. Rev. Stat. § 16-3-303.5 (2014); 725 Ill. Comp. Stat. 137 (2017); Ind. Code Ann. § 35-33-5-15 (2016); Me. Rev. Stat. Ann. tit. 16, § 648 (2017); Md. Code Ann., Crim. Proc. § 1-203.1 (2019); Minn. Stat. Ann. § 626A.42 (2014); Mont. Code Ann. § 46-5-110(1)(a) (2013); N.H. Rev. Stat. Ann. § 644-A:2 (2015); 12 R.I. Gen. Laws Ann. § 12-32-2 (2019); Tenn. Code Ann. § 39-13-610(b) (2014); Utah Code Ann. § 77-23c-102 (2019); 13 Vt. Stat. Ann. tit. 13, § 8102 (2016); Va. Code Ann. § 19.2-70.3m (2018); Wash. Rev. Code Ann. § 9.73.260 (2015); Wis. Stat. Ann. § 968.373 (2014).

Additionally, the government's misuse of Section 215 of the Patriot Act to collect Americans' call records in bulk spurred legislative reform efforts only when the surveillance came to light. Section 215 authorizes the government to compel the production of "any tangible thing," including "business records," where there are "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation." 50 U.S.C. § 1861. In 2013, a leaked order from the Foreign Intelligence Surveillance Court revealed that the government had, for years, secretly interpreted Section 215 to authorize the collection of telephone records from virtually every person in the United States. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian (June 6, 2013), https://perma.cc/AGF3-JQNC. After sustained public pushback against the government's secret use of Section 215 to carry out dragnet telephone surveillance, Congress ended and replaced the program in 2015, and the government suspended the program entirely in 2018. *See* Charlie Savage, *Disputed N.S.A. Phone Program Is Shut Down, Aide Says*, N.Y. Times (Mar. 4, 2019), https://nyti.ms/2PuFJCg.

Similarly, in 2015, the public learned for the first time that, starting in the 1990s, the DEA had secretly collected and stored billions of records of Americans' international phone calls. *See* Brad Heath, *U.S. Secretly Tracked Billions of Calls for Decades*, USA Today (Apr. 7, 2015), https://perma.cc/6986-TCBJ. The

program was quickly challenged in federal court, where the judge ordered the government to respond to discovery about the program. Order, *Human Rights Watch v. Drug Enf't Admin.*, No. 15-cv-2573-PSG (C.D. Cal. Aug. 14, 2015), ECF No. 38. Through that discovery, the public learned that the program had been shut down in 2013, soon after the Section 215 bulk call records program became public and received significant public backlash. *See* Mark Rumold, *A Victory for Privacy and Transparency: HRW v. DEA*, EFF (Dec. 14, 2015), https://perma.cc/7KGP-4S7M.

Had the government's past misuse of NSLs, reliance on exigent letters, warrantless Stingray surveillance, and bulk call records programs remained secret, companies and individuals might still well be suffering from those abuses. It was only through disclosure that the public, legislature, and the courts were able to rein in these privacy-violating surveillance activities.

III. INDEFINITE NONDISCLOSURE ORDERS FAIL CONSTITUTIONAL SCRUTINY.

A "regulation or law that restricts speech based on its topic, idea, message, or content is 'content based' on its face, and is accordingly subject to strict scrutiny." *In re NSL*, 863 F.3d at 1123. As this Court recently made clear in another NSL case, a nondisclosure order prohibiting the recipient from disclosing the fact that the FBI has sought or obtained access to information or records is

exactly this kind of restriction. *Id.* Accordingly, nondisclosure orders must be narrowly tailored to serve a compelling government interest. *Id*.

A nondisclosure order of unlimited duration is not narrowly tailored to the government's interest in protecting its investigations. As Appellant explains in its principal brief, the nondisclosure order at issue in this case will likely never be subject to mandatory government review. *See* Appellant's Br. at 23–24, ECF No. 31. The nondisclosure order is therefore effectively a nondisclosure order in perpetuity, and may well prevent the recipient from *ever* disclosing the order, even, potentially, years after the government has closed its investigation.

"A restriction is not narrowly tailored 'if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.'" *In re NSL*, 863 F.3d at 1124 (quoting *Reno v. ACLU*, 521 U.S. 844, 874 (1997)). A nondisclosure order with a specified, reasonable duration would be an equally effective and less restrictive alternative, and would not prevent the government from issuing subsequent nondisclosure orders of finite duration should nondisclosure remain necessary. Courts have recognized that the "loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury," *Elrod v. Burns*, 427 U.S. 347, 373 (1976), and thus NSL gag orders cannot be permitted to persist long after their rationale expires. Amici believe that the NSL statute violates the First Amendment

on its face, in part because it fails to limit the FBI's authority to impose indefinite nondisclosure orders. *See supra*, note 2 (discussing pending petition for rehearing and rehearing en banc on this question). Regardless, as this Court directed, "reviewing courts" are "bound to ensure that the nondisclosure requirement does not remain in place longer than is necessary to serve the government's compelling interest." *In re NSL*, 863 F.3d at 1126.

Under that holding, then, many nondisclosure orders would need to dissolve rather quickly, in some cases in a matter of weeks or days, as they become "unnecessary"—whether due to an arrest, the end of an investigation, or some other reason. At the very least, federal courts considering NSLs and other nondisclosure orders have concluded that—as an outer limit—a 180-day limitation may satisfy issues of administrative burden raised by the government. *See In re Nat'l Sec. Letter*, 165 F. Supp. 3d 352, 355 (D. Md. 2015) (imposing 180-day duration on an indefinite NSL where FBI Termination Procedures did not require mandated review); *see also Matter of Search Warrant for [redacted].com*, 248 F. Supp. 3d 970, 984 (C.D. Cal. 2017) (imposing 180-day limit on nondisclosure order issued pursuant to 18 U.S.C. § 2705(b)); *In re Search Warrant Issued to Google, Inc.*, 269 F. Supp. 3d 1205, 1218 (N.D. Ala. 2017) (same); *In re Sealing*

and Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 895 (S.D. Tex. 2008) (same).[9]

It is not sufficient that the NSL recipient may request that the government petition for judicial review of the gag order. The recipient is not privy to the investigation and has no way to know the point at which the gag order is no longer justified. *See Matter of Search Warrant for [redacted].com*, 248 F. Supp. 3d at 983 (holding indefinite gag order under 18 U.S.C. § 2705(b) unconstitutional and imposing 180-day limit). "[P]utting the onus on the speaker to lift a no-longer-justified content-based restriction" is hardly narrow tailoring—in fact, "[a]dding the fact that the speaker cannot know when the restriction's *raison d'etre* fades effectively equates to no tailoring at all." *Id*. (quotation marks omitted). The recipient may well forgo its constitutional speech rights if exercising them requires the recipient to "incur the trouble and expense of potentially futile court trips" in order to test whether the restriction on its speech in fact remains necessary. *Id.*

[9] The government may claim that NSLs require a longer duration than Section 2705(b) gag orders because NSLs are issued in national security investigations rather than criminal investigations, but that distinction should not be dispositive. Unlike NSLs, Section 2705(b) gag orders must be judicially approved. In the NSL context, the government need only review the need for nondisclosure orders internally. Requiring that it do so at regular intervals, such as every 180 days, imposes a lesser burden than requiring it to regularly justify a gag order to a court. Moreover, the need for regular internal review is greater in the absence of any judicial supervision that serves to hold the government accountable.

The government bears the burden of justifying the constitutionality of its own restrictions on speech. *United States v. Playboy Entm't Grp.*, 529 U.S. 803, 816 (2000). Thus, it is the government's burden to demonstrate that a gag order banning speech indefinitely, and effectively in perpetuity, is the least restrictive means of advancing its interest. Amici cannot conceive of a factual scenario where the government could meet such a burden.

CONCLUSION

Accordingly, this Court should vacate the district court's judgment and remand with instructions to limit the nondisclosure order to a duration narrowly tailored to the government's specific interest in this case.

Dated: April 29, 2019

By: /s/ *Andrew Crocker*

Naomi Gilens
Patrick Toomey
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Email: ngilens@aclu.org
Telephone: (212) 549-2500

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94103
Email: jgranick@aclu.org
Telephone: (415) 343-0758

Andrew Crocker
Aaron Mackey
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: andrew@eff.org
Telephone: (415) 436-9333

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amici Curiae Electronic Frontier Foundation and American Civil Liberties Union in Support of Appellant complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,352 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016, the word processing system used to prepare the brief, in 14-point font in Times New Roman font.

Dated: April 29, 2019

By: /s/ *Andrew Crocker*
Andrew Crocker

Counsel for Amici Curiae
Electronic Frontier Foundation and
American Civil Liberties Union
Foundation

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on April 29, 2019.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: April 29, 2019

By: /s/ *Andrew Crocker*
Andrew Crocker

Counsel for Amici Curiae
Electronic Frontier Foundation and
American Civil Liberties Union
Foundation