No. 23-1264

In the Supreme Court of the United States

X CORP., FKA TWITTER, INC., *Petitioner,*

v.

UNITED STATES

On Petition for a Writ of Certiorari
to the United States Court of Appeals
for the District of Columbia Circuit

BRIEF FOR PROJECT FOR PRIVACY AND SURVEILLANCE ACCOUNTABILITY, INC. AS *AMICUS CURIAE* SUPPORTING PETITIONER

GENE C. SCHAERR
Counsel of Record
ERIK S. JAFFE
AARON C. WARD
SCHAERR | JAFFE LLP
1717 K Street NW
Suite 900
Washington, DC 20006
(202) 787-1060
gschaerr@schaerr-jaffe.com
Counsel for Amicus Curiae

JULY 3, 2024

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Other Authorities

INTRODUCTION AND INTEREST OF *AMICUS CURIAE*[1]

This Court recently reiterated that the government may not coerce third parties to indirectly restrain or punish someone else's speech. *National Rifle Ass'n of Am.* v. *Vullo*, 602 U.S. 175, 144 S. Ct. 1316, 1322 (2024) (quoting *Bantam Books, Inc.* v. *Sullivan*, 372 U.S. 58, 67 (1963)). And this case raises an important parallel question: May the government conscript a third party as, in effect, an adjunct spy while directly restraining that third party's speech—all so the government can strike more effectively at its target? This Court's First Amendment precedent strongly supports the conclusion that such prior restraints are forbidden unless they can pass strict scrutiny.

Federal agencies, however, routinely evade the clear implications of this Court's First Amendment precedent because, even though companies that provide cloud-based data services face the scenario presented here tens of thousands of times a year, they are rarely able to litigate it. This case provides a rare vehicle that allows the Court to address a shockingly common First Amendment violation. And for that reason (and those stated in the petition), the Court should grant review here.

The facts here are salient: The government sought to circumvent a claim of executive privilege by seizing

---

[1] This brief was not authored in whole or in part by counsel for any party and no person or entity other than *amicus curiae* or its counsel has made a monetary contribution toward the brief's preparation or submission. All parties were notified of the intent to file this brief at least 10 days prior to the deadline.

records from Petitioner, a third-party data host. Using a common mechanism called a non-disclosure order (NDO), Respondents then prevented Petitioner from discussing the matter with its user. Allegedly, this was to preserve the secrecy of an investigation, but the government itself *already* had publicized the material details of the investigation.

After Petitioner sued, the D.C. District Court purported to apply strict scrutiny, and the D.C. Circuit affirmed. But the analysis applied below did not remotely resemble strict scrutiny: It required neither a compelling interest nor narrow tailoring. And it did not attempt to require the "procedural safeguards designed to obviate the dangers of a censorship system" involving a prior restraint on speech. *Freedman* v. *Maryland*, 380 U.S. 51, 58 (1965).

This all-too-common scenario makes a mockery of longstanding precedent governing prior restraints. And it will only become more frequent as third-party cloud storage becomes increasingly common for everything from business records to personal files to communications. Moreover, as illustrated here, NDOs can be used to undermine other constitutionally protected rights, including those protected by the Fourth and Sixth Amendments. Allowing this behavior to stand would eviscerate both the "degree of privacy" and degree of freedom of speech "that existed when the [Bill of Rights] was adopted." *Carpenter* v. *United States*, 585 U.S. 296, 305 (2018) (quoting *Kyllo* v. *United States*, 533 U.S. 27, 34 (2001)).

Protection of constitutional rights and guarding against an over-reaching surveillance state are key missions of *amicus curiae* Project for Privacy and

Surveillance Accountability, Inc. (PPSA), a nonprofit, nonpartisan organization. PPSA urges this Court to grant *certiorari* and apply its long-standing First Amendment precedent to the NDO context.

SUMMARY

The NDO at issue here violates the First Amendment because it does not satisfy strict scrutiny and lacks the necessary procedural requirements for a prior restraint on speech. And such First Amendment failings are especially troubling and important to address because the government's tactics here—using an NDO attached to a search warrant to deliberately circumvent a legal privilege—could also be used to erode Fourth and Sixth Amendment rights, among others, in this and a range of similar circumstances in which agencies or courts issue NDOs.

This case is an ideal vehicle and opportunity to address this issue, as similar NDOs are issued tens of thousands of times a year yet are extraordinarily difficult to litigate. The problem will only grow given the rapid rise of third-party data hosting, with the number of data centers in the United States more than doubling since 2021. And it could grow exponentially given a recent change to the definition of "electronic communication service provider" in the Foreign Intelligence Surveillance Act (FISA)—a change that would allow the government to issue NDOs to an extraordinary number of unsophisticated and vulnerable businesses and private associations.

This case thus offers a rare glimpse at the tip of an iceberg of surveillance-related prior restraints that

rarely come to light but can do titanic damage to constitutional rights.

ADDITIONAL REASONS TO GRANT REVIEW

For the reasons Petitioner explains, the NDO at issue here is an unjustified and unconstitutional prior restraint on speech. Restricting a third-party's speech to preserve the "secrecy" of a well-publicized investigation neither serves a compelling interest nor is narrowly tailored. Pet. 25-26; compare *Cutter* v. *Wilkinson*, 544 U.S. 709, 723 n.11 (2005) (prison security is a compelling interest) with *Holt* v. *Hobbs*, 574 U.S. 352, 363 (2015) (marginal gain in prison security from prohibiting inmate from growing short beard is not a compelling interest). And here the government did not even attempt to implement the procedural safeguards needed for a prior restraint. *Southeastern Promotions, Ltd.* v. *Conrad*, 420 U.S. 546, 560 (1975).

Unfortunately, as shown below, similar prior restraints are issued tens of thousands of times a year yet are almost never challenged in court because of the unusual difficulty of bringing such challenges. And, as the events here show, such restraints often do not face proper scrutiny even when litigated. Furthermore, the threat posed by this practice will only grow—and become more difficult to challenge—as third-party cloud storage grows, and as a recent FISA amendment is implemented. These developments will only further expand the use of NDOs—with constitutional implications well beyond the First Amendment. This Court's review is thus both urgent and timely.

I. The NDO Here Violates the First Amendment and Is Symptomatic of the Wide Abuse of Nondisclosure Orders.

The government has numerous avenues to issue NDOs like the one received by Petitioner here. One is the Stored Communications Act (SCA), as used here.[2] Pet. App. 2a-3a; 18 U.S.C. § 2705. Another, perhaps more common avenue involves "National Security Letters (NSLs)" which, as one credible commentator has explained, "are administrative subpoenas that the FBI uses to demand information from Internet service providers without prior judicial approval. They almost always include nondisclosure orders, *** which prohibit the recipient from discussing the letter's contents or even its mere existence"[3]; 18 U.S.C. § 2709.[4] And various FISA provisions offer further opportunities. See, *e.g.*, 50 U.S.C. §§ 1881a(h)(1)(A), 1881b(c)(5)(B); Mot. for Declaratory J. at 7–8, *In Re Motion For Declaratory Judgment That Linkedin May Report Aggregate Data Regarding FISA Orders*, No. 13-07 (FISA Ct. Sept. 7, 2013), available at https://tinyurl.com/5tveeaff.

---

[2] See Alexandra Burke, *When Silence Is Not Golden: The Stored Communications Act, Gag Orders, and the First Amendment*, 69 Baylor L. Rev. 596, 600 (2017).

[3] Rebecca Wexler, *Gags as Guidance: Expanding Notice of National Security Letter Investigations to Targets and the Public*, 31 Berkeley Tech. L.J. 325, 325 (2016); see 18 U.S.C. §§ 2703, 2705, 2709.

[4] Other statutory provisions provide for NSLs but are less relevant to data hosts. See Cong. Rsch. Serv., *RL33320, National Security Letters in Foreign Intelligence Investigations: Legal Background* 1 & n.1 (2015), https://tinyurl.com/57hnzfa9 (noting five different NSL-authorization statutes).

1. Regardless of how they are obtained, because such NDOs are content-based restrictions on speech, they must pass strict scrutiny, and thus must be "narrowly tailored to serve compelling state interests." *Reed* v. *Town of Gilbert,* 576 U.S. 155, 163 (2015) (citations omitted). And, as prior restraints on speech, NDOs face an even higher hurdle: They "must fit within one of the narrowly defined exceptions to the prohibition against prior restraints, and, second, must have been accomplished with procedural safeguards that reduce the danger of suppressing constitutionally protected speech." *Southeastern Promotions,* 420 U.S. at 559 (citing *Bantam Books,* 372 U.S. at 71). Even then, an NDO "comes to this Court bearing a heavy presumption against its constitutional validity." *Id.* at 558 (quoting *Bantam Books*, 372 U.S. at 70).

As Petitioner explains, the NDO here failed to satisfy strict scrutiny. See Pet. 25-30. It is difficult to see how the government could have a compelling interest in maintaining secrecy of details that it had, in substance, already publicized. And it would be truly perverse to claim the government had a compelling interest in circumventing legal rights, such as those afforded by executive privilege, by going through a third party. See *Carpenter* v. *United States*, 585 U.S. 296, 309 (2018) (applying privacy rights to data held by a third party).

The NDO here further fails to satisfy the procedural requirements for prior restraints on speech, and the lower court decisions holding otherwise conflict with precedent from other circuit courts and with the clear text of the Court's precedent in *Freedman* v. *Maryland*, 380 U.S. 51, 58 (1965); Pet.

15-23; see also *Southeastern Promotions*, 420 U.S. at 560 (listing three minimum procedural safeguards). Thus, the NDO clearly violates the First Amendment.

2. Petitioner is far from alone in suffering such violations of its right to speak freely but is nearly alone in its ability to seek judicial review. While NDOs are a common burden on data hosts, they are overwhelmingly difficult to challenge. For instance, Microsoft alone was subject to over 3,000 NDOs issued under the SCA provision here in the 20-month period leading up to May 2016. *Microsoft Corp.* v. *United States Dep't of Just.*, 233 F. Supp. 3d 887, 897 (W.D. Wash. 2017); see also Stephen W. Smith, *Gagged, Sealed & Delivered: Reforming ECPA's Secret Docket*, 6 Harv. L. & Pol'y Rev. 313, 313 (2012) (estimating "tens of thousands of secret cases every year" under the SCA and related provisions of the Electronic Communications Privacy Act). Yet providers rarely challenge these orders, and appeals are even rarer. Smith, *supra,* at 328.

The situation is arguably even worse for NDOs attached to National Security Letters. Even though "tens of thousands of [National Security Letters] are issued each year—and by the government's own estimate, 97% of them may come with a nondisclosure order[,]" a very small number have ever been challenged in federal court. *In re National Sec. Letter*, 930 F. Supp. 2d 1064, 1074 (N.D. Cal. 2013) (citing *Doe* v. *Gonzales*, 500 F. Supp. 2d 379, 405 (S.D.N.Y. 2007), *aff'd in part and rev'd in part on other grounds sub nom. John Doe, Inc.* v. *Mukasey,* 549 F.3d 861 (2d Cir. 2008), *superseded by statute,* USA Freedom Act of 2015, Pub. L. No. 114-23, § 502(f), 129 Stat. 268, 288,

as recognized in In re Three Nat'l Sec. Letters, 35 F.4th 1181 (9th Cir. 2022)).

This is in part by design. NDOs, attached to an NSL or not, facially appear to prohibit disclosure even to a lawyer. Rachel Dallal, *Speak No Evil: National Security Letters, Gag Orders, and the First Amendment*, 33 Berkeley Tech. L.J. 1115, 1116 & n.5 (2018) (noting disclosure is barred to "any person" (quoting 18 U.S.C. § 2709(c)); 18 U.S.C. § 2705(b) (authorizing orders barring disclosure to "any other person").[5] It is unsurprising that many hosting services simply make the risk-averse decision to comply with a plain and blunt reading of the text to avoid potential civil or criminal jeopardy, and thus forego seeking any legal representation.[6]

A further reason for the lack of lawsuits is a misalignment of incentives. Many electronic service

---

[5] FOIA productions make clear that, despite statutory confirmation of a right to disclose the order to a lawyer when attached to an NSL, actual NDOs only sporadically provide notice of this right. See Elec. Priv. Info. Ctr. (EPIC), *Digital Library, Electronic Communications and Privacy Act, Model Gag Applications & Orders: FOIA Production Sept. 5, 2017*, EPIC.org (Aug. 4, 2011) (showing two government templates for proposed nondisclosure orders), https://epic.org/wp-content/uploads/privacy/ecpa/EPIC-16-04-14-DOJ-FOIA-20170905-Production.pdf; compare *id.* at 000003 (noting exception "for the purpose of receiving legal advice") with *id.* at 000011 (stating the target "shall not disclose the existence of the Application or this Order of the Court to any other person unless and until authorized to do so by the Court" without any notice of the exception).

[6] See Elec. Frontier Found., *Issues, National Security Letters: FAQ* (noting confusion about whether the letters can be discussed with a lawyer), https://tinyurl.com/5bhwnufx (last visited July 2, 2024).

providers are not concerned enough about the rights of their clients to spend the time and money needed to litigate in favor of their own speech rights. See Smith, *supra*, at 328 ("The provider's own privacy interests are not at stake, and it is compensated for most expenses of complying with the order. Costs of appeal would almost certainly outweigh any uncompensated inconvenience."). Petitioner's willingness and ability to do so here underscores that this is an ideal vehicle to address the First Amendment harms associated with such NDOs.

II. NDOs Will Become a Worse Threat to First Amendment Rights as Third Party Cloud Storage Becomes More Common and Recent Statutory Changes are Implemented.

Fast-moving market, technological and statutory developments make this Court's review all the more urgent. Constitutional rights, including those protected by the First Amendment, should not exist only "at the mercy of advancing technology," *Carpenter*, 585 U.S. at 305 (quoting *Kyllo* v. *United States*, 533 U.S. 27, 35 (2001)). Any "rule" the Court adopts "must take account of more sophisticated systems that are already in use or in development." *Kyllo*, 533 U.S. at 36.

1. Here, the developing technology requiring a modern translation of historical privacy protection is the extraordinary growth in third-party data hosting. The rise of third-party data hosting offers the government a convenient and growing opportunity to use NDOs to maneuver around a surveillance target's constitutional rights, and thus is likely to lead to more restraints on the speech of the data hosts.

The rise of data centers has been prolific, more than doubling in just 3 years. The United States has gone from approximately 2,600 data centers in 2021 to over 5,300 data centers in 2024. Compare Brian Dagle, Off. of Indus., U.S. Int'l Trade Comm'n, *Data Centers Around The World: A Quick Look* 1 (May 2021)[7] with Cloudscene, *Market Profile: United States of America* (2024).[8] Even this understates the trend: Each data center might be used by multiple hosts, and those hosts might also use overseas data centers.

Such third-party hosting centers are part of a permeating trend, not merely a growing niche. Last year, computer science publisher O'Reilly found that 90% of businesses use some form of off-premise data hosting—including close to half of non-tech-focused small businesses. Cody Slingerland, *101+ Cloud Computing Statistics That Will Blow Your Mind*, CloudZero (updated Jan. 3, 2024), https://tinyurl.com/bdfzx2ta. The data hosted by such third parties is often quite sensitive, and likely to attract the attention of investigative agencies. Personal information such as identification documents, financial information, healthcare records, and social media posts are all increasingly stored in the cloud. *Id.* These, along with data from text and email applications, "reflect[] a wealth of detail about" the "familial, political, professional, religious, and sexual associations" of their users, which likely constitute a majority of the

---

[7] Available at https://tinyurl.com/2h7dkc3n.

[8] Available at https://tinyurl.com/2p9kwyjr. Even if estimates vary, this provides an apples-to-apples comparison, as the 2021 U.S. International Trade Commission report relied on Cloudscene data. See Dagle, *supra.*

U.S. population. *United States* v. *Jones*, 565 U.S. 400, 415 (2012) (SOTOMAYOR, J., concurring).

2. Moreover, the definition of "electronic communication service provider" has recently been expanded to include businesses or associations that have nothing to do with electronic communications at all, but who merely "ha[ve] access to *equipment* that is being or may be used to transmit or store wire or electronic communications," 50 U.S.C. §§ 1881(b)(4)(E), 1885(6)(E) (emphasis added). Thus, the government is now able to issue these NSL-attached NDOs to small businesses who do nothing more than provide a public WiFi network—or who provide no network at all, but simply purchase the necessary equipment to do so later. 18 U.S.C. § 2709(a). This legal development dramatically increases the points of entry available for surveillance under an NSL, and enables the government to choose to issue NSLs, and NDOs raising the same First Amendment issues as the one here, to those data hosts least likely to defend themselves or the targets of surveillance. This development will also likely expand FISA-related NDOs. See, *e.g.*, 50 U.S.C. §§ 1881a(h)(1)(A), 1881b(c)(5)(B) (provisions authorizing nonspecific "secrecy" orders). This Court's guidance will assist the FISC in grappling with its own unique issues.

As long as such data is an easy target for investigative agencies, the data hosts—and with recent legislative developments, virtually any business with an internet connection—will face ever-increasing burdens from an ever-increasing number of NDOs. Yet the decisions below effectively gave the government a license to continue increasing that

burden, without the usual checks and balances. See, *e.g.*, Pet. App. 26a-27a (rejecting *Freedman*'s applicability), 52(a) (admitting that NDOs are a content-based restriction on speech, then applying intermediate scrutiny). That development highlights the need for this Court to clearly articulate that, contrary to the ruling below, NDOs are not exempt from normal First Amendment safeguards.

III. Widespread Use of NDOs Threatens Other Constitutionally Protected Rights, Including Fourth and Sixth Amendment Rights.

This case also has ramifications well beyond data hosts' First Amendment rights. Here, the government used an NDO to circumvent potential executive privilege issues, but such tactics could easily be used to circumvent other rights.

The most obvious application would be similarly subverting the attorney-client privilege, by accessing texts, emails, and voicemails routinely stored by third-party hosts. In criminal cases, this could be used to eviscerate any meaningful Sixth Amendment protections. See, *e.g.*, *Shillinger* v. *Haworth*, 70 F.3d 1132, 1142 (10th Cir. 1995) (intentionally intruding upon defense communications violates Sixth Amendment); *United States* v. *Mastroianni*, 749 F.2d 900, 905 (1st Cir. 1984) (same).

In addition, NDOs pose an extraordinary risk of Fourth Amendment violations, as such orders allow searches for incriminating and private information without any real judicial review. As the Southern District of New York once held, "§ 2709"—the NDO

provision associated with NSLs to electronic communications service providers—"violates the Fourth Amendment because, at least as [then] applied, it effectively bars or substantially deters any judicial challenge to the propriety of an NSL request." *Doe* v. *Ashcroft*, 334 F. Supp. 2d 471, 475 (S.D.N.Y. 2004), *vacated sub nom. Doe* v. *Gonzales*, 449 F.3d 415 (2d Cir. 2006).

While the opinion there was vacated as moot after statutory inclusion of the right to disclose the order to an attorney,[9] in practice, NSL-attached NDOs continue to use broader language, often neglect to mention this right, and thus still deter challenges from all data hosts except those legally savvy enough to know of the exception beforehand. See EPIC, *supra* n.5 (noting FOIA production of sample order prohibiting any disclosure without noting attorney-advice exception). And the NDO provision at issue here still fails to provide such a right at all. 18 U.S.C. § 2705. In any event, the misalignment of incentives—as data hosts may be reluctant or unable to spend time, money, and expertise to protect the rights of an individual who may not even be their direct customer—still "substantially deters" any challenge to the NDO.

Widespread use of NDOs also allows circumvention of the Fourth Amendment by significantly increasing the difficulty of challenging searches of certain types of sensitive data that are almost exclusively stored by third parties, such as cell phone location data. For instance, allowing some meaningful disclosure—

[9] See 18 U.S.C. § 2709(c)(2)(A)(ii).

either to the target or to a court to challenge the propriety of the search on the target's behalf—is necessary to give force to this Court's holding in *Carpenter*, 585 U.S. at 309-310, that individuals have a reasonable expectation of privacy in their location data.

CONCLUSION

Nondisclosure orders, whether obtained under the SCA, accompanying National Security Letters, or obtained through the FISC, pose a grave threat to data hosts' First Amendment rights, and also to a host of other constitutional rights of the government's surveillance targets. But, because of both the nature of the orders and the incentives to challenge them, they are almost never litigated in a meaningful way. This case presents a rare opportunity to clarify the law surrounding NDOs, an issue that will only grow more pressing in light of recent technological and statutory developments. For that reason, and those stated by Petitioner, this Court should grant *certiorari* and reverse the erroneous decision below.

Respectfully submitted,

GENE C. SCHAERR
Counsel of Record
ERIK S. JAFFE
AARON C. WARD
SCHAERR | JAFFE LLP
1717 K Street NW, Suite 900
Washington, DC 20006
(202) 787-1060
gschaerr@schaerr-jaffe.com

Counsel for Amicus Curiae

July 3, 2024