19-1891-cv

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

IN RE GRAND JURY SUBPOENA DATED MARCH 20, 2019

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR ORDER TO DISCLOSE NON-CONTENT INFORMATION

UNITED STATES OF AMERICA,
Appellee,

v.

GOOGLE LLC,
Appellant.

On Appeal from the United States District Court for the Southern District of New York, Nos. 19-MAG-2821, 19-MAG-3232 (Preska, J.)

REDACTED OPENING BRIEF FOR APPELLANT GOOGLE LLC

CATHERINE M.A. CARROLL
JONATHAN G. CEDARBAUM
ARI HOLTZBLATT
ALEX HEMMER
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue NW
Washington, D.C. 20006
(202) 663-6000

September 30, 2019

CORPORATE DISCLOSURE STATEMENT

Appellant Google LLC is a subsidiary of XXVI Holdings Inc., which in turn is a subsidiary of Alphabet Inc., a publicly traded company. No publicly traded company holds more than 10% of Alphabet Inc.'s stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

Page(s)

DOCKETED CASES

STATUTES AND RULES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

INTRODUCTION

This case concerns the constitutionality of two gag orders that restrict Google LLC's First Amendment right to speak about government access to its customers' data. As a provider of cloud storage and computing services, Google strives to maintain the privacy of customer data and to communicate transparently with its customers whenever their data is accessed by third parties, including law enforcement. But here, the government obtained two *ex parte* orders under 18 U.S.C. § 2705(b) prohibiting Google from disclosing to anyone that it had received legal process demanding that it turn over to the government certain enterprise customers' data in connection with a criminal investigation.

The gag orders were issued by magistrate judges based on the government's *ex parte* applications, which Google and its attorneys have never seen. Because the gag orders constitute content-based prior restraints on Google's speech, the magistrate judges should have required the government to submit facts demonstrating that the orders were narrowly tailored to serve a compelling government interest and made their own independent determinations that the government's asserted need for secrecy was justified despite the intrusion on Google's First Amendment rights. But there is no indication on the face of the orders that the magistrate judges held the government to that burden. And when Google moved to vacate the orders on First Amendment grounds, the district court

held that Google did not even have standing to challenge them. The court further held that the orders did not violate the First Amendment because Google had not met a purported obligation to justify a more narrowly tailored approach.

The district court's order should be reversed. Google plainly has standing to bring a First Amendment challenge to orders prohibiting Google's own speech, particularly speech about a matter that is central to Google's business and its relationship with its customers. And the district court failed to apply the correct First Amendment standards in upholding those gag orders. This Court should reconsider the constitutionality of the orders under the proper First Amendment standards or vacate and remand for the district court to do so in the first instance.

JURISDICTIONAL STATEMENT

The district court had jurisdiction under 28 U.S.C. § 1331. *See also* 18 U.S.C. § 2703(d) (permitting service providers to seek review of orders issued under the Stored Communications Act).

This Court has appellate jurisdiction under 28 U.S.C. § 1291 and the collateral-order doctrine. *See In re Grand Jury Subpoena*, 103 F.3d 234, 236 (2d Cir. 1996) (exercising jurisdiction under the collateral-order doctrine in appeal of order closing courtroom and sealing all papers). The collateral-order doctrine allows a court of appeals to review "rulings that … do not end the litigation [but] are appropriately deemed 'final,'" *Mohawk Indus., Inc. v. Carpenter*, 558 U.S. 100,

106 (2009) (quoting *Cohen v. Beneficial Indus. Loan Corp.*, 337 U.S. 541, 545-546 (1949)), because the ruling is conclusive of the issue on appeal, resolves an important question separate from the merits, and would be effectively unreviewable on appeal from a final judgment, *SEC v. Rajaratnam*, 622 F.3d 159, 167 (2d Cir. 2010). All three conditions are met in appeals of disclosure or nondisclosure orders, as this Court has repeatedly recognized. *See United States v. HSBC Bank USA, N.A.*, 863 F.3d 125, 133-134 (2d Cir. 2017) (order unsealing independent monitor report); *SEC v. TheStreet.com*, 273 F.3d 222, 228 (2d Cir. 2001) (order unsealing confidential testimony); *In re Grand Jury Subpoena*, 103 F.3d at 236 (order closing courtroom and sealing all papers); *Application of The Herald Co.*, 734 F.2d 93, 96 (2d Cir. 1984) (same); *Application of Nat'l Broad. Co.* (*NBC*), 635 F.2d 945, 949 n.2 (2d Cir. 1980) (order permitting disclosure of evidence in criminal case).

Here, the district court's order denying Google's motion to vacate the gag orders is conclusive of whether those orders violate the First Amendment. *See TheStreet.com*, 273 F.3d at 228. It resolves an "important question[] separate from the merits," *Rajaratnam*, 622 F.3d at 167, because it does not go to the merits of the underlying criminal investigation, *see TheStreet.com*, 273 F.3d at 228. And it would be effectively unreviewable in an appeal arising out of any criminal

proceeding that followed the investigation, because Google would not be a party to such a proceeding. *See Rajaratnam*, 622 F.3d at 167; *NBC*, 635 F.2d at 949 n.2.

STATEMENT OF THE ISSUES

1. Whether Google has standing to bring a First Amendment challenge to gag orders issued under 18 U.S.C. § 2705(b) that prohibit Google's own speech.

2. Whether the gag orders issued in this case violate the First Amendment.

STATEMENT OF THE CASE

This case arises on appeal from the district court's (Preska, J.) denial of Google's motion to vacate two nondisclosure orders issued under 18 U.S.C. § 2705(b). *See* JA11-51.

A. Statutory Background

Section 2705(b)was enacted over thirty years ago as part of the Stored Communications Act ("SCA"), Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860 (1986). The SCA governs the privacy of electronic communications, including how and under what circumstances law enforcement may obtain certain records from providers of electronic communication services or remote computing services. The SCA authorizes the government to compel a service provider to disclose information about a customer's electronic communications using three types of legal process: a warrant from a court of competent jurisdiction, *see* 18

U.S.C. § 2703(c)(1)(A); a grand jury subpoena or administrative subpoena issued under federal or state law, *see id.* § 2703(c)(1)(E), (2); or a court order (sometimes called a "§ 2703(d) order") based on specific and articulable facts showing reasonable grounds to believe the records are relevant and material to an ongoing criminal investigation, *see id.* § 2703(c)(2)(B), (d). Using these mechanisms, the government can compel a provider to disclose records such as the customer's name, address, and bank account or credit card number, and the dates, times, and locations (*e.g.*, temporarily assigned network addresses) from which the customer used the service. *See id.* § 2703(c)(2).[1]

The SCA does not require the government to inform the customer when it obtains such records from the service provider. 18 U.S.C. § 2703(c)(3).[2] And, as

[1] To compel a provider to disclose the contents of electronic communications, law enforcement must generally obtain a warrant based on probable cause. *See* 18 U.S.C. § 2703(a). Although § 2703(b) purports to allow law enforcement to forgo a warrant in favor of lesser legal process to obtain contents of certain types of communications under certain conditions, that provision has been held unconstitutional, *see United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010), and the Department of Justice has followed that holding as a matter of policy since 2013, *see* H.R. Rep. No. 114-528, at 9 (2016); *see also Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018) (describing as "sensible" a rule that would require the government to seek a warrant to obtain "modern-day equivalents of an individual's own 'papers' or 'effects,' even when those papers or effects are held by a third party").

[2] If the government were to seek contents of customer communications using any legal process less than a warrant, *but see supra* n.1, it would be required to give prior notice to the customer. 18 U.S.C. § 2703(b)(1)(B). But the government

relevant here, § 2705(b) authorizes the government to apply to a court for an order "commanding" the service provider from which the government seeks customer records "not to notify any other person of the existence of the warrant, subpoena, or court order" by which the records are obtained. *Id.* § 2705(b). The court "shall enter" such an order "if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in" any of five enumerated harms: "endangering the life or physical safety of an individual," a person's "flight from prosecution," the "destruction of or tampering with evidence," the "intimidation of potential witnesses," or other "serious[] jeopard[y]" to an investigation or "unduly delaying a trial." *Id.*

The SCA reflects the social and technological landscape of the 1980s—a landscape that is unrecognizable today. In 1986, when the SCA was enacted, "a globally-connected Internet available to the general public for routine e-mail and other uses was still years in the future." *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 206 (2d Cir. 2016), *vacated as moot sub nom. United States v. Microsoft Corp.*, 138 S. Ct. 1186 (2018) (per curiam). Email, when it was sent, was often printed out and delivered in hard copy by courier or the U.S. Postal Service. *See* Kerr, *The Next Generation*

---

can delay that notification for up to ninety days upon a finding that certain adverse results might follow from notification. *Id.* § 2705(a).

Communications Privacy Act, 16 U. Pa. L. Rev. 373, 381 (2014). And there was nothing on the scale of what we today call "cloud computing"—*i.e.*, the storage of personal and enterprise data on servers owned and maintained by third parties like Google and the use of Internet-based tools and virtual computing to facilitate collaboration and communication. *See* Medina, *The Stored Communications Act: An Old Statute For Modern Times*, 63 Am. U. L. Rev. 267, 272-273 (2013).

Today, individuals, companies, educational institutions, and governments alike use cloud computing services to host and manipulate vast quantities of sensitive data—emails, pictures, documents, and more. *See* 51 Computer Scientists Amicus Br. 7, *United States v. Microsoft Corp.*, No. 17-2 (U.S. Jan. 17, 2018) (estimating that "more than a billion people around the world safeguard their private emails and other data" in the cloud). Businesses and organizations increasingly rely on third-party cloud service providers to facilitate communication and collaboration—and to store their most sensitive business documents—rather than using their own servers. Under such arrangements, the enterprise customer contracts with a service provider like Google to host its online business data and email for a fee. The company's accounts may bear the company's domain name (for instance, email addresses ending in "@company.com"), but are stored and supported by the service provider, not by the company itself, on servers owned by the service provider. Today, more companies rely on cloud computing than ever

before: The market for cloud services tops $200 billion, and it is growing at an "[e]xponential[]" rate.[3]

The rapid expansion of cloud computing has had important consequences for federal criminal investigations. As the U.S. Department of Justice recognized in a 2017 white paper, "[p]rior to the advent of widespread cloud services, prosecutors had to approach a company or similar enterprise directly for electronic data stored on servers located on an enterprise's premises." U.S. Dep't of Justice, Crim. Div., Computer Crime & Intellectual Prop. Sec., *Seeking Enterprise Customer Data Held by Cloud Service Providers* 1 (Dec. 2017), https://www.justice.gov/criminal-ccips/file/1017511/download ("2017 DOJ White Paper"). Under this approach, the government would use some form of legal process directed to the enterprise itself to obtain data belonging to the enterprise, its employees, or its customers. In some circumstances, that approach raised the possibility that the subject of the investigation might learn of the investigation's existence, depending on whether the subject of the investigation was the enterprise itself or an employee or customer of the enterprise. But the government could often guard against that risk by going to "an individual within the enterprise"—often the "general counsel or legal

[3] Gartner, Press Release, *Gartner Forecasts Worldwide Public Cloud Revenue to Grow 17.5 Percent in 2019* (Apr. 2, 2019), https://www.gartner.com/en/newsroom/press-releases/2019-04-02-gartner-forecasts-worldwide-public-cloud-revenue-to-g.

representative"—who would "understand law enforcement needs and … the importance of preserving enterprise data." *Id.* at 2. That individual could facilitate the enterprise's compliance with (and potentially help to narrow) the legal request, while also being well positioned to interpose any objections that the enterprise might have to disclosure of the data, including the assertion of constitutional or evidentiary privileges.

The shift to cloud computing, however, has created an opening for the government to seek to use the SCA to circumvent this process. Instead of obtaining records directly from an enterprise, the government sometimes seeks those records from the enterprise's cloud-service provider. In some cases, it does so because it is concerned about the consequences of approaching the enterprise directly. 2017 DOJ White Paper at 2-3. But, as the Justice Department acknowledges, in some cases it does so simply out of convenience—because it believes that approaching the enterprise directly will be too slow or technologically cumbersome. *Id.* at 3. The Department has taken the position that "prosecutors should seek data directly from the enterprise" if possible, rather than seeking legal process against the service provider under the SCA. *Id.* at 2. Such an approach—the traditional approach—"parallels the approach that would be employed if the enterprise maintained data on its own servers, rather than in the cloud." *Id.* And it permits the enterprise to "interpose privilege and other objections to disclosure" on

its own behalf. *Id.* Nevertheless, under the SCA, the government can seek to obtain sensitive data from the service provider without informing the enterprise, *supra* pp. 5-6, and as discussed, § 2705(b) allows the government in some circumstances to obtain a court order prohibiting the cloud-service provider from informing its enterprise customer.

B. Google's Enterprise Cloud Services

Google is a U.S.-based technology company that provides products and services related to the Internet. In addition to well-known services such as Search, Maps, and Gmail, Google also offers several services optimized for enterprise customers to help simplify the workplace—services that involve storing and processing enterprise information in the cloud.[4] One of those enterprise services is called "G Suite"—a productivity suite that includes email, word processing, and applications for storage, spreadsheets, presentations, and calendars, all hosted on Google's servers.[5] Businesses and organizations large and small across a range of industries use G Suite to connect with their employees and customers, create new platforms for presenting and storing their information, and manage their data

[4] Thacker, *5 Million And Counting: How G Suite Is Transforming Work*, Google Cloud Blog (Feb. 4, 2019), https://cloud.google.com/blog/products/g-suite/5-million-and-counting-how-g-suite-is-transforming-work.

[5] *See* G Suite, Features, https://gsuite.google.com/features/ (visited Sept. 30, 2019).

online.[6] Over five million businesses entrust G Suite with their data today, including 64 percent of the Fortune 500. *See Google Cloud Security & Compliance Whitepaper* 23, https://static.googleusercontent.com/media/gsuite.google.com/en//files/google-apps-security-and-compliance-whitepaper.pdf (visited Sept. 30, 2019) ("Security White Paper"). Even governmental agencies, including law-enforcement agencies, use G Suite to secure their most sensitive data.

Recognizing the importance and sensitivity of the data its customers entrust to it, Google takes a "Security First" approach with respect to these products. Google does not purport to own G Suite customer data, Google does not scan the data for advertisements, and Google does not sell G Suite data to third parties. Security White Paper at 12. Indeed, protecting customer data is essential to Google's business. Such protection is a primary design consideration for all of Google's infrastructure, applications, and personnel operations.[7] But security is not simply an engineering issue.

An essential component of Google's "Security First" approach is its commitment to transparency concerning access to customer data. For instance,

---

[6] *Id.*

[7] *See Google Security Whitepaper* 11 (Jan. 2019), https://services.google.com/fh/files/misc/google_security_wp.pdf ("Google Cloud runs on a technology platform that is conceived, designed and built to operate securely.").

Google's contracts with its enterprise customers contain terms requiring Google to notify those customers when the government seeks the customers' confidential information, unless there is an emergency or such disclosure is prohibited by law.[8] Google's transparency permits its customers to make informed decisions about whether and how to use the cloud; it allows those customers to trust Google with the security of their data; and it maintains as much as possible the visibility into data access that Google's enterprise customers would have had before the advent of the cloud, when the enterprise necessarily would have known about government efforts to obtain records from it directly. Google's approach likewise ensures that its customers have the information necessary to interpose relevant legal objections if their data is ever sought by the government—objections that Google cannot always assert on its customers' behalf.

Google's ability to communicate with its customers about law enforcement attempts to access data—rooted in its contractual promises and historical

[8] *See* G Suite (Online) Agreement § 7.2(b), https://gsuite.google.com/terms/2013/1/premier_terms.html (requiring Google to "use commercially reasonable efforts to notify the other party before disclosing that party's Confidential Information in accordance with Legal Process" unless Google "is legally prohibited from giving notice") (visited Sept. 30, 2019); *see also* Businesses and Data, https://privacy.google.com/businesses/security/ ("[W]e work hard to inform businesses about these requests as soon as we can, barring emergency circumstances or where we are prohibited by the legal nature of the request.") (visited Sept. 30, 2019).

commitment to privacy and transparency—is thus essential to Google's business model and customer relationships.

C. Procedural History

On March 20, 2019, the government obtained a grand jury subpoena ordering Google to produce records pertaining to certain enterprise customer accounts and domain names. JA1.[9] The requested records included the names, user names, and addresses associated with the identified accounts, as well as telephone numbers and email addresses, dates of birth and social security numbers, and network address and device identifiers. JA3-4. The subpoena also sought records of the session times and durations and IP addresses associated with the accounts; the length of service, means and source of payment, and list of services used; and all "linked accounts," which the subpoena did not define. *Id.*

Along with the subpoena, the government obtained an order under § 2705(b) prohibiting Google from disclosing to any other person, for a period of one year, the existence of the subpoena or the gag order (except for purposes of receiving legal advice). JA6.[10] The order stated that a magistrate judge had determined

---

[9] The domain names are associated with enterprise customers that appear to be [redacted] *See* JA3-4; *see also* JA9-10.

[10] The rules governing the secrecy of grand jury proceedings do not, of their own force, preclude the recipient of a grand jury subpoena from disclosing it. *See* Fed. R. Crim. P. 6(e)(2). Those rules apply only to grand jurors and certain government officials. *Id.*

based on the government's *ex parte* application, which neither Google nor its attorneys have seen, that there was reason to believe that disclosure of the subpoena's existence would result in "one or more" of the consequences enumerated in § 2705(b)—*i.e.*, endangering an individual's life or safety, flight from prosecution, destruction or tampering with evidence, witness intimidation, "or" seriously jeopardizing an investigation or delaying a trial. *Id.* The order did not specify which of those consequences the magistrate judge found would result if Google notified its customers about the subpoena, made no particularized findings as to why that consequence might result, did not address the possibility of less intrusive means to address any such consequence, and did not mention Google's First Amendment rights.

On April 2, 2019, the government served on Google a court order requiring the production of additional records under 18 U.S.C. § 2703(d). JA7. That order pertained to accounts associated with the same enterprise customer domain names as the subpoena. *See* JA9. In addition to the types of records sought by the subpoena for certain identified accounts associated with the enterprise domains, the § 2703(d) order also demanded the production of records corresponding to unidentified accounts associated with the enterprise domains. JA9-10. For both the identified accounts and the unidentified accounts in the domain, the § 2703(d) order sought to compel (a) "header information" identifying the names, user

names, and IP addresses of the senders and recipients of all communications, including email, along with the date and time stamps of those communications and (b) information for accounts linked by "cookie values, phone number(s), recovery email(s), device(s), or secondary email"—that is, a list of all accounts accessed using the same devices as (or having other links to) all accounts in the domain. *Id.* This demand required Google to turn over information about, for instance, any accounts belonging to friends or family of the account owners, if those accounts were accessed on the account owners' devices or shared the same secondary contact information.

Like the subpoena, the § 2703(d) order was accompanied by a gag order issued under § 2705(b) prohibiting Google from disclosing the existence of the § 2703(d) order to any other person for a period of one year. JA8. The order stated that "it appear[ed]" that disclosure "would seriously jeopardize" the underlying criminal investigation. JA7. Like the gag order accompanying the subpoena, the gag order accompanying the § 2703(d) order made no particularized findings supporting that conclusion, did not address the possibility of less intrusive means, and did not mention Google's First Amendment rights.

Concerned about its inability to inform its enterprise customers about the subpoena and § 2703(d) order, as it ordinarily would do when served with legal process, Google moved to vacate the nondisclosure orders. *See* Mem. of Law in

Support of Mot. to Vacate Gag Orders and Quash or Modify Order Issued Pursuant to 18 U.S.C. § 2703(d), *In re Grand Jury Subpoena to Google, LLC Dated March 20, 2019*, Nos. 19-MAG-2821, 19-MAG-3232 (S.D.N.Y. Apr. 15, 2019) ("Motion"). Google argued that the orders violated its First Amendment rights by restraining Google's speech and were not narrowly tailored to serve a compelling governmental interest, as required by the First Amendment. *Id.* at 13-17.[11] Google explained its general commitment to informing its customers when the government seeks records associated with their accounts. *Id.* at 4. It argued that, among other things, disclosing the existence of the subpoena and § 2703(d) order to the affected enterprise customers would permit those customers to raise any applicable defenses, including [redacted]. *Id.* at 8-13; *see supra* n.9.

The district court denied Google's motion to vacate the gag orders. Adopting an argument the government had not urged, the Court held that Google

[11] Google also moved to quash the subpoena and the § 2703(d) order, which the district court denied. The scope and validity of the subpoena and the § 2703(d) order are not before this Court on appeal.

lacked standing to challenge the gag orders. JA22-23.[12] It also held that Google's First Amendment claims failed in any event. JA23.

As to standing, the district court noted that Google could not raise objections on behalf of its customers and found that Google failed to demonstrate an injury it would suffer itself as a direct result of the gag orders. JA23. Although the court acknowledged Google's argument that the gag orders imposed content-based prior restraints on Google's own speech, it found no actual or imminent injury to Google because, even assuming the gag orders were content-based, they survived strict scrutiny. *Id.* The court therefore found Google's injuries too uncertain or attenuated to support Article III standing. JA23-24.

On the merits, the district court turned first to what it viewed as Google's attempt to raise claims on behalf of its customers, holding that the enterprises whose records the government sought did not have viable constitutional objections to the gag orders or to the subpoena and § 2703(d) order. JA28-41. The district court then rejected Google's argument that the gag orders violated Google's own

[12] While the government argued below that Google lacked standing to challenge the grand jury subpoena and § 2703(d) order—an argument that focused mainly on Google's third-party standing to raise objections on behalf of its customers—the government did not dispute that Google had standing to challenge the gag orders to the extent they infringe on Google's own speech. *See* Gov't Opp. to Google's Motion to Vacate or Amend 8, *In re Grand Jury Subpoena to Google, LLC Dated March 20, 2019*, Nos. 19-MAG-2821, 19-MAG-3232 (S.D.N.Y. Apr. 29, 2019).

First Amendment rights, concluding that, even assuming the orders were content-based, they survived strict scrutiny. JA42. As to Google's argument that the gag orders were not sufficiently tailored in duration, the court stated that Google had "cited to no authority" supporting its argument that a one-year nondisclosure period was too long. JA43. "[T]wo neutral magistrate judges," the court reasoned, had "determined that the year-long [nondisclosure orders] were appropriate," and Google had not shown that their judgment was incorrect. *Id.*

The court also rejected Google's argument that Google should be permitted to inform an "appropriate official" at the enterprises associated with the requested records about the subpoena and § 2703(d) order as a less restrictive manner of serving the government's interests. Although that was the traditional method for the government to obtain enterprise data before the advent of the cloud, *see supra* pp. 8-9, the court found Google's argument "undercut" by the fact that § 2705(b) does not mention such a procedure and instead provides for a complete prohibition on disclosure to any person upon a finding of a "reason to believe" that disclosure would result in an enumerated harm. JA43-45.

The court further rejected Google's argument that the magistrate judge had to make any particularized finding as to which statutory factors justified the issuance of a nondisclosure order, explaining that neither the First Amendment nor Justice Department policy required such particularity. JA46-48.

Finally, the district court found that there were no less restrictive alternatives that would be as effective in achieving the statutory purpose. In so concluding, the court indicated that no such scrutiny was even needed. Citing *Seattle Times Co. v. Rhinehart*, 467 U.S. 20, 32 (1984), and this Court's decision in *Kamasinski v. Judicial Review Council*, 44 F.3d 106, 111 (2d Cir. 1994), the court stated that a statute or order prohibiting disclosure of information "learned solely by means of participating in confidential proceedings or grand jury investigations" is "less restrictive of First Amendment interests" than a prohibition against disclosure of information that is "independently obtained." JA48-49. The court agreed with the government that the gag orders here restrict Google's disclosure of a limited category of information that Google learned about only by receiving legal process and that the orders do not limit Google's right to speak on issues of public importance or to express particular views. JA50. Accordingly, the court found that the gag orders did "'little violence'" to Google's First Amendment rights and therefore were "not invalid because they are narrowly tailored to achieve the Government's compelling interest in the integrity of its ongoing, covert criminal investigation." JA50-51.

Google timely appealed. JA95.

SUMMARY OF ARGUMENT

The district court erred twice over: Google has Article III standing to bring a First Amendment challenge to gag orders that prohibit Google's own speech, and the court failed to hold the government to the appropriate burden in analyzing the validity of those orders under the First Amendment.

First, Google plainly has standing to bring a First Amendment challenge to the gag orders. Those orders expressly and immediately prohibit Google's own speech, precluding Google from engaging in communication that it views as essential to its mission and its relationship with its customers. Such a prohibition is a paradigmatic restriction on speech and a paradigmatic injury for purposes of Article III standing. The district court reached the opposite conclusion only by making a series of errors. Most notably, the court conflated the standing analysis (whether Google is injured by the gag orders) and the merits analysis (whether the orders are constitutional). The court also erroneously concluded that Google's injury was too uncertain to support standing, and it improperly confused the injury to Google's speech rights with the injury to Google's customers that arises from the government's resort to secrecy.

Second, the district court failed to hold the government to its burden in rejecting Google's First Amendment argument on the merits. The gag orders constitute content-based prior restraints on Google's speech. The government

therefore bore the burden to establish that the orders are narrowly tailored to serve a compelling governmental interest—that is, it was the government's burden to prove a compelling purpose for the orders and that no less restrictive alternative orders would have sufficed to meet that purpose. But neither the magistrate judges nor the district judge required that showing—notwithstanding the court's lip service to the strict-scrutiny standard—or clearly made an independent determination that the government had proved a need for secrecy that outweighed Google's First Amendment rights.

The gag orders themselves make no reference to the First Amendment and reflect no particularized findings about the harms that would occur if the subpoena or § 2703(d) order were disclosed or why those harms could not be alleviated through a less restrictive order. Indeed, one of the gag orders does not even specify which of the statutorily enumerated grounds the magistrate judge found to be satisfied. The magistrate simply found that "one or more" of the enumerated harms would occur. JA6. In rejecting Google's motion to vacate, the district court then erred—despite reciting the narrow-tailoring requirement—by repeatedly placing the burden on Google to show why the gag orders were not warranted rather than requiring the government to demonstrate that the orders were justified despite the imposition on Google's First Amendment rights.

This Court should clarify that Google has standing and hold the government to its burden under the First Amendment by requiring it to demonstrate that the gag orders are narrowly tailored to serve a compelling state interest and that no less restrictive alternative could protect that interest. The Court should review the record, including the government's *ex parte* submission, and apply the correct standard in deciding whether the gag orders should be vacated. Alternatively, this Court should clarify the relevant substantive and procedural standards a court must apply to ensure that a gag order complies with the First Amendment and remand the case to the district court to apply those standards.

STANDARD OF REVIEW

This Court reviews orders compelling or prohibiting disclosure of information for abuse of discretion, but reviews issues of law underlying such orders de novo. *See SEC v. TheStreet.com*, 273 F.3d 222, 228 (2d Cir. 2001) (lifting of protective order); *United States v. Doe*, 63 F.3d 121, 125 (2d Cir. 1995) (closing of courtroom); *see also In re Grand Jury Subpoena*, 103 F.3d 234, 236 (2d Cir. 1996) ("We review the issues of law related to the district court's closure order *de novo*."). Here, the denial of Google's motion to vacate rests on questions of law; accordingly, this Court's review is de novo. *See Citizens United v. Schneiderman*, 882 F.3d 374, 380 (2d Cir. 2018) (First Amendment); *Kreisler v. Second Ave. Diner Corp.*, 731 F.3d 184, 187 n.3 (2d Cir. 2013) (standing).

ARGUMENT

I. GOOGLE HAS STANDING TO CHALLENGE THE GAG ORDERS BECAUSE THEY INFRINGE ON GOOGLE'S OWN FIRST AMENDMENT RIGHTS

The district court first denied Google's motion to vacate the gag orders on the ground that Google lacked standing to challenge them. JA23-24, 27-28. That conclusion is wrong. Google has standing to challenge the orders because they impose a direct and immediate restriction on Google's right to speak.

A. Google Meets All Three Requirements For Article III Standing

A party has standing to challenge an invasion of its First Amendment rights if it establishes injury-in-fact, causation, and redressability. *See National Org. for Marriage, Inc. v. Walsh*, 714 F.3d 682, 688 (2d Cir. 2013); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-561 (1992). Google meets each of those elements.

First, the gag orders plainly give rise to injury-in-fact, as they restrain Google from speaking about the grand jury subpoena and the § 2703(d) order to its customers or anyone else. A restriction on speech is a paradigmatic injury-in-fact. *See Alexander v. United States*, 509 U.S. 544, 550 (1993); *Able v. United States*, 88 F.3d 1280, 1288 (2d Cir. 1996) ("[E]ven minimal impairments on [the right to free speech] create … injury."). And a party barred by the government from engaging in protected speech—that is, a party subject to a prior restraint—has Article III standing to challenge the state action barring its speech. *See, e.g.*, *Susan B.*

Anthony List v. Driehaus, 573 U.S. 149, 158 (2014); *Virginia v. Am. Booksellers Ass'n*, 484 U.S. 383, 392 (1988); *National Org. for Marriage*, 714 F.3d at 689.

In purpose and effect, an order issued under § 2705(b) operates as a restriction on speech: The order "command[s]" a provider of an electronic communication service or remote computing service "not to notify any other person" about the existence of the related warrant, subpoena, or court order. 18 U.S.C. § 2705(b). A "command[] … not to notify" another person about something is a classic restriction on speech, and courts in jurisdictions across the country have thus had no difficulty characterizing a § 2705(b) order as an imposition on providers' First Amendment rights. *See, e.g.*, *In re Search Warrant Issued to Google, Inc.*, 269 F. Supp. 3d 1205, 1215 (N.D. Ala. 2017) ("§ 2705(b) constitutes a prior restraint on speech and a content-based speech restriction"); *Microsoft Corp. v. U.S. Dep't of Justice*, 233 F. Supp. 3d 887, 899-900 (W.D. Wash. 2017) (finding standing based on the alleged impairment of service provider's "'legally protected interest' in speaking about government investigations due to … orders issued pursuant to Section 2705(b)"); *In re Grand Jury Subpoena for [Redacted]@yahoo.com*, 79 F. Supp. 3d 1091 (N.D. Cal. 2015) (agreeing that a § 2705(b) order "would amount to a[] … prior restraint of Yahoo!'s First Amendment right to inform the public of its role in searching and seizing its information"). Indeed, Google is aware of no decision other than the

opinion below in which a court has found that the recipient of a § 2705(b) order was not injured by that order for purposes of Article III standing. *Cf. In re Nat'l Security Letter*, 863 F.3d 1110, 1121 (9th Cir. 2017) (considering provider's challenge to nondisclosure regime governing national security letters without addressing standing); *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 870 (2d Cir. 2008) (similar).[13]

The restraint on speech imposed by the gag orders here is particularly harmful to Google because it compromises a core element of Google's mission—its commitment to transparency in maintaining the privacy and security of customer data. As discussed, *see supra* pp. 11-12, Google promises its customers that it will inform them when law enforcement seeks to obtain their data except in an emergency or where it is unlawful to do so. That transparency is an important part of Google's efforts to ensure that its customers retain as much ownership and control over their data in the cloud as they would have over data on their own servers. By impeding Google's ability to engage in such communication with its

[13] The district court cited *In re Grand Jury Subpoena Issued to Twitter, Inc.*, No. 3:17-mc-40-M-BN, 2017 WL 9287146, at *5 (N.D. Tex. Sept. 22, 2017), *report and recommendation adopted*, 2017 WL 9287147 (N.D. Tex. Oct. 19, 2017), but the standing analysis in that decision concerned the service provider's challenge to a subpoena, not its separate challenge to the § 2705(b) gag order that accompanied that subpoena. *See id.* at *4-5. Indeed, far from holding that the service provider lacked standing to challenge the gag order, the court grant the provider's motion to vacate it. *Id.* at *7.

customers, the gag orders undermine Google's relationship with its customers and its commitment to safeguard the privacy and security of customer data—a significant injury-in-fact that is more than adequate to establish Article III standing.

The second and third prongs of the standing inquiry—causation and redressability—are likewise satisfied here. *See National Org. for Marriage*, 714 F.3d at 688. The gag orders are—literally—the cause of the imposition on Google's First Amendment rights. Without the orders, Google would be free (and, indeed, contractually obligated) to inform its customers about the government's requests for their records. And if the gag orders were set aside or narrowed as a result of Google's motion to vacate, Google could notify its customers about the subpoena and § 2703(d) order, thus redressing the injury to its First Amendment rights. There should thus be no dispute that Google has standing.

B. The District Court's Standing Analysis Is Fundamentally Flawed

The district court nevertheless concluded that Google lacked standing to challenge the § 2705(b) gag orders. That decision rests on three related errors.

First, the court conflated the question whether Google has standing with the question whether Google's challenge should succeed on the merits. The district court understood Google to be arguing that it had standing because the gag orders impose "content-based prior restraints on Google's speech." JA23. But the court

then rejected Google's standing on the ground that, in the court's view, even "assuming the [nondisclosure orders] are content-based, … they survive strict scrutiny." *Id.* That merits-first approach is incorrect. The question whether a party has standing to challenge a government action should be "resolved irrespective of the merits" of that challenge. *Brooklyn Legal Servs. Corp. v. Legal Servs. Corp.*, 462 F.3d 219, 227 (2d Cir. 2006); *accord Dean v. Blumenthal*, 577 F.3d 60, 66 n.4 (2d Cir. 2009). The district court erred in conflating the two.

Second, the district court asserted without explanation that any intrusion on Google's First Amendment rights was unlikely to actually occur—that is, that Google's claimed injuries were "neither 'actual nor imminent' because they [were] not 'certainly pending' nor is 'there a substantial risk that [they would] occur.'" JA23 (citation omitted). That conclusion is plainly incorrect. The gag orders do not impose some distant or contingent restriction on Google's speech; they impose an immediate prohibition on Google's ability to engage in certain speech with its customers or anyone else. This is likewise not a case in which a speaker alleges only a "subjective chill" on speech. *Latino Officers Ass'n v. Safir*, 170 F.3d 167, 170 (2d Cir. 1999). The gag orders explicitly and presently bar Google from telling its customers that it has been compelled to produce their data to the government. That injury is immediate and actual.

Finally, the district court appears at times to have understood Google to be asserting harms to the rights of its customers. *See* JA22-23 (citing doctrine of third-party standing). But Google did not ask the district court to adjudicate its customers' First Amendment rights. Google argued that the gag orders impair its own First Amendment rights. The objections that Google's customers might interpose to the grand jury subpoena and the § 2703(d) order constitute a key reason why the suppressed speech is so important to Google. *See* Motion 8. For example, [redacted]. For many reasons, Google is not well-positioned to assert those objections on behalf of its customers, which is in part why speaking freely about the orders is so important to Google's business. But the injury asserted here is an injury to Google itself, in the form of a restriction on Google's own speech. The district court fundamentally misunderstood that point and erroneously denied standing on that basis.

II. THE GAG ORDERS VIOLATE THE FIRST AMENDMENT

The district court likewise erred in sustaining the gag orders against Google's First Amendment challenge by failing to hold the government to its

burden to justify the intrusion on Google's speech rights. The gag orders should therefore be reexamined under the proper standard.

A. The Gag Orders Are Content-Based Prior Restraints Subject To Strict Scrutiny

The First Amendment prohibits the government from abridging the freedom of speech. Although First Amendment rights are not absolute, gag orders like those issued here sit at the intersection of two core First Amendment protections—the protection against prior restraints (*i.e.*, governmental acts that forbid speech before it occurs) and the protection against content-based restrictions of speech.

First, a § 2705(b) gag order constitutes a prior restraint—the "most serious and the least tolerable infringement on First Amendment rights," *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 559 (1976), which "comes to [a court] with a 'heavy presumption' against its constitutional validity," *Organization for a Better Austin v. Keefe*, 402 U.S. 415, 419 (1971). A court order "forbidding certain communications when issued in advance of the time that such communications are to occur" is a paradigmatic prior restraint. *Alexander v. United States*, 509 U.S. 544, 550 (1993) (emphasis and quotation marks omitted). A gag order under § 2705(b) operates in exactly that manner: It is a "predetermined judicial prohibition restraining specified expression." *In re Sealing & Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 881 (S.D. Tex. 2008). For that reason, courts have concluded that such orders constitute prior restraints. *Id.*; *see*

also Microsoft Corp. v. U.S. Dep't of Justice, 223 F. Supp. 3d 887, 905 (W.D. Wash. 2017).

Second, a § 2705(b) gag order imposes a content-based restriction on speech. A restriction on speech is content-based if it "applies to particular speech because of the topic discussed or the idea or message expressed." *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2227 (2015). By "target[ing] speech based on its communicative content," such a restriction—like a prior restraint—is "presumptively unconstitutional." *Id.* at 2226. A gag order under § 2705(b) is content-based because it "effectively preclude[s] speech on an entire topic—the electronic surveillance order and [the] underlying criminal investigation." *In re Sealing*, 562 F. Supp. 2d at 881-882; *see also In re Nat'l Sec. Letter*, 863 F.3d at 1123 (national security letter nondisclosure requirement "is content based on its face").

Because a § 2705(b) gag order is a content-based prior restraint, two consequences follow. First, because the order operates as a prior restraint, it can be issued only pursuant to the "procedural safeguards" that the Supreme Court described in *Freedman v. Maryland*, 380 U.S. 51 (1965)—safeguards "that reduce the danger of suppressing constitutionally protected speech," *Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 559 (1975). Specifically, "expeditious judicial review" is required, and "the censor must bear the burden of going to court

to suppress the speech and must bear the burden of proof once in court." *Thomas v. Chicago Park Dist.*, 534 U.S. 316, 321 (2002); *see John Doe, Inc.*, 549 F.3d at 871. Second, because the order is both content-based and a prior restraint, the highest level of substantive scrutiny applies. *See Reed*, 135 S. Ct. at 2227 (content-based laws must "satisfy strict scrutiny"); *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963) (prior restraint comes to court "bearing a heavy presumption against its constitutional validity"). Before issuing a gag order, a court must find that the order is "narrowly tailored to serve compelling state interests," *Reed*, 135 S. Ct. at 2226, and that there are no "less restrictive alternatives [that] would be at least as effective" as the order, *Reno v. ACLU*, 521 U.S. 844, 874 (1997).

When the government seeks to justify a gag order on the ground that disclosure would likely result in a statutorily enumerated harm, the government "must at least indicate the nature of the apprehended harm and provide a court with some basis to assure itself (based on *in camera* presentations where appropriate) that the link between disclosure and risk of harm is substantial." *John Doe, Inc.*, 549 F.3d at 881. A court "cannot, consistent with strict scrutiny standards, uphold a nondisclosure requirement" based on the government's "conclusory assurance that such a likelihood exists." *Id.* Rather, to support a gag order under § 2705(b), a court must make its own determination—and the government must submit facts

sufficient to support that determination—that the gag order is necessary to serve a compelling governmental interest and that the scope and duration of the order are narrowly tailored to advance that interest. *See Reed*, 135 S. Ct. at 2226.

Below, the government argued, and the district court at times appeared to agree, that the government did not have to meet these standards because the gag orders foreclose only a limited category of speech on a subject that Google knows about only because of the grand jury subpoena and § 2703(d) order demanding production of customer data to the government. The court analogized the gag orders to rules prohibiting the disclosure of information obtained during confidential proceedings to review misconduct complaints against judges, *see Kamasinski v. Judicial Review Council*, 44 F.3d 106, 110-112 (2d Cir. 1994), or obtained through pretrial discovery, *see Seattle Times Co. v. Rhinehart*, 567 U.S. 20, 31-32 (1984). *See* JA48-51.

The district court's reasoning conflicts with this Court's decision in *John Doe, Inc.*, 549 F.3d 861. *John Doe, Inc.* considered a constitutional challenge to one of the statutes that authorized issuance of national security letters ("NSLs"), many of which, like a § 2705(b) order, bar the recipient from disclosing that the recipient has been compelled to produce records to the government. The plaintiffs argued that the NSL statute operated as a "content-based prior restraint that must be tested against all the substantive and procedural limitations applicable to such

an impairment of expression." *Id.* at 873. In response, the government made the same argument that it advanced below in this case—that the restrictions on speech imposed by the NSL statute were permissible under a less demanding constitutional standard because they suppressed not "a pre-existing desire to speak," but only speech resulting from "governmental interaction with" the recipient of legal process. *Id.* at 874 (citing *Kamasinski*, 44 F.3d 106, and *Rhinehart*, 467 U.S. 20).

This Court rejected the government's proposed analogy. *John Doe, Inc.*, 549 F.3d at 876-877. The cases relied upon by the government, the Court reasoned, arose in the context of discrete and temporary proceedings in which "the justification for … secrecy" inhered in "the nature of the proceeding." *Id.* The Court saw no similarity between the parties seeking disclosure in those cases and the plaintiff before it, which "had no interaction with the Government" until the government demanded that the plaintiff produce certain records and "imposed [a] nondisclosure requirement upon it." *Id.* at 878. The same is true here. Unlike a litigant in a civil suit (as in *Rhinehart*) or a participant in a misconduct proceeding (as in *Kamasinski*), Google is not being asked to keep silent about information it learned only through its participation in a secret proceeding; it is being forced to stay silent about actions the government demanded that it take on a subject that is central to its business. And like the nondisclosure orders in *John Doe, Inc.*, the gag

orders here are not inherent to a secret proceeding but were "imposed at the demand of the Executive Branch under circumstances where secrecy might or might not be warranted, depending on the circumstances alleged to justify such secrecy." *Id.* at 877.[14]

John Doe, Inc. establishes that strict scrutiny must govern a court's decision whether to issue (or vacate) a gag order and whether "the circumstances alleged to justify such secrecy" in fact exist. Although the Court in that case declined to definitively resolve the applicable standard of review, it did so only because the statute's constitutional defects were apparent under either traditional strict scrutiny or a standard that was "not quite as 'exacting' a form of strict scrutiny." *John Doe, Inc.*, 549 F.3d at 878. The Court should make clear here that the § 2705(b) gag orders here are content-based prior restraints on speech that are subject to strict scrutiny—the standard actually applied in *John Doe, Inc.* *Id.* at 878.

[14] That one of the gag orders at issue in this case relates to a grand jury subpoena does not support the district court's analysis. As noted, *supra* n.10, the secrecy rules applicable to grand juries and discussed in *John Doe, Inc.* apply only to certain persons and only to proceedings before the grand jury itself. *See* Fed. R. Crim. P. 6(e)(2)(B). Those rules do not impose any obligation of secrecy on grand jury witnesses or recipients of grand jury subpoenas. *See* Fed. R. Crim. P. 6(e)(2); *see also* Fed. R. Crim. P. 6(e)(2)(A) ("No obligation of secrecy may be imposed on any person except" those enumerated in Rule 6(e)(2)(B)); *In re Application of USA for an Order Pursuant to 28 U.S.C. § 1651(a) Precluding Notice of a Grand Jury Subpoena*, No. 19-wr-10, 2019 WL 4619698, at *2-3 (D.D.C. Aug. 6, 2019) (addressing inapplicability of Rule 6(e) to recipients of grand jury subpoenas).

B. The Government Bears The Burden To Demonstrate, And The Court Must Independently Determine, That The Gag Orders Are Narrowly Tailored To Serve A Compelling Governmental Interest And That No Less Restrictive Alternative Is Available

Strict scrutiny requires the government to prove that a gag order is "narrowly tailored to serve compelling state interests." *Reed*, 135 S. Ct. at 2226. Even in an *in camera, ex parte* proceeding, that standard requires the government to proffer specific facts to support its asserted interest in obtaining a gag order. It requires the court to consider both the government's interests in nondisclosure and the provider's First Amendment rights, based on the record before the court. And it requires the court to make an independent determination—without simply accepting the government's representations—that the gag order is authorized and consistent with the First Amendment. *See John Doe, Inc.*, 549 F.3d at 881 (reviewing court cannot "uphold a nondisclosure requirement on a conclusory assurance" that a statutory standard is satisfied); *id.* at 882 (court must "balance 'the potential harm against the particular First Amendment interest raised by a particular challenge,'" and doing so is "an important aspect of judicial review of prior restraints").

The narrow-tailoring analysis will almost always require a reviewing court to consider a number of applicable factors. For instance, as the Justice Department explained in a 2017 policy memorandum, the duration of a nondisclosure order is an important factor in determining whether it is narrowly tailored. *See*

Memorandum from Deputy Attorney General Rod J. Rosenstein to Heads of Department Law Enforcement Components et al. at 2 (Oct. 19, 2017), https://www.justice.gov/criminal-ccips/page/file/1005791/download ("Rosenstein Memorandum"); *see also Microsoft Corp.*, 233 F. Supp. 3d at 908 (explaining that "indefinite nondisclosure orders impermissibly burden … First Amendment rights"). The breadth of the underlying production order is likewise relevant: The broader the scope of the request or the greater the number of customers whose data is sought, the more speech is suppressed by the gag order and the greater the imposition on the cloud provider's First Amendment rights. Here, for example, Google has been silenced from speaking at all about a subpoena and § 2703(d) order that broadly demanded production of all subscriber and header information for all accounts registered under domain names [redacted], as well as a list of all accounts (no matter whom they belong to) that are "linked" to the target accounts by any common device, cookies, or secondary contact information. JA3-4, 9-10.

Moreover, where the government seeks records associated with an organization, courts' obligation to ensure that "there are no 'less restrictive alternatives,'" *John Doe, Inc.*, 549 F.3d at 878 (quoting *Reno*, 521 U.S. at 874), means that they must ask whether a gag order prohibiting all disclosures to any person is truly necessary, or whether records can be obtained directly from the

organization or with the knowledge of the organization's legal representative without compromising the integrity of the investigation. As described above, *supra* pp. 8-9, for decades the government obtained records directly from enterprises associated in some way with the subject of an investigation despite the risk that doing so could result in the disclosure of the investigation to the subject. The government managed that risk by approaching "an individual within the enterprise who is an appropriate contact for securing the data"—generally, "the general counsel or legal representative." 2017 DOJ White Paper 2. The expansion of cloud computing does not obviate that alternative course of action. Indeed, as the Department explained in 2017, "prosecutors *should* seek data directly from the enterprise" where practical by dealing with the enterprise's legal representatives. *Id.* (emphasis added). A prosecutor seeking instead to obtain data from a cloud provider under a broad gag order prohibiting the provider from disclosing anything to its enterprise customer should be required to demonstrate that the less restrictive alternative of allowing the provider to disclose the legal process to the enterprise's legal representative is impossible (and that the government is not seeking records from the provider merely because it is more convenient than seeking them from the enterprise). *Reno*, 521 U.S. at 874.

As to each of these factors, a reviewing court cannot rely on the government's "conclusory assurance[s]" in issuing a gag order. *John Doe, Inc.*,

549 F.3d at 881. Instead, the court must make its own determination, based on facts submitted by the government, that the need for secrecy is justified and that the government's interests cannot be safeguarded in a manner that imposes a lesser burden on the service provider's First Amendment rights. *Id.*

C. The District Court Failed To Hold The Government To Its Burden

Neither Google nor its attorneys—including undersigned counsel—have seen the *ex parte* applications that the government submitted in support of its requests for the two gag orders at issue. But on their face, the gag orders give no indication that the government met its burden under the First Amendment. And although the district court at times referred to the strict-scrutiny standard, its analysis in substance did not hold the government to that burden.

There is no indication that the magistrate judges held the government to the appropriate standard or even understood themselves to be under a duty to issue "narrowly tailored" orders in the first instance. The March 20, 2019 gag order—the order accompanying the grand jury subpoena—is facially insufficient. That order rests only on the magistrate judge's determination that "one or more" of the enumerated statutory factors is present. JA6. That indeterminate finding suggests that the government failed to establish a specific reason justifying the gag order and that the magistrate did not consider whether the gag order was narrowly tailored to serve any particular interest. If a court cannot "uphold a nondisclosure

requirement on a conclusory assurance" that a statutory standard is satisfied, *John Doe, Inc.*, 549 F.3d at 881, a court certainly cannot do so on the basis that, in its view, "one or more" of the relevant standards are met. "[T]he Government must at least indicate the nature of the apprehended harm." *Id.*[15]

While the April 2, 2019 gag order—the one accompanying the § 2703(d) order—does specify which harm the court believed would follow from disclosure of the § 2703(d) order, the April 2 order also does not appear to be narrowly tailored. For instance, the gag order gives no indication that the government presented any case-specific facts in support of its *ex parte* application, rather than simply relying on insufficient "boilerplate assertions" that not all subjects are aware of the ongoing investigation. *See In re Grand Jury Subpoena to Facebook*, No. 16-mc-1300, 2016 WL 9274455, at *4 (E.D.N.Y. May 12, 2016). As one court in this Circuit has observed, "there is simply no reason to presume that disclosure of [a] subpoena to the customer whose records the government seeks will harm the investigation in any way." *Id.* Rather, the government must make a

[15] The district court rejected this argument on the ground that a Justice Department memorandum issued in 2017 "contemplates" that prosecutors may obtain § 2705(b) orders without specifying the harm that would follow from the disclosure of the existence of legal process. *See* JA46 (citing Rosenstein Memorandum 2). But the memorandum in fact states that a prosecutor "should identify which of the [enumerated] factors … apply and explain why." Rosenstein Memorandum 2. To the extent the memorandum condones a failure to do so, it contravenes the constitutional requirements this Court has identified. *See supra* pp. 35-38.

factual showing about, among other things, "the relationship, if any, between the customer whose records are sought and any target of the investigation." *Id.* Nothing on the face of the April 2 gag order suggests the government made such a showing here, and the magistrate judge thus made only a conclusory finding that it "appear[ed]" that disclosure would jeopardize the investigation. JA7. There is likewise no indication that the magistrate judge considered the impact of the order on Google's First Amendment rights or the availability of less restrictive alternatives, rather than merely determining whether the statutory standards were satisfied. *Id.*

The district court's analysis was likewise deficient. In denying Google's motion to vacate, the district court repeatedly refused to hold the government to its burden to show that the gag orders were narrowly tailored, instead deferring to the magistrate judges' willingness to issue the orders and placing a burden on Google to show that the magistrate judges had erred. The district court repeatedly returned to the fact that "neutral magistrate judges" had issued the gag orders. *See, e.g.*, JA14, 26, 33, 44 n.13, 45. And it repeatedly rejected Google's arguments that the government should be required to justify any aspect of the orders—their duration, their scope, or the grounds on which they were issued.

Google argued, for instance, that the government should be required to show that a shorter period would not satisfy its purposes. But the district court rejected

that argument, criticizing Google for failing to "cite[] … authority supporting its baseless assertion" that a one-year order *might* not be appropriate in a given case. JA43. That gets the analysis exactly backwards. It is not Google's burden to show that the order is not narrowly tailored; it is the government's burden to show that it is. *See Reed*, 135 S. Ct. at 2227; *Thomas*, 534 U.S. at 321 ("[T]he censor must … bear the burden of proof once in court.").

The district court similarly did not require the government to show that there were no "'less restrictive alternatives,'" *John Doe, Inc.*, 549 F.3d at 878 (quoting *Reno*, 521 U.S. at 874)—including, in the context of a request for enterprise records, why it would not be acceptable to allow Google to alert an attorney at the enterprise with responsibility for enterprise-level data about the request. As described above, *see supra* pp. 8-9, legal representatives often play such a gatekeeping role for enterprises, and before the advent of cloud computing, the government routinely had to take exactly that approach to obtain the records it sought. The district court should have required the government to demonstrate why allowing a carefully limited disclosure to the enterprise customers' legal representatives is not a "less restrictive alternative" that would serve the government's interests without imposing the broadest possible gag order.

The court rejected this argument out of hand on the ground that § 2705(b) does not require the government to follow such a procedure. JA44. But

compliance with the statute alone does not answer the First Amendment question. *See John Doe, Inc.*, 549 F.3d at 871 ("Once constitutional standards have been authoritatively enunciated, Congress may not legislatively super[s]ede them."). *Freedman* and its progeny establish as much. Those decisions require expeditious judicial review of prior restraints to test not only whether the government has an interest in suppressing speech, but whether that interest outweighs the particular First Amendment interests of the particular speaker in a particular case. *See Southeastern Promotions*, 420 U.S. at 560-561 (decision to suppress speech must be made by a "court" that is "responsive … to constitutionally protected interests in free expression"); *Freedman*, 380 U.S. at 58 (explaining that "only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression").

The district court also reasoned that a less restrictive procedure was not necessary because "a neutral magistrate judge" had already "balanc[ed] … First Amendment interests with the Government's interest." JA45. But as noted, there is no indication that the magistrate judges here in fact did conduct such a balance or even understood themselves to be conducting a constitutional analysis. And even if they had, the fact that a magistrate judge has issued a § 2705(b) order cannot absolve the district court of its responsibility to conduct a de novo review of the First Amendment question. *See In re Search of Info. Associated with*

[redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-00757, 2017 WL 3445634, at *2-5 (D.D.C. July 31, 2017). As the Supreme Court explained in *Freedman*, "only a judicial determination in an *adversary proceeding* ensures the necessary sensitivity to freedom of expression," 380 U.S. at 58 (emphasis added), and it is only before the district court that any adversarial consideration of a gag order's impact on the service provider's rights can occur.

Google and its attorneys do not and cannot know what particular interests the government asserted here, what if any facts or evidence the government adduced to substantiate those interests, or whether those interests truly justified the broadest possible year-long gag order despite the availability of less restrictive alternatives. Only a court can make that decision on the basis of the government's *ex parte* submissions. But it must do so under the correct legal standard, holding the government to its burden to demonstrate that the gag order and the resulting intrusion on free speech is truly necessary. The government's sealed submissions are presumably in the record, and this Court is well positioned to conduct that analysis on de novo review. Alternatively, the Court should identify the governing legal principles, vacate the order denying Google's motion to vacate, and remand to the district court to reexamine the gag orders under the correct standard. *See John Doe, Inc.*, 549 F.3d at 885 ("remand[ing] so that the Government may have

an opportunity to sustain its burden of proof and satisfy the constitutional standards we have outlined for maintaining the disclosure requirement").

CONCLUSION

The district court's order denying Google's motion to vacate should be reversed or else vacated and remanded for the district court to apply the correct legal standard.

Respectfully submitted,

/s/ Catherine M.A. Carroll
CATHERINE M.A. CARROLL
JONATHAN G. CEDARBAUM
ARI HOLTZBLATT
ALEX HEMMER
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 663-6000

September 30, 2019

CERTIFICATE OF COMPLIANCE

The foregoing brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B)—as modified by Local Rule 32.1(a)(4)(A)—in that the brief, according to the word-count feature of the word-processing system with which it was prepared (Microsoft Word), contains 10,355 words.

/s/ Catherine M.A. Carroll
CATHERINE M.A. CARROLL

CERTIFICATE OF SERVICE

I hereby certify that, on September 30th, 2019, I filed the Sealed Opening Brief of Appellant Google LLC and the Sealed Joint Appendix with the Clerk of the Court by hand. I served these documents on all parties by sending paper and electronic copies of the documents to the address listed below:

Nicolas Roos
United States Attorney's Office, Southern District of New York
One St. Andrew's Plaza
New York, NY 10007
nicolas.roos@usdoj.gov

Counsel for the United States

/s/ Catherine M.A. Carroll
CATHERINE M.A. CARROLL