20-1653(L),

20-3945(Con)

UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

IN RE: IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH SPECIFIED E-MAIL ACCOUNTS

MICROSOFT CORPORATION,
Appellant,
v.
UNITED STATES OF AMERICA,
Appellee.

On Appeal from the United States District Court for the Eastern District of New York, No. 18-mj-723 (Donnelly, J.)

BRIEF FOR AMICI CURIAE AMAZON.COM, INC., APPLE INC., AND GOOGLE LLC IN SUPPORT OF APPELLANT MICROSOFT CORPORATION AND REVERSAL

DANIEL S. SILVER
CHRISTOPHER J. MORVILLO
CLIFFORD CHANCE US LLP
31 West 52nd Street
New York, NY 10019
(212) 878-8000

Counsel for Amazon.com, Inc.

CATHERINE M.A. CARROLL
ARI HOLTZBLATT
ALEX HEMMER
JORDAN E. OROSZ
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue NW
Washington, DC 20006
(202) 663-6000

Counsel for Apple Inc. and Google LLC

December 21, 2020

CORPORATE DISCLOSURE STATEMENT

Amazon.com, Inc. has no parent corporation and no publicly held corporation owns 10% or more of Amazon.com's stock.

Apple Inc. has no parent corporation and no publicly held corporation owns 10% or more of Apple's stock.

Google LLC is an indirect subsidiary of Alphabet Inc., a publicly traded company. Alphabet Inc. does not have a parent company and no publicly traded company holds more than 10% of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

Page(s)

STATUTES, RULES, AND REGULATIONS

OTHER AUTHORITIES

INTEREST OF AMICI CURIAE[1]

Amici are technology companies that provide products and services related to the Internet, including products and services that customers use to store and process data in the "cloud." Cloud computing enables customers—from individual people to large enterprises—to communicate and collaborate in real-time; to work seamlessly from multiple devices; and to store and share emails, photographs, documents, and other data.

Amazon.com, Inc. seeks to be Earth's most customer-centric company and is guided by four principles: customer obsession rather than competitor focus, passion for invention, commitment to operational excellence, and long-term thinking. Amazon's cloud computing business, Amazon Web Services ("AWS"), offers over 175 fully featured services from data centers globally. Millions of customers—including the fastest-growing startups, largest enterprises, and leading government agencies—are using AWS to lower costs, become more agile, and innovate faster.

Apple Inc. offers secure hardware, software, and servers to customers worldwide. Apple's business strategy leverages its unique ability to design and develop its own operating systems, hardware, application software, and services to

[1] This brief was neither authored nor funded by any party or person other than amici and their counsel. *See* Fed. R. App. P. 29(a)(4)(E); 2d Cir. R. 29.1. All parties to this appeal have consented to the filing of this brief.

provide customers products and solutions with security, ease of use, seamless integration, and innovative design. In addition to the iPhone, iPad, Mac computer, and iPod, Apple offers its users iCloud—a cloud service for storing photos, contacts, calendars, documents, device backups, and more, keeping everything up to date and available to customers on whatever device they are using. Apple is committed to its users' privacy and to helping users understand how it handles their personal information. Apple strives to provide straightforward disclosures when it is compelled to comply with requests for user data from law enforcement.

Google LLC is a diversified technology company whose mission is to organize the world's information and make it universally accessible and useful. Google offers a variety of web-based products and services, including Search, Gmail, Maps, and YouTube, that are used by people throughout the United States and around the world. Google also offers enterprise cloud services like Google Cloud Platform and Workspace (formerly known as G Suite), which includes email, word processing, and applications for storage, spreadsheets, presentations, and calendars, all hosted on Google's servers.

Amici often compete vigorously for customers with Microsoft and with each other. But amici here speak with one voice because of the importance of this case to them and to their customers. Amici have been champions of cloud computing and believe deeply in its potential. That makes amici uniquely well positioned to

understand the threats to cloud computing that are posed by secret government searches of cloud accounts. Amici therefore submit this brief in support of Microsoft's challenge to a nondisclosure order issued under 18 U.S.C. § 2705(b) to explain how the government's overreach in the use of such orders can impose unjustified and unconstitutional burdens on free speech while undermining the trust and security necessary to a successful cloud model.

Amici respect the important work of law enforcement. Technology companies like amici have, or in the future may have, obligations under the Stored Communications Act of 1986, 18 U.S.C. § 2701 *et seq*. ("SCA"), and other laws to deliver customer data to law enforcement in response to valid legal process. Amici take these obligations seriously, while objecting where appropriate to legal requests that appear to exceed the government's authority. Amici have full-time teams of employees dedicated to responding to law-enforcement requests. In just the last six months of 2019, amici collectively responded to tens of thousands of U.S. government data requests in criminal investigations.[2] Amici also publish guidelines for law enforcement that explain their products, describe what customer data can be requested through legal process, and set out how best to serve process

[2] *See* Amazon.com, *Amazon Information Request Report*, https://bit.ly/34xR9xw (all cited websites visited December 20, 2020); Apple, *Transparency Report: United States of America*, https://apple.co/2JcA0SQ; Google, *Transparency Report*, https://bit.ly/3ataT9r.

on the company.[3] Amici, in short, have no desire to stymie legally valid governmental efforts to investigate crime and apprehend those who have committed it.

But amici also believe that their customers have a right to be informed of government searches of their private data and that amici have a right to inform them—and to inform the public about law-enforcement practices in regard to private data. While those rights may be limited as necessary to protect compelling government interests, too often the government has resorted to gag orders by default—based on generalized preferences for secrecy or boilerplate considerations that fail to meet the rigorous scrutiny the First Amendment requires. Particularly because such orders are issued ex parte, the government and the court together bear a responsibility to ensure that the government's burden under the strict scrutiny standard is met. Here, the district court applied that standard in a manner that weakens First Amendment protections.

[3] *See* Amazon.com, *Amazon Law Enforcement Guidelines*, https://bit.ly/38hEsIm; Apple, *Legal Process Guidelines*, https://apple.co/3auMa4M; Google, *How Google Handles Government Requests for User Information*, https://bit.ly/38lxuCe.

ARGUMENT

I. STRICT SCRUTINY SHOULD BE APPLIED TO ENSURE THAT SUPPRESSION OF SPEECH UNDER § 2705(b) IS THE EXCEPTION, NOT THE RULE

As Microsoft explains (at 19-21), a court considering an application for a gag order under 18 U.S.C. § 2705(b) must apply strict scrutiny to ensure the order satisfies the First Amendment. That rigorous review is necessary to protect the important interests that are compromised when the government seeks to restrict providers' speech to their customers. Those interests concern both the success and security of cloud-based services and the core speech rights of cloud providers.

A. First, rigorous scrutiny of gag orders is necessary to ensure the privacy and security of data in the cloud computing age. Transparency is a critical element of any secure and successful cloud computing model. Before the widespread adoption of cloud services, enterprises stored their own data on their own servers. Law enforcement had to approach an enterprise directly to obtain enterprise data, which gave the enterprise control over its data and visibility when third parties sought to access that data. 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) ("2017 DOJ White Paper").[4] That control and transparency allowed enterprises to protect their own interests when

[4] https://bit.ly/38f3N5y.

law enforcement sought their data—for example, by asserting privileges or constitutional objections.

People and organizations—and even governmental agencies, including law-enforcement agencies—have increasingly turned to cloud-based models hosted by service providers like amici to store and process their most sensitive emails, documents, and other records. *See supra* pp. 1-4. Doing so brings many advantages. Cloud customers need not incur the expense or difficulties of maintaining their own systems, but can instead harness the applications, processing power, and storage capacity of cloud services. Cloud-based computing also brings increased speed and connectivity—not only to computers and smartphones, but also thermostats, smart-home tools, and other "Internet of Things" devices. These advantages have been especially important during the coronavirus pandemic. Businesses, people, and even courts have had to rely more than ever on email and digital messaging to collaborate, relay sensitive information, and keep the economy moving.[5]

The success of that cloud model depends crucially on customers' ability to trust that they will retain a similar degree of control and transparency as they

[5] *See* Sayegh, *As COVID-19 Pushes Businesses To Their Limit, The Cloud Rises Above*, Forbes (May 26, 2020), https://bit.ly/2WyQPug ("At no other point in time has there ever been such a need for the instant availability of IT resources enabled by the cloud than during this coronavirus pandemic. The cloud continues to transform connectivity between people and businesses on a global scale.").

would have had if they stored their own data. Recognizing that need for security and the sensitivity of the data that customers entrust to them, amici prioritize the security of their customers' data in a wide range of ways. Amici do not disclose customer data unless compelled to do so by valid and binding legal process.[6] If they are nonetheless compelled to disclose customer content, amici will give their customers reasonable notice of the demand (unless they are legally prohibited or prevented by emergency from doing so) to allow the customer to seek a protective order or other appropriate remedy.[7]

A commitment to transparency helps cloud customers make informed decisions about whether and how to use the cloud; it allows customers to trust amici with their proprietary and sensitive data; and it maintains to the greatest extent possible the visibility that customers had before the cloud when law enforcement had to seek records from customers directly. Indeed, businesses that do not perceive that the law provides adequate protection for their data against

---

[6] Amici may also provide customer information to law enforcement in the case of serious emergencies, for example, if amici reasonably believe that doing so would prevent someone from dying or from suffering serious physical harm. Even in emergencies, amici consider these requests in light of their policies and applicable law.

[7] *See generally* Amazon.com, *AWS Cloud Security*, https://amzn.to/2Knm7ld; Amazon.com, *Law Enforcement Information Requests*, https://amzn.to/3atnnOd; Apple, *Apple Transparency Report: Government and Private Party Requests*, https://apple.co/3pdnJwu; Google, *How Google Handles Government Requests for User Information*, https://bit.ly/2WuXYf5.

secret government access will remain hesitant to leverage the cloud, and overseas enterprises that do choose cloud-based services will hesitate to engage U.S.-based providers—hesitation that undermines U.S. economic growth and productivity.

Recognizing the important values at stake when the government uses the SCA to obtain records from a provider of cloud services, even the Justice Department has taken the position in regard to enterprise data that "prosecutors should seek data directly from the enterprise" if possible, rather than seeking legal process against the service provider under the SCA. 2017 DOJ White Paper at 2. Such an approach—the traditional, transparent 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 customer to "interpose privilege and other objections to disclosure" on its own behalf. *Id.*

For similar reasons, when law enforcement nonetheless chooses to obtain data from the cloud service provider, secrecy should be the exception, not the rule. As the Supreme Court has held, the burden must rest with the government—not the service provider—to demonstrate, based on the specific facts of the particular case, a substantial link between disclosure and a risk of harm to a compelling governmental interest and that no less restrictive alternative would effectively protect the government's interests. *See, e.g.*, *Reed v. Town of Gilbert*, 576 U.S. 155, 162 (2015); *Thomas v. Chicago Park Dist.*, 534 U.S. 316, 321 (2002); *Reno v.*

ACLU, 521 U.S. 844, 874 (1997); *John Doe, Inc. v. Mukasey*, 549 F.3d 861, 881 (2d Cir. 2008). Watering down or departing from that standard in a manner that facilitates secret law-enforcement access to sensitive enterprise data risks eroding users' confidence in U.S.-based cloud services—to the detriment of users, providers, and the economy as a whole.

B. Rigorous scrutiny of gag orders is likewise necessary to protect robust debate about a matter of public concern. Gag orders under § 2705(b) directly restrict providers' speech about an important issue. As Microsoft has explained (at 19-22), the restriction that a gag order imposes is both content-based and 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).

The suppressed speech at issue here is a core element of service providers' relationships with their customers, but it also goes to an issue of public concern—namely, governmental surveillance of private materials stored in the cloud. Members of the public have the right to know when the government searches their private accounts and—absent exceptional and compelling circumstances—amici should have the right to tell them. Visibility into governmental access to data in the cloud enables cloud customers to engage in a fully informed public debate

about the extent to which the government should be able to exploit the shift to cloud computing to circumvent the control and transparency that customers used to have when the government had to obtain records from the enterprise directly.

The public also has a substantial interest in receiving the information necessary to inform public policymaking regarding the appropriate privacy safeguards for the new and evolving digital technological context. *See Stromberg v. California*, 283 U.S. 359, 369 (1931) ("The maintenance of the opportunity for free political discussion to the end that government may be responsive to the will of the people and that changes may be obtained by lawful means, an opportunity essential to the security of the Republic, is a fundamental principle of our constitutional system."). The procedures and standards governing access to electronic communications are the subject of vigorous public debate, particularly as the digital environment continues to evolve further away from the now-unrecognizable social and technological landscape that prevailed when the SCA was enacted in 1986. *See, e.g.*, Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 390 (2014); Schwartz, *Legal Access to the Global Cloud*, 118 Colum. L. Rev. 1681, 1682-1683 (2018). Amici already provide aggregate statistics in their transparency reports. *See supra* p. 3 & n.2. But when § 2705(b) orders are issued indiscriminately and without a meaningful check, cloud users and the public are prevented from learning more concrete facts

that would enable them to evaluate whether the government is overreaching in a manner that requires a democratic response.

"The First Amendment reflects 'a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open.'" *Snyder v. Phelps*, 562 U.S. 443, 452 (2011) (quoting *N.Y. Times Co. v. Sullivan*, 376 U.S. 254, 270 (1964)). Gag orders impede that robust discussion by precluding service providers from disclosing to their customers key facts about law-enforcement access to data. Faithful adherence to the highest level of First Amendment scrutiny is necessary to protect basic principles of free speech.

II. THE GOVERNMENT'S USE OF § 2705(B) IS OFTEN INSUFFICIENTLY PROTECTIVE OF FIRST AMENDMENT RIGHTS

The First Amendment places a heavy burden on the government to justify the intrusion into protected speech that a gag order under § 2705(b) entails. Especially because those orders are obtained ex parte, the government shares a special responsibility with the reviewing court to ensure that gag orders are sought only where the specific facts of a particular case make secrecy necessary and that any such order is appropriately tailored in scope and duration to the specific exigencies of that case. In amici's experience, however, law enforcement often defaults to the assumption—contrary to the Justice Department's own policy statements, *supra* p. 8—that data should be obtained from the service provider

rather than the customer and that gag orders should be imposed as a matter of routine.

As noted, before the advent of the cloud, the government had to go directly to enterprises when it wanted to obtain enterprise records for use in an ongoing criminal investigation. *Supra* pp. 5-6. But today, in the experience of amici, the government increasingly seeks those records from the enterprise's cloud-service provider. In some cases, law enforcement takes this approach because it is concerned about the consequences of approaching the enterprise directly. 2017 DOJ White Paper at 2-3. But, as the Justice Department has acknowledged, 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.

Moreover, when amici are compelled to produce customer data to law enforcement, they are often prevented from telling the customer or any other person because such legal requests are commonly accompanied by gag orders. Indeed, in amici's experience, the government obtains gag orders under § 2705(b) not with the rarity that one would expect given the stringency of the strict-scrutiny standard, but routinely—in connection with a substantial proportion if not a majority of legal requests.

Exacerbating the problem, the government often obtains gag orders that reflect boilerplate, default practices, suggesting little individualized consideration of the need for secrecy and the scope of the order in light of the specific facts of the particular case. For example, in one district in this Circuit, it is the "regular practice" of prosecutors to seek gag orders of one full year's duration, *In re Grand Jury Subpoena to Google, LLC*, No. 1:20-mc-00035-LAP, slip op. at 22, (S.D.N.Y. Jun. 3, 2019), *appeal docketed sub nom. United States v. Google*, No. 19-1891 (2d Cir.), notwithstanding that one year is the maximum duration permissible under Department of Justice policy absent "exceptional circumstances" and supervisor approval. *See* Memorandum from Deputy Attorney General Rod J. Rosenstein to Heads of Department Law Enforcement Components et al. at 2 (Oct. 19, 2017).[8]

Seeking a year-long restraint on speech as a matter of course is not narrow tailoring. Instead, the First Amendment—and Department of Justice policy—require the government to make a particularized showing, based on evidence, why the restraint on speech is warranted for the duration requested, and why a shorter duration will not suffice. *See id*. at 2 ("In applying for a § 2705(b) order, prosecutors should tailor the application to include the available facts of the specific case and/or concerns attendant to the particular type of investigation."); *see also Thomas*, 534 U.S. at 321 ("[T]he censor must bear the burden of going to

[8] https://bit.ly/3nGCZBS.

court to suppress the speech and must bear the burden of proof once in court."); *In re Grand Jury Subpoena to [Redacted,] Inc.*, No. 18-mc-0334, 2018 WL 718383, at *4 n.4 (E.D.N.Y. Feb. 5, 2018) (government requests for § 2705(b) gag orders must be supported by an explanation of why the requested duration is necessary).

Some magistrate judges have rightly rejected applications for gag orders justified only by "boilerplate assertions." *See, e.g.*, *In re Grand Jury Subpoena to Facebook*, No. 16-mc-1300, 2016 WL 9274455, at *4 (E.D.N.Y. May 12, 2016); *In re Grand Jury Subpoena to [Redacted,] Inc.*, 2018 WL 718383, at *1. But in amici's experience, they remain common. As this court has explained in a similar context—the closure of a courtroom—the First Amendment generally requires a trial judge to "articulate on the public or sealed record a sufficiently detailed basis for his serious concern about public dissemination risks and for his marked preference for closure over alternative remedies to permit an appellate court to judge." *In re Application of The Herald Co.*, 734 F.2d 93, 103 (2d Cir. 1984). Such a rule makes good sense, and should govern here, too: A court considering issuing a § 2705(b) order should be required to identify case-specific facts that justify a gag order in order to both facilitate judicial review and guard against the prospect that gag orders become a matter of routine, without regard to the First Amendment, whenever the government would prefer to investigate in secret.

In amici's experience, however, gag orders regularly include little or no information that would reflect any efforts at balancing—by the government or the court—the government's asserted interest in secrecy with the important free speech values at stake. That is true even in cases where the government's investigation has already been widely publicized in major news outlets, in which any compelling government interest the government may have in secrecy is substantially diminished. *Cf. In re Grand Jury Subpoena, Judith Miller*, 493 F.3d 152, 154 (D.C. Cir. 2007) ("Grand jury secrecy is not unyielding when there is no secrecy left to protect.").

By making increased use of § 2705(b) and seeking to justify it based on a generalized premise that transparency always risks compromising an investigation, the government has aimed to carve for itself a realm of secrecy for obtaining records from cloud service providers that it never would have enjoyed outside of the cloud environment. In other contexts, the government has never been generally entitled to conduct all investigative activities in secret. At common law, police officers were generally required to knock and announce their presence before entering a suspect's home to execute a warrant. *See Wilson v. Arkansas*, 514 U.S. 927, 931-933 (1995). The common law likewise required officers to provide written notice, in the form of an "inventory," to anyone whose property was searched or seized. *See Wilkes v. Wood*, 98 Eng. Rep. 489, 498 (C.P. 1763). This

rule formed the basis of *Berger v. New York*, 388 U.S. 41 (1967), which struck down as unconstitutional a state statute permitting wiretapping without notice, *see id.* at 60 (condemning statute in part because it "has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts"). And it is implemented today by Federal Rule of Criminal Procedure 41, which requires an officer executing a search warrant to provide notice to the person whose property was searched or seized. *See* Fed. R. Crim. P. 41(f)(1)(C); *see also United States v. Pangburn*, 983 F.2d 449, 452 (2d Cir. 1993).

Importantly, courts and the federal rules disfavor restricting witnesses from disclosing their involvement in criminal matters absent due consideration for their First Amendment interests. The rules governing federal grand jury proceedings state a presumption against secrecy, expressly prohibiting imposing an "obligation of secrecy" on anyone save certain listed individuals; witnesses are not on the list. Fed. R. Crim. P. 6(e)(2). The Rules Committee's notes explain that the Committee considered and rejected imposing "an[] obligation of secrecy on witnesses"—a practice it viewed as "an unnecessary hardship" that "may lead to injustice." Fed. R. Crim. P. 6(e) n.2. And courts have divided on whether orders gagging grand jury witnesses may be issued *at all*. *See* 3 LaFave et al., *Criminal Procedure* § 8.5(d) (4th ed.); *In re Grand Jury Proceedings*, 814 F.2d 61, 68-70 (1st Cir.

1987) (citing cases). Even those courts that have upheld gag orders in the grand jury context have limited them to "exceptional cases." *Id*. These courts have emphasized that "the policy of non-secrecy as to grand jury witnesses … should not be set aside except in situations where the need for secrecy outweighs the countervailing policy," and explained that "this need must be shown with particularity." *In re Grand Jury Subpoena Duces Tecum*, 797 F.2d 676, 680 (8th Cir. 1986). As one judge of this Court put it, a gag order is not warranted where the government's case rests only on "the prosecutor's formulaic conclusion that the 'investigation would be frustrated.'" *In re Grand Jury Subpoena Duces Tecum*, 575 F. Supp. 93, 94 (S.D.N.Y. 1983) (Leval, J.). Such an order "interferes with a variety of important freedoms, including speech and association," and so should not "be issued on so meager a basis." *Id.*

In short, while the government may conduct investigations in secrecy up to a point, there is no presumption that an investigation must remain secret for its entire duration, even after the government has invaded a person's privacy by conducting a search or seizing records. And it is only in exceptional cases that the government may compel witnesses to maintain secrecy by means of a gag order. The government should not be permitted to treat § 2705(b) as an outlier under which secrecy is not the exception but the rule.

III. THE DISTRICT COURT FAILED TO APPLY STRICT SCRUTINY IN THE MANNER NECESSARY TO GUARD AGAINST GOVERNMENT OVERREACH

Given the importance of the First Amendment interests at stake, it is incumbent upon courts to apply the strict scrutiny standard rigorously to hold the government to its burden and guard against government overreach. Here, however, although the district court at times recited the appropriate strict scrutiny standard, it failed to adhere to that standard in substance. *See* JA-90 to JA-95. The district court's approach would broadly permit gag orders as a default matter while improperly shifting the burden to service providers to establish that complete secrecy is unnecessary. *Cf. Thomas*, 534 U.S. at 321 (First Amendment requires the government to "go[] to court to suppress … speech and [to] bear the burden of proof" once there).

For example, the district court here concluded that the gag order was narrowly tailored—and that no limited disclosure to anyone at the enterprise would be practical—based on speculation about a "risk" that "higher-ups" in the company were involved in the alleged conspiracy. JA-93. Under this reasoning, however, strict scrutiny in effect will *always* be satisfied when the government has not yet ruled out the possibility that executives are implicated in the criminal behavior—even when there is no specific reason to think that the enterprise as a whole is devoted to criminal conduct and no reason to doubt the efficacy of the enterprise's compliance structures for handling legal process appropriately. The government is

obligated to prove—with "specific evidence," *United States v. Playboy Entm't Grp., Inc.*, 529 U.S. 803, 820 (2000)—that there are no "less restrictive alternatives," *Reno*, 521 U.S. at 874, to a wholesale gag. Mere "anecdote and supposition," *Playboy Entm't*, 529 U.S. at 822, that a senior executive *might* be involved in the conspiracy is insufficient to justify the most extreme possible restriction on speech.

The court also rejected Microsoft's proposal to make a limited disclosure to a select individual at the enterprise. In amici's experience, such disclosures are frequently possible without unduly undermining a government investigation. As explained, 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. *Supra* pp. 5-6. The government could and did manage that risk by approaching "an individual within the enterprise who is an appropriate contact for securing the data," such as "the general counsel or legal representative." 2017 DOJ White Paper at 2. Consider, for instance, an investigation into a small number of employees of a large corporation. In such a case, disclosing to the corporation's general counsel the existence of a subpoena for the employees' emails (or simply seeking those emails directly from the corporation) would be exceedingly unlikely to prejudice the investigation, as the Justice Department itself recognizes. *See id.*

The expansion of cloud computing does not obviate that alternative course of action; indeed, the Justice Department's own guidance suggests that prosecutors should follow it where practical. 2017 DOJ White Paper at 2. As one court in this circuit has explained, "there is no reason to assume that tipping off an investigative target to the investigation's existence necessarily 'will' result in one of the harms contemplated by the SCA," *In re Grand Jury Subpoena to Facebook*, 2016 WL 9274455, at *4, especially where the disclosure would be to an attorney governed by professional and ethical obligations.

The district court nevertheless concluded that "vet[ting]" select individuals would be "unduly burdensome" for the government. JA-94 (quotation marks omitted). But Supreme Court precedent intentionally places that burden on the government, not on the speaker, to avoid unduly infringing on or chilling protected speech. *See Reno*, 521 U.S. at 874; *Thomas*, 534 U.S. at 321 ("[T]he censor … must bear the burden of proof…."). The government is not required to "vet" every employee in the company to do so. Rather, the government must explain why, in its view, no one in or associated with the enterprise in that particular case—including in-house or outside counsel—could receive a limited disclosure from a service provider without compromising the integrity of the investigation.

The district court should have required the government to meet that burden. Instead, the court relied on speculation and shifted that burden to the provider,

making secrecy the default except in cases where the service provider can persuade the government that some limited disclosure can be made. Moreover, the court erred in rejecting Microsoft's proposed alternative on the ground that a carefully limited disclosure would not be "as effective" as a complete ban on Microsoft's speech. JA-93; *see also* JA-109. As Microsoft has explained (at 26-29), no alternative could ever be "as effective" as a complete ban, but the First Amendment nonetheless requires the government to adopt a less-restrictive alternative that protects the government's interests even if it is not a "perfect solution." *Ashcroft v. ACLU*, 542 U.S. 656, 668 (2004); *see also Playboy Entm't*, 529 U.S. at 815, 822-824.

Given these infirmities in the district court's application of strict scrutiny, the Court should reverse and hold the government to its burden of demonstrating—based on particularized, case-specific facts and evidence, *see Playboy Entm't*, 529 U.S. at 820—that the gag order issued in this case was narrowly tailored.

CONCLUSION

For the foregoing reasons, the decision below should be reversed.

Respectfully submitted,

/s/ Catherine M.A. Carroll

DANIEL S. SILVER
CHRISTOPHER J. MORVILLO
CLIFFORD CHANCE US LLP
31 West 52nd Street
New York, NY 10019
(212) 878-8000

Counsel for Amazon.com, Inc.

CATHERINE M.A. CARROLL
ARI HOLTZBLATT
ALEX HEMMER
JORDAN E. OROSZ
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 663-6000

Counsel for Apple Inc. and Google LLC

December 21, 2020

CERTIFICATE OF COMPLIANCE

The foregoing brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 29(a)(5), as modified by Local Rule 29.1(c), in that the brief, according to the word-count feature of the word-processing system with which it was prepared (Microsoft Word), contains 4,835 words.

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