Clerk of the Court
Received 10/04/2022 05:00 PM

No. 22-CV-0239

IN THE DISTRICT OF COLUMBIA COURT OF APPEALS

META PLATFORMS, INC.,

Appellant,

v.

DISTRICT OF COLUMBIA,

Appellee.

On Appeal From The District of Columbia Superior Court
Before The Honorable Anthony C. Epstein
Case No. CA2-4450-21

BRIEF FOR APPELLANT

JOSHUA S. LIPSHUTZ
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, NW
Washington, DC 20036-5306
(202) 955-8500

CATHERINE M.A. CARROLL*
**Counsel for Oral Argument*
RONALD C. MACHEN
GEORGE P. VARGHESE
ARI HOLTZBLATT
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 663-6000

October 4, 2022

RULE 28(A)(2)(A) STATEMENT

The parties to this case are appellant Meta Platforms, Inc. ("Meta") and appellee District of Columbia.

Before the Superior Court, Meta was represented by Joshua S. Lipshutz of Gibson, Dunn & Crutcher LLP. The District of Columbia was represented by Benjamin Wiseman, Adam Teitelbaum, and Elizabeth Feldstein.

Meta is represented in this Court by Catherine M.A. Carroll, Ronald C. Machen, George P. Varghese, and Ari Holtzblatt of Wilmer Cutler Pickering Hale and Dorr LLP and by Joshua S. Lipshutz of Gibson, Dunn & Crutcher LLP. The District of Columbia is represented by Benjamin Wiseman, Adam Teitelbaum, and Elizabeth Feldstein.

RULE 26.1 DISCLOSURE STATEMENT

Appellant Meta has no parent corporation and no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

INTRODUCTION

This appeal presents the important question whether the government can, consistent with the Stored Communications Act and the First Amendment, compel a provider of electronic communication services to disclose to the government the contents of users' online communications–unmasking anonymous users' identities in the process—using only an administrative subpoena. The case arises out of an investigation by the D.C. Office of the Attorney General ("OAG") into the adequacy of efforts by Meta Platforms, Inc. ("Meta") to fight misinformation posted on Facebook about the safety and efficacy of COVID-19 vaccines. The First Amendment precludes OAG from regulating Meta's efforts directly, because doing so would interfere with Meta's right to exercise editorial control and judgment over what content is published on the Facebook platform. *E.g.*, *Miami Herald Publ'g Co. v. Tornillo*, 418 U.S. 241, 257-258 (1974). OAG accordingly couched its investigation as an inquiry into the truthfulness of Meta's public statements about the steps it has taken to combat COVID-19 vaccine misinformation. Invoking its authority under the D.C. Consumer Protection Procedures Act ("CPPA"), OAG issued an administrative subpoena demanding that Meta produce several categories of documents and information relating to its enforcement of its COVID-19 misinformation policies.

In response, Meta provided substantial information to enable OAG to evaluate the consistency of Meta's actions with its public statements—including information about the total volume of content that Meta has removed from or demoted on Facebook for violating its COVID-19 misinformation policies and the volume of such content reviewed or flagged for fact-checking review. But Meta concluded it could not comply with one request in the administrative subpoena. That request, referred to as Request #2, demands information revealing the identities of individuals or entities based on the content of their speech, specifically those who posted content concerning vaccines in violation of Meta's COVID-19 misinformation policies. It also seeks information on the nature of each violation and steps Meta took in response in each case. App. 4-5 ("Request #2"). That request violates the federal Stored Communications Act ("SCA"), 18 U.S.C. § 2703, which provides that OAG cannot rely on an administrative subpoena but instead must obtain a warrant to compel Meta to disclose the contents of user communications. Request #2 also violates the First Amendment—by interfering with Meta's exercise of protected editorial judgment and intruding into the rights of speech and association of Meta's users without satisfying exacting scrutiny.

The Superior Court nonetheless granted OAG's petition for enforcement of Request #2. In doing so, the court committed two significant legal errors, each of which independently requires reversal.

First, the Superior Court erred in holding that the SCA permits OAG to compel the information sought by Request #2 using only an administrative subpoena. The text, structure, and legislative history of the SCA all make clear that a governmental entity seeking to compel a provider of electronic communication services ("ECS") to disclose user communications must comply with Section 2703 of the SCA, which establishes the requirements for "[g]overnmental access to customer communications." *Facebook, Inc. v. Pepe*, 241 A.3d 248, 254 n.12 (D.C. 2020). And Section 2703 provides that a governmental entity "may require" disclosure of contents of communications "only pursuant to a warrant." 18 U.S.C. § 2703(a)(1). In holding otherwise, the Superior Court correctly recognized that Request #2 seeks contents of communications, but it concluded that the government may disregard the requirements of Section 2703 whenever a different section of the SCA, Section 2702, would permit the ECS provider to voluntarily disclose the communications based on the user's implicit consent. That reasoning would dramatically expand the government's power to unilaterally demand access to online communications, with far-reaching implications for millions of internet users. The Superior Court's holding finds no support in the SCA. It ignores Congress's intent to impose stringent standards to protect online communications against government intrusion. And it stands alone

among judicial decisions applying the SCA. This Court should reverse that erroneous and unprecedented holding.

Second, the Superior Court independently erred in holding that Request #2 satisfies the exacting scrutiny demanded by the First Amendment. Request #2 intrudes on protected First Amendment interests in two ways. It seeks to probe Meta's protected exercise of editorial control over user-submitted content it published on its privately owned website in violation of Meta's own First Amendment rights; and it threatens to chill the protected expression of Meta's users by compelling disclosure of the identities of people whose speech and associations OAG disfavors. Given these First Amendment implications, Request #2 must satisfy (at a minimum) exacting scrutiny. Contrary to the Superior Court's conclusion, however, Request #2 is in no way adequately tailored to any substantial governmental interest. OAG can readily achieve the purposes it claims to be pursuing in its investigation through alternative avenues without forcing disclosure of the identities of every user who posted vaccine-related content that violated a COVID-19 misinformation policy—disclosure that courts have long recognized to pose a harmful threat to protected expression. The implications of the Superior Court's ruling are not limited to COVID-19-related content. Under the reasoning adopted here, government officials who are hostile to speech about any topic—from immigration to climate change—could use a subpoena to demand

the identities of every Facebook user who posted on any of those topics, simply by purporting to conduct a consumer-protection investigation. The Court should reverse.

JURISDICTIONAL STATEMENT

The Superior Court had jurisdiction over OAG's motion to enforce the administrative subpoena under D.C. Code §§ 1-301.88d(d) and 28-3909(a). This Court has jurisdiction under D.C. Code. § 11-721(a)(1), which confers jurisdiction on this Court over "all final orders and judgments of the Superior Court of the District Columbia." Under *Kemp v. Gay*, 947 F.2d 1493 (D.C. Cir. 1991), an order enforcing an administrative subpoena concludes the only judicial proceeding before the court and is therefore "a final order ripe for review" on immediate appeal, with no order of contempt required. *See id.* at 1495-1497 (allowing immediate appeal of order enforcing administrative subpoena); *see also Crane v. Crane*, 657 A.2d 312, 315-316 (D.C. 1995) (recognizing that "discovery orders may be considered final and appealable where the discovery request is the only proceeding pending before the court").

STATEMENT OF ISSUES

1. Whether the Superior Court erred in holding that OAG, a governmental entity, can compel a service provider such as Meta to disclose the

contents of a user's communications without complying with the requirements set forth in 18 U.S.C. § 2703, including the warrant requirement.

2. Whether the Superior Court erred in holding that Request #2 satisfies the exacting scrutiny demanded by the First Amendment for compulsory disclosure.

STATEMENT OF THE CASE

A. Statutory Framework

Enacted as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860, the Stored Communications Act ("SCA") extends "'Fourth Amendment-like privacy protections'" to stored electronic communications by "'regulating the relationship between government investigators and service providers in possession of users' private information.'" *Walker v. Coffey*, 956 F.3d 163, 167 (3d Cir. 2020) (quoting Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1212 (2004)). The SCA "provides this enhanced privacy protection" by limiting both "the government's ability to compel providers to disclose their users' information" and "the providers' ability to disclose such information to the government." *Id.* (citing 18 U.S.C. §§ 2702, 2703).

The SCA "broadly prohibits providers from disclosing the contents of covered communications" to anyone, "stating that providers 'shall not knowingly

divulge to any person or entity the contents' of covered communications, except as provided." *Facebook v. Wint*, 199 A.3d 625, 628 (D.C. 2019) (quoting 18 U.S.C. § 2702(a)(1)). Under Section 2702, entitled "[v]oluntary disclosure of customer communications or records," that prohibition is subject to nine enumerated exceptions in which a service provider "may" voluntarily disclose contents of communications. *See* 18 U.S.C. § 2702(b). As relevant here, an ECS provider "may divulge the contents of a communication" when the originator or the intended recipient has "lawful[ly] consent[ed]" to disclosure. *Id.* § 2702(b)(3). In addition, the provider "may divulge" contents of communications without violating Section 2702 when disclosure is "otherwise authorized" under other statutory provisions, including Section 2703.

Section 2703, entitled "[r]equired disclosure of customer communications or records," delineates when and how a "governmental entity" "may require" a service provider to disclose contents or records of an electronic communication, 18 U.S.C. § 2703(a). The procedures and standards a governmental entity must follow to compel disclosure depend on the nature of the information the government seeks to obtain. With respect to the "contents" of communications that have been in electronic storage for 180 days or less, the government "may require disclosure" by the service provider "only pursuant to a warrant." *Id.* As to contents of communications in storage for more than 180 days, Section 2703

likewise requires the government to obtain a "warrant" unless—in a statutory alternative that has been largely abrogated by Fourth Amendment case law—the government gives "prior notice" to the subscriber or customer. *Id.* § 2703(b).[1]

In contrast, for non-content records, a governmental entity generally "may require" disclosure using either a warrant or a court order issued upon a lesser showing than probable cause. 18 U.S.C. § 2703(c)(1), (d). Alternatively, the government "may require" disclosure of such non-content records with the "consent of the subscriber or customer." *Id.* § 2703(c)(1)(C). If the government uses only an administrative subpoena or a trial or grand jury subpoena, without providing notice to the subscriber or customer, it can compel disclosure of only a limited category of basic subscriber information. *Id.* § 2703(c)(2).

---

[1] The SCA's original distinction between communications in storage for more or less than 180 days has largely been abandoned, as courts and the U.S. Department of Justice now uniformly agree that people can have a reasonable expectation of privacy in their content regardless of how long the communication has been in storage. *See United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010); DOJ, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 122-123 (2009) (noting that stored emails are "contents" under the SCA), https://www.justice.gov/file/442111/download; H.R. Rep. No. 114-528, at 9 (2016).

B. Factual Background

Meta offers an array of products and services to more than 2 billion users worldwide.[2] Among these services is Facebook:[3] a website and app where users can maintain accounts,[4] create Pages;[5] gather to share status updates, stories, and other content on those Pages; browse for content through their News Feed;[6] and advocate and fundraise for causes.[7]

To help Facebook remain a safe and useful space, Meta has adopted and enforces a series of policies that govern what content can be posted on the platform. After the COVID-19 pandemic began, Meta adopted policies that aim to "protect people from harmful content and new types of abuse related to COVID-19

---

[2] Clegg, *Combating COVID-19 Misinformation Across Our Apps*, META (Mar. 25, 2020) (describing Meta's work to provide 2 billion Facebook and Instagram users with resources from public-health authorities), https://about.fb.com/news/2020/03/combating-covid-19-misinformation/.

[3] *What are the Meta Products?*, META, https://www.facebook.com/help/1561485474074139/.

[4] *Creating an Account*, META, https://www.facebook.com/help/570785306433644/.

[5] *Create and Manage a Page*, META, https://www.facebook.com/help/135275340210354/.

[6] *Your Home Page*, META, https://www.facebook.com/help/753701661398957/.

[7] *See People Raise Over $2 Billion for Causes on Facebook*, META (Feb. 6, 2020), https://about.fb.com/news/2019/09/2-billion-for-causes/.

and vaccines."[8] One such policy states that Meta removes content that repeats other false health information "that [has been] widely debunked by leading health organizations such as the World Health Organization (WHO) and the Centers for Disease Control and Prevention (CDC)."[9] The policy also states that Meta will "remove content containing links to off-platform content" that it identifies as violating its COVID-19 and vaccine misinformation rules, and "remove any Pages, Groups, Events, Or Instagram Accounts" that "instruct or encourage users to employ code words when discussing vaccines or COVID-19 to evade [Meta's] detection."[10] Meta uses artificial intelligence ("AI") systems to detect when someone tries to share content flagged as COVID-19 misinformation.[11] Meta also shows "strong warning labels and notifications" to people who come across the false information Meta has identified or try to share it.[12] By adopting these policies, Meta aims to "combat misinformation about vaccines and diseases,"

---

8 *See, e.g.*, *COVID-19 and Vaccine Policy Updates & Protections*, META, https://www.facebook.com/help/230764881494641/.

9 *Id*.

10 *Id*.

11 *Using AI to Detect COVID-19 Misinformation and Exploitative Content,* META AI, (May 12, 2020), https://ai.facebook.com/blog/using-ai-to-detect-covid-19-misinformation-and-exploitative-content/.

12 Clegg, *Combatting COVID-19 Misinformation Across Our Apps*, *supra* note 2.

which it believes could result in reduced vaccinations and harm public health and safety.[13]

Dissatisfied with the "extent of Facebook's efforts to combat vaccine misinformation" and Meta's "public statements" regarding those efforts, Super. Ct. - Mem. in Support of Pet. ("Pet. Mem.") 2 (Nov. 30, 2021) , OAG launched an investigation into whether Meta's "handling of COVID-19 vaccine information posted on its social media platform" violates the CPPA. App. 7. As the predicate for this investigation, OAG cited several statements in which Meta offered qualitative descriptions of general steps it intended to take to restrict vaccine-related misinformation, such as describing its decision to demote, rather than remove, certain vaccine-related misinformation as a "break the glass" measure, and pledging to "immediately" enforce a new and broader definition of vaccine misinformation "with a particular focus on Pages, groups, and accounts that violate these rules." Pet. Mem. 4. OAG also cited the following statement concerning Meta's efforts to combat COVID-19 misinformation—not just vaccine-related information—as a whole: "Since the beginning of the pandemic, across our entire platform, we have removed over 3,000 accounts, Pages, and groups for repeatedly

---

[13] *COVID-19 and Vaccine Policy Updates & Protections*, META, *supra* note 8.

violating our rules against spreading COVID-19 and vaccine misinformation and removed more than 20 million pieces of content for breaking these rules."[14]

OAG identified no quantitative statements concerning Meta's enforcement of its misinformation policies specific to COVID-19 *vaccines*, such as statements about the number of vaccine-related violations or statements about Meta's enforcement decisions in particular cases. To the contrary, OAG has admitted that "with respect to COVID-19 *vaccine* misinformation in particular"—the sole subject of the government's investigation—"Facebook has not publicly disclosed the total volume of content reviewed, identified as false, demoted, or removed, or the total number of accounts, pages, and groups suspended or banned." Pet. Mem. 5. According to OAG, Meta's qualitative public statements about its general plans for limiting vaccine-related misinformation entitle OAG to investigate not only the subjects of those statements, but also specific decisions and actions that Meta has taken in tens and potentially hundreds of thousands or millions of particular cases with respect to individual users regarding vaccine-related misinformation.

On June 21, 2021, OAG issued an administrative subpoena ordering Meta to produce various categories of documents. In response, Meta provided information

---

[14] Bickert, *How We're Taking Action Against Vaccine Misinformation Superspreaders*, META, (Aug. 18, 2021), https://about.fb.com/news/2021/08/taking-action-against-vaccinemisinformation-superspreaders/.

to OAG about its continued efforts to enforce terms-of-service violations related to the spread of COVID-19 misinformation on the Facebook platform and produced information and documents in response to several of OAG's requests. For example, Meta provided information in response to OAG's request for "the total volume of content that has been removed or demoted by Facebook for violating Facebook's COVID-19 misinformation policy with respect to content concerning vaccines." App. 5 ("Request #3").[15] And Meta likewise provided information about the "volume of content" related to COVID-19 misinformation that Meta had reviewed and taken action against (or had in queue for review) throughout the first half of 2021. *Id.* ("Request #4").

However, Meta objected to producing documents in response to Request #2, which demanded "documents sufficient to identify all Facebook groups, pages, and accounts that have violated Facebook's COVID-19 misinformation policies with respect to content concerning vaccines," including the identities of individuals or entities associated with those groups, pages, or accounts, the nature of the violation, and Facebook's response. App. 4-5. Meta objected on the ground that the request violates the SCA because identifying users whose posts Meta had determined violated its COVID-19 misinformation policies would disclose the

[15] As Meta has repeatedly informed OAG, Meta does not separately track COVID-19 misinformation specific to vaccines in particular.

contents of the users' communications, and as Meta explained, pursuant to Section 2703 of the SCA, the government may compel disclosure of contents only by using a warrant—not, as here, an administrative subpoena.[16]

C. Procedural History

OAG filed a petition for enforcement of Request #2 of the administrative subpoena. App. 7. In opposition, Meta maintained that Request #2 violates the SCA because OAG did not obtain a warrant, as required by Section 2703. Super. Ct. Opp. - To Pet. for Enforcement 3-15 (Jan. 31, 2022). Meta further maintained that Request #2 violates the First Amendment. With respect to the First Amendment, Meta contended that disclosing the identity of users whose posts had violated Meta's COVID-19 misinformation policies would chill their speech and so would violate the users' First Amendment rights. And furthermore, Meta objected that compelling it to produce granular information about how it exercised editorial control over vaccine misinformation on its platform in potentially millions of specific cases would infringe Meta's own First Amendment rights.

The Superior Court (Epstein, J.) granted the petition in part. The court first agreed with Meta that Request #2 seeks the "contents" of user communications and thus triggers the SCA's robust protections against required disclosure of such material to the government. App. 19. As the court explained, the statutory

---

[16] Meta preserved other objections as well that are not at issue here.

definition of "'contents'" includes "not only the literal text of electronic communications but also identifying information that would have the 'logical effect' of revealing the substance or intended message." *Id.* (quoting *O'Grady v. Superior Court*, 139 Cal. App. 4th 1423, 1448 (2006)); *see also* 18 U.S.C. § 2510(8) (defining "contents" for SCA purposes as "any information concerning the substance, purport, or meaning of [an electronic] communication"). Here, "revealing the identities of users who violated Facebook's policies on vaccine misinformation" would have "the logical and practical effect" of revealing the "contents of their communications" because "identifying them necessarily means disclosing that they communicated information about vaccines." App. 19-20 (quotation marks omitted). The court also rejected OAG's contention that the content Meta removed is not subject to the SCA. App. 21 (citing *Republic of Gambia v. Facebook, Inc.*, 575 F. Supp. 3d 8 (D.D.C. 2021)).

The Superior Court nonetheless held that the SCA permits OAG to compel Meta to produce the contents of user communications using only an administrative subpoena. App. 21-27. The court did not identify any provision in Section 2703 that authorizes a governmental entity to use an administrative subpoena in this context. Instead, the court pointed to Section 2702. As explained above, that section "broadly prohibits" disclosure of contents to any person or entity, except where one of nine enumerated exceptions permits voluntary disclosure. *Wint*, 199

A.3d at 628. The Superior Court relied on the so-called "consent exception" in paragraph 2702(b)(3), which provides that a provider "may divulge the contents of a communication … with the lawful consent" of the user. According to the court, "if disclosure by Facebook is *permitted* under paragraph (c)(3)" because a user has in some sense consented to disclosure, then "the same disclosure can be *compelled* by subpoena." App. 24 (citing *Facebook, Inc. v. Pepe*, 241 A.3d 248 (D.C. 2020)). The court held that the SCA "does not state explicitly that § 2703 provides the *exclusive* method by which government agencies can obtain content" from an ECS provider and that there was no "reason why Congress would have prevented disclosure of content to government agencies with user consent." App. 23.

The Superior Court concluded that the consent necessary to trigger Section 2702(b)(3) exists here, at least insofar as Request #2 seeks only "public posts." App. 25. According to the court, "when a user posts content on Facebook that is generally accessible to the public, the user implicitly consents to disclosure by" the provider, thereby placing all such "public posts" within the scope of the consent exception in Section 2702(c)(3). *Id*. Accordingly, the court concluded that Section 2702(c)(3) permits OAG to compel production of the contents of public posts

using only an administrative subpoena, rather than following the more demanding procedures required by Section 2703.[17]

With respect to Meta's First Amendment arguments, the Superior Court held that enforcing Request #2 would not infringe on Meta's right to moderate content on Facebook because OAG seeks only to investigate Meta's public statements concerning its content-moderation policies, not to dictate whether or how Meta should apply those policies. App. 27. Furthermore, as to the First Amendment rights of Meta's users, the court held that Request #2 could withstand exacting scrutiny. The court agreed that Facebook users' advocacy about COVID-19 vaccines is "unquestionably … protected by the First Amendment," App. 28, and further acknowledged that unmasking the users whose posts were deemed to spread misinformation could subject those users to "greater risk" of "harsh or unfair criticism or even threats by others who disagree with them," App. 29. But the court concluded that OAG has a "compelling interest" in investigating Meta's statements under the CPPA and that Request #2 is "narrowly tailored" to that

[17] In briefing the petition for enforcement, OAG defined "public posts" to mean "posts to pages or public groups that are inherently visible to the public regardless of whether the user has a Facebook account" and "posts to nominally private groups that either have so many members that they are functionally public or otherwise evince an intent to reach the public." App. 26. The Superior Court directed the parties to "try to reach agreement on an approach that identifies public posts in a way that protects non-public posts from disclosure and that does not impose an undue burden on Meta." *Id.*

investigative goal because the information it seeks is "relevant" to the truthfulness of Meta's public statements. App. 29-30. Although, as OAG conceded, Meta has never actually made any public quantitative statements about the total volume of posts related to COVID *vaccine* misinformation it reviewed or took action against—*i.e.*, the information targeted by Request #2—the court thought OAG's interest in that information was sufficiently "reasonable" to satisfy First Amendment scrutiny given the apparent absence of "less intrusive means that the District could employ." App. 30. Finally, the court observed that Request #2 seeks "information that these Facebook users themselves chose to make public" and that "nothing in the record suggests that providing this user-specific information to the District will result in any reprisals against Facebook users." App. 31.

Meta moved for reconsideration. App. 37. Meta argued that the Superior Court erred in concluding that OAG may compel disclosure of content from Meta pursuant to Section 2702 of the SCA because government-compelled disclosures are governed exclusively by Section 2703. The court denied Meta's motion, adhering to the view that a governmental entity need not comply with Section 2703 where the consent exception of Section 2702 applies. App. 41.

STANDARD OF REVIEW

This Court reviews de novo the "legal conclusions" reached by the Superior Court in granting the petition for enforcement. *Solers, Inc. v. Doe*, 977 A.2d 941, 947-948 (D.C. 2009) (quotation marks omitted); *see id.* at 948 (trial court "necessarily abuse[s] its discretion if it based its ruling on an erroneous view of the law" (quotation marks omitted)).

SUMMARY OF ARGUMENT

The Superior Court committed two legal errors in granting OAG's petition to enforce Request #2.

First, the court erred in concluding that OAG can compel an ECS provider to disclose the contents of user communications without complying with Section 2703 of the SCA. The SCA's plain text, structure, and legislative history all confirm that, regardless of whether an exception in Section 2702 would permit voluntary disclosure by the provider, a governmental entity may require disclosure only as provided by Section 2703. Case law, including the reasoning of this Court's decision in *Facebook, Inc. v. Pepe*, 241 A.3d 248 (D.C. 2020), likewise confirms that efforts by the government to compel disclosure are subject to Section 2703. The Superior Court's decision is an outlier among cases interpreting the SCA that threatens to significantly expand the power of governmental entities to

unilaterally force disclosure of user communications, contrary to Congress's intent to protect those communications from government intrusion.

Second, and independently, the Superior Court's order misapplies First Amendment precedent. Request #2 intrudes on both Meta's First Amendment rights to exercise editorial judgment over the content on its platform and Meta's users' First Amendment rights of free speech and association. As a result of these intrusions, Request #2 had to satisfy exacting scrutiny. But OAG has proffered no important governmental interest sufficient to justify the First Amendment intrusion and has failed to demonstrate a substantial relationship between Request #2 and any such interest. Moreover, less restrictive alternatives, such as aggregated or anonymous information, would have provided ample basis for OAG to investigate the truthfulness of Meta's public statements about its general efforts to combat COVID-19 misinformation without raising the same First Amendment concerns. OAG has no legitimate need to know the identities of each and every Facebook user who violated Meta's COVID-19 misinformation policies, the specific details of each violation, or the editorial decisions Meta made in each case. Accordingly, even if OAG's request could be squared with the SCA—which it cannot—the Superior Court's order should be reversed because it fails to comply with the First Amendment.

ARGUMENT

I. OAG MAY COMPEL DISCLOSURE OF THE INFORMATION SOUGHT IN REQUEST #2 ONLY BY USING A WARRANT

Under the SCA, a governmental entity seeking to compel disclosure of user communications may do so only as provided in Section 2703. Here, because Request #2 seeks the contents of communications, Section 2703 requires OAG to use a warrant. 18 U.S.C. § 2703(a). The Superior Court's contrary interpretation of the SCA—which appears to be unprecedented—contravenes the statute's text, structure, and legislative history and case law applying it. If upheld, the interpretation would dramatically expand the power of any governmental entity to compel the disclosure of customer communications—not only in investigations of providers, such as this one, but also in investigations targeting one or more of the billions of individual users of these services. To restore the robust protections for users that Congress intended, this Court should reverse.

A. The Text And Structure Of The SCA Make Clear A Governmental Entity Must Comply With Section 2703 To Compel Disclosure

Analysis of the SCA begins and ends with the statutory text, which controls where, as here, "the language is unambiguous and does not produce an absurd result." *Facebook, Inc. v. Pepe*, 241 A.3d 248, 254 (D.C. 2020) (quoting *Facebook, Inc. v. Wint*, 199 A.3d 625, 628 (D.C. 2019)). That language demonstrates that a governmental entity, including OAG, may compel disclosure

of user communications only by complying with the applicable requirements of Section 2703.

As enacted, Section 2703 set forth the "[r]equirements for governmental access" to stored electronic communications. 100 Stat. 1861.[18] Recognizing the potential mismatches between traditional Fourth Amendment doctrine and communications over an online network, Congress enacted the SCA—and Section 2703 in particular—to ensure that "Fourth Amendment-like privacy protections" would continue to safeguard communications on the Internet. Kerr, 72 Geo. Wash. L. Rev. at 1214; *see also, id.* at 1209-1220; H.R. Rep. No. 99-647, at 68 (1986) (in discussing Section 2703, noting that "[t]he [House] Committee required the government to obtain a search warrant because it concluded that the contents of a message in storage were protected by the Fourth Amendment"). Where contents of communications are at issue—the most sensitive information the government might seize—Congress imposed the most stringent standard for governmental access by requiring the government to obtain a warrant. Specifically, Section 2703(a)(1) provides that a governmental entity "may require" an ECS provider,

---

[18] In 2001, Congress amended the title of Section 2703 to its current heading: "Required disclosure of customer communications or records." Pub. L. No. 107-56, § 212, 115 Stat. 272, 285 (2001). At the same time, Congress amended the title of Section 2702 to read "Voluntary disclosure of customer communications or records." 115 Stat. 284.

such as Meta, to disclose the contents of communications in electronic storage for one hundred and eighty days or less "*only* pursuant to a warrant." 18 U.S.C. § 2703(a) (emphasis added). "Only" is a term of exclusion. It means "alone in a class or category: sole." *Merriam-Webster Online Dictionary* ("only").[19] The text of Section 2703(a) thus leaves no doubt that a warrant is the sole—exclusive—means by which the government "may require" disclosure of content stored for 180 days or less.

Even as to content in storage for more than 180 days, Section 2703 permits a "governmental entity" to "require … disclos[ure]" using an administrative subpoena—like the one at issue here—only if the government provides "prior notice" to the subscriber. 18 U.S.C. § 2703(b). Otherwise, a "warrant" is required. *Id.*[20]

The statute delineates only a narrow category of information that a "governmental entity may require a provider … to disclose" using an administrative subpoena alone, and that category is limited to certain non-content records. 18 U.S.C. § 2703(c) (2). In this way, the statute carefully specifies and

---

[19] *Available at* https://www.merriam-webster.com/dictionary/only.

[20] As noted above, the SCA's original distinction between communications in storage for more or less than 180 days has been largely abrogated because users can have a reasonable expectation of privacy in their content regardless of how long the communication has been in storage. *Supra* p. 8.

restricts the circumstances in which a governmental entity may use an "administrative subpoena" to compel disclosure. *See Andrus v. Glover Constr. Co.*, 446 U.S. 608, 616-617 (1980) ("Where Congress explicitly enumerated certain exceptions[,] … additional exceptions could not be implied in the absence of evidence of a contrary legislative intent."). The Superior Court's interpretation disregards Congress's deliberate decision to limit when an administrative subpoena may be used.

The SCA's structure likewise confirms that the government may compel disclosure of stored communications only by complying with Section 2703. *See, e.g.*, *Wint*, 199 A.3d at 628 (taking legislature's "structural choices into consideration when interpreting statutory provisions" (quotation marks omitted)); *Nunnally v. District of Columbia Metro. Police Dep't*, 80 A.3d 1004, 1010-1011 (D.C. 2013) (statutory text must be interpreted in light of context). As this Court explained in *Wint*, the SCA carefully distinguishes between the rules governing "[v]oluntary disclosure," which are set forth in Section 2702, and those governing "[r]equired disclosure" to "governmental entities," which are set forth in Section 2703. *Wint*, 199 A.3d at 628 (quotation marks omitted). For this reason, the U.S. Department of Justice has acknowledged that Section 2703, not Section 2702, outlines the steps that "federal and state law enforcement officers must follow to compel disclosure" of content under the SCA. DOJ, *Searching and Seizing*

Computers and Obtaining Electronic Evidence in Criminal Investigations 115-116 (2009), *supra* note 1.

The Superior Court blurred the distinction between Sections 2702 and 2703 by recasting the question in this case as whether the government may "obtain" content via the provisions in Section 2702. App. 23. But that has never been in dispute. Sections 2702(b)(3) and (6)-(9), for example—including the consent exception that the Superior Court found applicable here—expressly permit an ECS provider to *voluntarily* disclose content without violating the general prohibition of Section 2702 under specified circumstances, including to governmental entities. 18 U.S.C. § 2702(b)(3), (6)-(9). The issue here, however, is not whether Meta may voluntarily disclose the requested customer communications without violating the SCA (which would be governed by Section 2702). It is whether OAG, a governmental entity, may unilaterally *compel* Meta to disclose information protected by the SCA. That demand must adhere to Section 2703's rules governing "required" disclosures, 18 U.S.C. § 2703(a), not Section 2702's rules for "[v]oluntary" disclosures.[21]

[21] The Superior Court relatedly construed Meta's argument as a contention about the scope of the consent exception itself, analyzing whether Section 2702(b)(3) permits disclosure only "to non-governmental entities." App. 22. But that, again, has never been in dispute. That OAG is a "governmental entity" is relevant not because it implicates some limitation in Section 2702(b)(3), but

B. The SCA's Legislative History Confirms That OAG May Compel Disclosure Only As Provided In Section 2703

Although the statutory text and structure alone suffice to demonstrate the Superior Court's error, the SCA's legislative history further supports the conclusion that a governmental entity seeking to compel disclosure must comply with Section 2703. *See Wint*, 199 A.3d at 628 ("We may also look to the legislative history to ensure that our interpretation is consistent with legislative intent."). The Senate and House Reports accompanying the SCA could not be more clear. The Senate Report explains that Section 2703(a) "provides requirements for the government to obtain the contents of an electronic communication that has been in electronic storage for 180 days or less. A government entity *can only* gain access to the contents of such an electronic communication pursuant to a warrant[.]" S. Rep. No. 99-541, at 38 (1986) (emphasis added). And as to communications in storage for more than 180 days, the Senate Report similarly emphasizes that "[i]f the Government wishes to obtain the contents of a communication without the required notice to the subscriber then the governmental entity *must obtain* a warrant[.]" *Id.* (emphasis added). The House Report likewise explains that Section 2703 sets forth "the procedures the government *must use* before it can obtain access to the contents of any electronic

---

because compelled disclosure of stored communications by "governmental entit[ies]" is subject to the requirements of Section 2703.

communication held by a provider of remote computing services." H.R. Rep. No. 99-647, at 67-68 (emphasis added).

The Superior Court disregarded this legislative history. Instead, the court speculated that Congress would not have had "any reason" to "prevent[] disclosure of content to government agencies with user consent." App. 23. But that reasoning ignores Congress's purpose in the SCA to adapt the Fourth Amendment's protections to evolving technologies—protections aimed at "guard[ing] against the arbitrary use of Government power to maintain surveillance over citizens." S. Rep. No. 99-541, at 1-2. Congress enacted unique "[r]equirements for *governmental* access" in particular, *id.* at 38 (emphasis added); *see* 100 Stat. 1861, because it recognized that "the enormous power of the government makes the potential consequences of its snooping far more ominous than those of … a private individual or firm," H.R. Rep. No. 99-647, at 19. By excusing the government from complying with Section 2703's strict requirements whenever the consent exception applies to permit a voluntary disclosure, the Superior Court gutted the SCA's protections against arbitrary use of that "enormous power," *id.*—not just in cases like this one, but in any case in which a governmental entity targets one of Facebook's billions of users for investigation.

Moreover, the Superior Court's assumption (App. 23) that Congress would have considered it unnecessary to demand compliance with Section 2703 in cases

involving user consent again ignores the statutory text. Where Congress intended user consent to supply an alternative source of authority for the government to compel disclosure without using the required legal process, Congress said so explicitly. Under Section 2703(c), a governmental entity "may require … disclos[ure]" of non-content records of electronic communications either by obtaining a warrant or court order, "*or*" by demonstrating "the consent of the subscriber or customer to such disclosure." 18 U.S.C. § 2703(c)(1)(C) (emphasis added). If Congress had similarly wished to allow the government to compel disclosure of contents either by obtaining a warrant or by demonstrating user consent, it "surely could have said so." *Riggs Nat'l Bank of Wash., D.C. v. District of Columbia*, 581 A.2d 1229, 1237 (D.C. 1990). Instead, Congress provided that the government may do so "only pursuant to a warrant" (allowing lesser legal process only for certain communications if accompanied by "prior notice") and did not cite user consent as an acceptable alternative. *Supra* p. 7. Congress's choice should be respected. *Virginia Uranium, Inc. v. Warren*, 139 S. Ct. 1894, 1900 (2019) (plurality) (courts must "respect not only what [the legislature] wrote but, as importantly, what it didn't write").

Indeed, the Superior Court's holding renders the reference to user consent in Section 2703(c)(1)(C) mere surplusage. Section 2702's provisions governing voluntary disclosure of non-content records—like the corresponding provisions

governing voluntary disclosure of contents, on which the Superior Court relied—permit an ECS provider to disclose records "with the lawful consent of the customer or subscriber." 18 U.S.C. § 2702(c)(2). Under the Superior Court's reasoning, in cases where that exception applied, the consent provision in Section 2703(c)(1)(C) would be wholly superfluous. This Court "must avoid" an interpretation that fails to give "effective meaning" to all of the SCA's terms. *District of Columbia v. District of Columbia Pub. Serv. Comm'n*, 963 A.2d 1144, 1157 (D.C. 2009) (quotation marks omitted).

C. The Superior Court's Decision Stands Alone

Although case law is limited, those courts that have addressed the question agree that governmental entities seeking to compel disclosure must comply with Section 2703. The Superior Court's decision here appears to be the sole outlier.

In *Facebook, Inc. v. Pepe*, 241 A.3d 248 (D.C. 2020), this Court considered the enforceability of a subpoena served by a criminal defendant seeking to obtain contents and records of an Instagram account that the defendant claimed was necessary to support his defense at trial. In determining the enforceability of the subpoena, the Court applied only Section 2702, and not 2703, because the proponent of the subpoena was not a "governmental entity." *See id.* at 253-254. This Court held the subpoena was enforceable because certain exceptions in Section 2702 (including the consent exception) applied. *Id.* at 254-255. Moreover,

the Court rejected the argument that Section 2702 gives the service provider "unfettered discretion" to choose whether to disclose that "preempts" the proponent's "ability to obtain information" by subpoena. *Id.* at 256. As the Court explained, where an exception to Section 2702's "general prohibition on disclosure" applies, the barrier to compliance with the subpoena is removed. *Id*. at 257. *Pepe* thus teaches that the permissive exceptions to Section 2702's general prohibition, standing alone, "do not purport to authorize providers to refuse" to comply with otherwise valid compulsory process. *Id.*

Significantly, however, in so holding, the Court was careful to distinguish the case before it—which involved a private litigant—from "[g]*overnmental* access to customer communications or records by warrant, subpoena, or court order." *Pepe*, 241 A.3d at 254 n.12 (emphasis added). The latter, the Court emphasized, "is addressed separately in [Section] 2703." *Id.* Thus, even where an exception in Section 2702 would permit a service provider to respond to valid compulsory process—and, under *Pepe*, would give the provider no authority to refuse—it is Section 2703 that addresses whether compulsory process served by a governmental entity is valid in the first place. As this Court observed, in circumstances when a provider "*must* divulge" information, the "mandat[e]" to do so comes not from Section 2702 itself, but from other provisions (such as Section 2703). *Id.* at 258 & n.30; *see id.* at 258 n.30 (noting that Section 2702 references mandatory disclosure

to governmental entities "*pursuant to*" the "*means specified in [Section] 2703*" (emphasis added)).

Accordingly, although *Pepe* had no occasion to consider an effort by a governmental entity to compel disclosure of contents using only a subpoena, its reasoning strongly indicates that the enforceability of such a subpoena is a question governed by Section 2703. Courts that have directly confronted government efforts to compel disclosure without complying with Section 2703 have reached the same conclusion. In *FTC v. Netscape Communications Corp.*, 196 F.R.D. 559 (N.D. Cal. 2000), the district court denied the FTC's motion to compel Netscape to provide non-content records in response to a subpoena that did not conform to the requirements of Section 2703. As the court explained, Section 2703 "enumerates" the "specif[ied] types" of legal process that agencies may use to compel disclosure and that "[t]o decide otherwise would effectively allow" the government to use other means (there, a Rule 45 discovery subpoena) to "circumvent the precautions and protections built into the [SCA] to protect subscriber privacy from government entities." *Id.* at 561. Similarly, in *People v. Harris*, 949 N.Y.S.2d 590 (N.Y. Crim. Ct. 2012), the court held that the New York County District Attorney's office "must obtain a search warrant" to "compel" Twitter to disclose the contents of

certain Tweets that had been in storage for 180 days or less. *Id.* at 596. Indeed, the court reached that conclusion even though the Tweets were publicly posted.[22]

The Superior Court cited no decisions to the contrary. App. 21-24; *see also* App. 41-42. Nor did OAG in opposing Meta's motion for reconsideration. Opp. to Meta's Mot. for Reconsideration 7-8 (Apr. 27, 2022). The Superior Court relied instead only on *Pepe*, but that reliance was gravely misplaced. The court construed *Pepe* to "hold[] that if disclosure by Facebook is *permitted* under [an exception to Section 2702], the same disclosure can be *compelled* by subpoena." App. 24. As explained, *Pepe* held no such thing. It instead recognized that whether a governmental entity may compel disclosure is not governed by Section 2702, but is "addressed separately in § 2703." 241 A.3d at 254 n.12; *see also Facebook, Inc. v. Superior Court*, 417 P.3d 725, 739 (Cal. 2018) (Section 2703 "governs compelled disclosure by covered providers to a governmental entity"). The Superior Court's decision thus stands alone in licensing a dramatic expansion of the government's authority to obtain the contents of user communications without complying with

[22] With respect to Tweets in storage for more than 180 days, the *Harris* court ordered their disclosure—but again, the court did so only because the court found that the government had complied with applicable requirements of Section 2703. *See Harris*, 949 N.Y.S.2d at 596 (holding that the contents of public tweets older than 180 days were "covered by the court order" that satisfied the requirements of Section 2703).

the protections Congress imposed in the SCA. This Court should correct that unfounded expansion.

II. REQUEST #2 VIOLATES THE FIRST AMENDMENT

The Superior Court erred in granting OAG's petition to enforce for a second, independent reason: enforcing the subpoena would infringe the First Amendment rights of both Meta itself and Meta's users, and OAG has not satisfied the exacting scrutiny required to justify such intrusions. Request #2 seeks highly detailed information about Meta's content-moderation decisions—information that is at the core of Meta's own First Amendment right to exercise editorial control and judgment over its platform. And the need for First Amendment protection is even more heightened here because Request #2 also targets Meta's users by seeking to unmask those who engaged in speech that is disfavored by OAG—namely, those who the OAG believes are responsible for harmful "proliferation of misinformation related to COVID-19 vaccines." App. 8.

Meta does not condone vaccine-related misinformation on its platform and seeks to remove and restrict it. There is, however, a world of difference between a private company, like Meta, taking such steps to regulate the content on its own privately operated website and the government demanding to know the identities of millions of people whose speech the government finds undesirable. "When it comes to 'a person's beliefs and associations,' '[b]road and sweeping state

inquiries into these protected areas … discourage citizens from exercising rights protected by the Constitution.'" *Americans for Prosperity Found. v. Bonta*, 141 S. Ct.2373, 2384 (2021) (quoting *Baird v. State Bar of Ariz.*, 401 U.S. 1, 6 (1971) (plurality op.) (emphasis added)). If the Superior Court's order is upheld, OAG or other government entities across the country could demand the identities of any number of targeted groups online—from racial-justice advocates to tax-reform advocates—under the guise of consumer protection, even without establishing a compelling justification and even without first pursuing less burdensome alternatives. To protect the rights of both Meta and Meta's users, this Court should reverse.

A. Request #2 Must Satisfy Exacting First Amendment Scrutiny

OAG's Request #2 demands granular information about every individual content-moderation decision Meta made regarding its enforcement of its COVID-19 vaccine-related misinformation policies over the course of months, including a list identifying each individual user Meta determined to have violated such policies. The First Amendment sharply restricts OAG's authority to compel such information (unless it can satisfy First Amendment scrutiny) for two distinct reasons.

First, OAG's demand probes and penalizes Meta's own First Amendment right to "exercise … editorial control and judgment" over what content is

disseminated through its platform. *Miami Herald Publ'g Co. v. Tornillo*, 418 U.S. 241, 257-258 (1974). Numerous courts have recognized that "[w]hen platforms choose to remove users or posts, deprioritize content in viewers' feeds or search results, or sanction breaches of their community standards, they engage in First-Amendment-protected activity." *NetChoice, LLC v. Attorney Gen., Fla.*, 34 F.4th 1196, 1213 (11th Cir. 2022). The editorial judgment exercised by social-media platforms is "inherently expressive." *Id.* "This is because a platform's decision to publish or not publish particular [content] says something about what that platform represents." *O'Handley v. Padilla*, 579 F. Supp. 3d 1163, 1188 (N.D. Cal. 2022), *appeal docketed* (9th Cir. Jan 18, 2022). Like a newspaper deciding which articles to publish or a parade organizer deciding which groups to let march, Meta's content-moderation decisions "operate[] together" to "shape and develop the nature, tone, and substance of the ongoing dialogue" on Facebook. *Id.*; *see also Hurley v. Irish-American Gay, Lesbian & Bisexual Group*, 515 U.S. 557, 568-569 (1995) (holding that parades are "a form of expression" that organizers exercise "by combining multifarious voices"); *Miami Herald*, 418 U.S. at 257-258 (holding that First Amendment protects newspaper's editorial judgments about what to publish in the newspaper). As the Supreme Court recently reaffirmed, the First Amendment protects "private entities' rights to exercise editorial control over speech and speakers on their properties or platforms." *Manhattan Cmty. Access*

Corp. v. Halleck, 139 S. Ct. 1921, 1932 (2019). "[W]hether" Meta's editorial judgments are deemed "fair or unfair," these expressive judgments are Meta's, not the government's, to make. *Miami Herald*, 418 U.S. at 258; *see also NetChoice*, 34 F.4th at 1210.[23]

Absent adequate justification and tailoring, the First Amendment bars OAG from using its investigative power to scrutinize and pressure Meta into changing how it exercises this protected editorial control over its platform, as OAG's demands do here. "Clearly, an investigation is subject to the command that the Congress shall make no law abridging freedom of speech or press or assembly." *Watkins v. United States*, 354 U.S. 178, 197 (1957). Accordingly, the First Amendment "may be invoked against infringement" by government investigations

---

[23] *See also Davison v. Facebook, Inc.*, 370 F. Supp. 3d 621, 629 (E.D. Va. 2019) ("Facebook has, as a private entity, the right to regulate the content of its platforms as it sees fit."), *aff'd*, 774 F. App'x 162 (4th Cir. 2019); *Isaac v. Twitter, Inc.*, 557 F.Supp.3d 1251, 1261 (S.D. Fla. Aug. 30, 2021) (Twitter "has a First Amendment right to decide what to publish and what not to publish on its platform") (quotation marks and citation omitted); *La'Tiejira v. Facebook, Inc.*, 272 F. Supp. 3d 981, 991 (S.D. Tex. 2017) (acknowledging "Facebook's First Amendment right to decide what to publish and what not to publish on its platform"); *Publius v. Boyer-Vine*, 237 F. Supp. 3d 997, 1008 (E.D. Cal. 2017) (owner of website has "First Amendment right to distribute and facilitate protected speech on the site"); *Zhang v. Baidu.com Inc.*, 10 F. Supp. 3d 433, 437-443 (S.D.N.Y. 2014) (holding that suit "to hold [website] liable for ... a conscious decision to design its search-engine algorithms to favor certain expression on core political subjects over other expression on those same political subjects" would "violate[] the fundamental rule of protection under the First Amendment, that a speaker has the autonomy to choose the content of his own message").

because "[a]buses of the investigative process may imperceptibly lead to abridgment of" First Amendment rights. *Id.* A government investigation is "sufficiently chilling when it is likely [to] deter a person of ordinary firmness from the exercise of First Amendment rights." *Benham v. City of Charlotte*, 635 F.3d 129, 135 (4th Cir. 2011) (quotation marks omitted).

In *White v. Lee*, for example, the Ninth Circuit held that an investigation by the Department of Housing and Urban Development ("HUD") into plaintiffs' opposition to a development project "unquestionably chilled the plaintiffs' exercise of their First Amendment rights" even though, unlike here, cooperation with the investigation was "'voluntary'" and HUD's document requests and questioning of residents occurred only "under *threat* of subpoena," rather than compulsory legal process. 227 F.3d 1214, 1223, 1228-1229 (9th Cir. 2000) (emphasis added); *see also Brodheim v. Cry*, 584 F.3d 1262, 1270 (9th Cir. 2009) (a government official's "'warn[ing]' … to stop doing something" was actionably adverse because "[b]y its very nature, … [it] carries the implication of some consequence of a failure to heed that warning").[24]

---

[24] *See also Abu-Jamal v. Price*, 154 F.3d 128, 136 (3d Cir. 1998) (enjoining "the investigation and enforcement" of a rule after finding First Amendment injury by an "investigation … [that] was both threatened and occurring"); *Pendleton v. St. Louis Ctny.*, 178 F.3d 1007, 1011 (8th Cir. 1999); *Little v. City of N. Miami*, 805 F.2d 962, 968 (11th Cir. 1986) (per curiam).

Because OAG's demand for detailed information about specific content-moderation decisions intrudes on Meta's First Amendment rights, OAG must, at a minimum, "convincingly show a substantial relation between the information sought and a subject of overriding and compelling interest." *Gibson v. Florida Legislative Investigation Comm*., 372 U.S. 539, 546 (1963); *see also Zerilli v. Smith*, 656 F.2d 705,714-715 (D.C. Cir. 1981) (applying a similar balancing test and concluding that appellants there were not entitled to disclosure because "appellants clearly have not fulfilled their obligation to exhaust possible alternative sources of information"); *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1057 (Colo. 2002) (en banc) ("Further, when government action implicates fundamental expressive rights, . . . courts commonly require that government action be no broader than necessary to advance its compelling interest.").

Second, even apart from Meta's own First Amendment rights, OAG's "dragnet" demand "for sensitive [identifying] information" threatens the First Amendment rights of Meta's users. *See Americans for Prosperity*, 141 S. Ct. at 2387. OAG seeks to identify potentially millions of users "associated with" speech that it views as undesirable. In this case, the speech concerns COVID-19 misinformation; in the next case, it could be some other topic that OAG or government officials in other jurisdictions choose to target—from immigration to tax policy. As the Supreme Court has made clear, "identification and fear of

reprisal might deter perfectly peaceful discussions of public matters of importance." *Talley v. California*, 362 U.S. 60, 65 (1960); *see also (WIN) Wash. Initiatives Now v. Rippie*, 213 F.3d 1132, 1138-1139 (9th Cir. 2000) (compelled disclosure to the State of the identities of online speakers chills speech). And that is all the more true in this case given the contentious nature of the speech at issue here. *See* App. 29 ("[P]eople on all sides of this debate may be (and probably have been) subjected to harsh or unfair criticism or even threats by others who disagree with them."); *see also Americans for Prosperity*, 141 S. Ct. at 2381 (applying heightened scrutiny because those whose identities were sought had been subject to harassment and "were likely to face similar retaliation in the future"). The Superior Court thus correctly recognized that "[j]ust as '[c]ompelled disclosure of affiliation with groups engaged in advocacy may constitute as effective a restraint on freedom of association as other forms of governmental action,' so too may compelled disclosure of speakers espousing unpopular points of view restrain freedom of expression." App. 29 (quoting *Americans for Prosperity*, 141 S. Ct. at 2382).[25]

[25] Courts permit service providers to assert their users' rights to free speech when those rights are at stake, as they are here. *See, e.g.*, *Publius*, 237 F. Supp. 3d at 1008-1009 n.5.

To protect the rights of both Meta and Meta's users, the First Amendment required OAG to justify the disclosure compelled by Request #2 under "exacting scrutiny."[26] *Americans for Prosperity*, 141 S. Ct. at 2383 ("compelled disclosure requirements are reviewed under exacting scrutiny"); *Buckley v. Valeo*, 424 U.S. 1, 64 (1976) ("We long have recognized that significant encroachments on First Amendment rights of the sort that compelled disclosure imposes … must survive exacting scrutiny."); *see also supra* p. 38 (discussing *Gibson*, 372 U.S. at 545-546). Under this standard, there must be "a substantial relation between the [Request] and a sufficiently important governmental interest." *Americans for Prosperity,* 141 S. Ct. at 2383 (quoting *Doe v. Reed*, 561 U.S. 186, 196 (2010). Additionally, the government's Request must be "narrowly tailored to the interest it promotes." *Id.* at 2384. As explained below, Request #2 cannot satisfy that heavy burden. [27]

---

[26] Because Request #2 seeks a content-based disclosure, it arguably should be subject to "strict scrutiny." *See, e.g.*, *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015) (noting that government regulation of speech that "target[s] speech based on its communicative content—[is] presumptively unconstitutional and may be justified only if the government proves that [it is] narrowly tailored to serve compelling state interests"). But Request #2 fails even the "exacting scrutiny" standard.

[27] *See also In re First Nat'l Bank,* 701 F.2d 115, 118-119 (10th Cir. 1983) (holding subpoena that would chill First Amendment conduct unenforceable absent showing of "compelling need to obtain documents identifying" members); *United States v. Citizens State Bank*, 612 F.2d 1091, 1094 (8th Cir. 1980) (reversing enforcement of subpoena request due to district court's failure to consider First

B. Request #2 Is Neither Substantially Related To A Sufficiently Important Interest Nor Narrowly Tailored

The Superior Court erred in concluding that OAG's extremely broad demand for detailed information about millions of content moderation decisions and the identities of millions of Facebook users satisfies exacting scrutiny.

To start, OAG failed to show that obtaining such wide-ranging information is substantially related to any sufficiently important governmental interest. The sole interest that OAG proffered is to assess whether Meta has made false or misleading statements about its efforts to combat COVID-19 vaccine-related misinformation that violated the District's consumer protection statute. App. 8. While OAG has a legitimate interest in consumer protection in general, however, it did not establish that interest is genuinely implicated here. As the Superior Court acknowledged, and OAG admitted, Meta has not made any public statements quantifying its efforts to restrict "COVID-19 *vaccine* misinformation in particular." App.30. Instead, Meta has made only highly general "public statements about its zeal in enforcing its policies and about the amount of content

---

Amendment implications); *Solers, Inc. v. Doe*, 977 A.2d 941, 951 (D.C. 2009) (denying enforcement of subpoena for "identifying information" due to First Amendment concerns). In fact, "courts have held that the threat to First Amendment rights may be more severe in discovery than in other areas because a party may try to gain advantage by probing into areas an individual or group wants to keep confidential." *Wyoming v. USDA*, 208 F.R.D. 449, 454-455 (D.D.C. 2002) (granting motion to quash subpoenas issued by Wyoming due to First Amendment concerns).

that it has taken down." *Id*. The Superior Court cited, for example, statements including "we've been … taking aggressive steps to stop misinformation and harmful content from spreading" and "[t]hese new policies will help us to continue to take aggressive action against misinformation about COVID-19 and vaccines." Super. Ct. OAG's Reply ISO Pet. for Enforcement 2 n.1 (Feb. 22, 2022); *see* App 30 (citing that statement erroneously to Reply 2 n.2).

But OAG has never shown that these are the kinds of statements that could—consistent with the First Amendment—form the basis of a valid enforcement action under the District's consumer protection laws. If the Washington Post or Fox News were to claim, for example, that they were "aggressively investigating government corruption" and "leaving no stone unturned," that would not permit OAG to demand the notebooks of all of their investigative reporters to test whether any consumers might be misled by such statements. And indeed, in analogous contexts, courts have concluded that similarly "[l]ofty but vague statements" about content moderation in particular are "impervious to being 'quantifiable'" and thus are non-actionable "puffery." *Prager Univ. v. Google LLC*, 951 F.3d 991, 1000 (9th Cir. 2020); *see also Glen Holly Entm't, Inc. v. Tektronix Inc*., 352 F.3d 367, 379 (9th Cir. 2003) (finding that "statements—generally describing the 'high priority'" a company places on certain efforts "were generalized, vague and unspecific assertions, constituting mere

'puffery' upon which a reasonable consumer could not rely"); *In re Harman Int'l Indus., Inc. Sec. Litig.*, 791 F.3d 90, 109 (D.C. Cir. 2015) (distinguishing actionable statements that "'could have misled a reasonable investor'" from "puffery" or "generalized statements of optimism that are not capable of objective verification"); *Lewis v. Google* LLC, 461 F. Supp. 3d 938, 950, 959 (N.D. Cal. 2020) (concluding that YouTube's statements that it believes "people should be able to speak freely, share opinions, foster open dialogue" and "have easy, open access to information" were non-actionable puffery), *aff'd*, 851 F. App'x 723 (9th Cir. 2021). The Superior Court should have rejected OAG's demands on this basis alone. *See WIN*, 213 F.3d at 1139 (finding state's interest in combatting campaign fraud was insufficient to override First Amendment burden where disclosure of names and identities would not establish whether crime occurred).

The Superior Court similarly erred in concluding that OAG's sweeping demands are narrowly tailored to any important interest. Even a "legitimate and substantial" governmental interest "cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved." *Shelton v. Tucker*, 364 U.S. 479, 488 (1960); *Americans for Prosperity*, 141 S. Ct. at 2384 ("Narrow tailoring is crucial where First Amendment activity is chilled."). Narrow tailoring fails where there is a "dramatic mismatch" between the interest

promoted and the "amount and sensitivity" of the information sought "in [purported] service of that end." *Americans for Prosperity*, 141 S. Ct. at 2386.

There is such a dramatic mismatch here. Even if OAG could establish a legitimate interest in investigating Meta's general statements about "aggressive[ly]" combatting COVID-19 vaccine-related misinformation, *but see supra* p. 41, OAG would hardly need to learn the identities of every Facebook user worldwide "associated with" demoted, flagged, or removed content hostile to COVID-19 vaccines to pursue that investigation. The Superior Court suggested that OAG might need all this information so it could assess "whether and how Facebook enforces its policies against repeat violators." App.30. Yet the court did not explain how anything learned about Meta's handling of repeat violators could possibly render Meta's vague public statements false or misleading. And neither the court nor OAG has ever explained why this or other inquiries could not be pursued through "any less intrusive alternatives," *Americans for Prosperity*, 141 S. Ct. at 2386, such as by obtaining a far smaller set of records related to "users who have been publicly identified as repeat violators," App.30, by evaluating aggregate information responsive to OAG's other subpoena requests, *supra* p. TK (describing other requests), or by obtaining more limited information that does not reveal users' identities.

OAG's other explanations reveal an even greater disconnect between the interest promoted and information sought. OAG cited Meta's August 2021 announcement that it "removed 20 million items of content that violated its COVID-19 misinformation policies," Pet. Mem. 4, but these statements are not limited to Meta's efforts to restrict COVID-19 *vaccine* misinformation, which is what the OAG is purportedly investigating. Vaccine misinformation constitutes only a subset of Meta's overall COVID-19 misinformation-related efforts encapsulated in the 20 million removed items. Facebook also, for example, prohibited posts encouraging sale of unofficial COVID-19 test kits, coordinating the deliberate spread of COVID-19, and denying the existence of COVID-19.[28] Even more fundamentally, OAG has never explained—nor could it—how the incredibly detailed and intrusive information that it seeks about identifiable individual users is necessary to evaluate any statement about the total number of posts that Meta has removed. Meta has already provided OAG with information regarding the content that Meta has removed. *See supra* 13. OAG cannot demonstrate that less restrictive alternatives, such as anonymized or aggregate information, would be insufficient to assess the veracity of Meta's statements about its general efforts regarding COVID-19 misinformation. Obtaining the

---

[28] *COVID-19 and Vaccine Policy Updates & Protections*, *supra* note 8.

actual identities of potentially millions of specific users whose content *was* removed or restricted will "have no possible bearing upon" OAG's apparent effort to show that Meta has failed to take action against as much content as it claimed. *Shelton*, 364 U.S. at 488. This misalignment between the demand for Meta to identify potentially millions of users and the specific statements that OAG claims to be investigating further confirms the need to quash Request #2. *See id.* at 490 (holding State's interest in teacher fitness insufficient to compel disclosure of every organization to which each teacher belonged).

C. The Superior Court's Other Reasons For Rejecting Meta's First Amendment Arguments Were Mistaken

The Superior Court provided other rationales for its decision but none can withstand scrutiny.

First, the Superior Court wrongly concluded that enforcing the subpoena would not infringe Meta's First Amendment rights because OAG claims only to be investigating Meta's public statements and is supposedly not trying to "dictate to Meta what content should remain on, or what content should be removed from, Facebook." App.27. That explanation beggars belief for all the reasons set forth above. If OAG were indeed investigating Meta's public statements, it could identify a set of potentially actionable statements that might legitimately underpin a bona fide consumer protection investigation and that bore the necessary close relationship to the sweeping information that OAG seeks. It has not.

But in any event, Meta's First Amendment rights are implicated here regardless of whether OAG has an interest in investigating Meta's public statements because the vast repository of information OAG is seeking lies at the heart of Meta's First Amendment rights. A subpoena that demanded notes taken at every editorial board meeting of a newspaper would surely trigger demanding First Amendment scrutiny. *See Gibson*, 372 U.S. at 546. By that same token, OAG cannot demand granular information about millions of specific content-moderation decisions—each of which reflect Meta's exercise of editorial control and judgment—without establishing that the government's interest in the subject matter of the investigation is "immediate, substantial, and subordinating," that there is a "substantial connection" between the information it seeks and the overriding governmental interest in the subject matter of the investigation, and that the means of obtaining the information is not more drastic than necessary to forward the asserted governmental interest. *Id.* at 551.

Second, the Superior Court wrongly discounted the First Amendment rights of Meta's users on the theory that Request #2 would not unmask any anonymous user because OAG seeks information identifying only users who posted publicly. That is both wrong and irrelevant. It is wrong because although users may have created public-facing posts, their identities would be hidden from the public unless their profiles included accurate and complete identifying information. The

Superior Court assumed that public posts would necessarily include accurate identifying information because Meta's rules require users to identify themselves using the same name they use in everyday life. But that ignores that some users nonetheless do not do so; and it ignores that OAG's demand for information "sufficient to identify … the identity of any individuals or entities," App. 9, that posted vaccine-related misinformation could include non-public addresses or phone numbers provided only to Meta that would reveal users' true identities and thus does implicate the robust right to "remain anonymous." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 341-342 (1995); *see also Solers, Inc. v. Doe*, 977 A.2d 941, 950-951 (D.C. 2009). Moreover, even if "some … might not mind—or might even prefer—the disclosure of their identities to the State," preventing disclosure of identifying information to the government remains important to the many users who prefer to remain anonymous. *Americans for Prosperity*, 141 S. Ct. at 2388.

The fact that some users might have identified themselves in public posts that have since been demoted or removed from Facebook is also irrelevant because naming names *to the government* uniquely risks chilling the First Amendment rights of Meta's users. As the Supreme Court has explained, "each government demand for disclosure brings with it an additional risk of chill." *Americans for Prosperity*, 141 S. Ct. at 2389. Consider, for example, a user grappling with

whether to vaccinate her family who posts a question premised on some misinformation she read elsewhere on the internet. That user might be willing to accept public criticism for her "voluntary and non-anonymous participation in public debates," App.32, and might be unbothered by the relatively mild imposition of having that post demoted on Facebook itself. But that does not mean that such a user would have no concerns about having her name and post turned over to the government on a blacklist of users associated with content that the government disfavors. Moreover, Request #2 most certainly risks chilling the robust discussion of COVID vaccines among millions of users on the Facebook platform, precisely what the First Amendment prohibits the government from doing.

CONCLUSION

The Court should reverse the order enforcing Request #2 of the administrative subpoena.

Respectfully submitted,

/s/ Catherine M.A. Carroll

JOSHUA S. LIPSHUTZ
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, NW
Washington, DC 20036-5306
(202) 955-8500

CATHERINE M.A. CARROLL*
*Counsel for Oral Argument
RONALD C. MACHEN
GEORGE P. VARGHESE
ARI HOLTZBLATT
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW

Washington, DC 20006
(202) 663-6000

October 4, 2022

CERTIFICATE OF COMPLIANCE

I hereby certify that this brief complies with the type-page limitations of D.C. Ct. App. R. 32(a)(5)-(6).

1. Exclusive of the exempted portions of the brief, as provided in D.C. Ct. App. R. 32(a)(6), the brief contains 49 pages.

2. The brief, including footnotes, has been prepared in 14-point Times New Roman font.

/s/ *Catherine M.A. Carroll*
CATHERINE M.A. CARROLL
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 663-6000

October 4, 2022

District of Columbia
Court of Appeals

REDACTION CERTIFICATE DISCLOSURE FORM

Pursuant to Administrative Order No. M-274-21 (filed June 17, 2021), this certificate must be filed in conjunction with all briefs submitted in all cases designated with a "CV" docketing number to include Civil I, Collections, Contracts, General Civil, Landlord and Tenant, Liens, Malpractice, Merit Personnel, Other Civil, Property, Real Property, Torts and Vehicle Cases.

I certify that I have reviewed the guidelines outlined in Administrative Order No. M-274-21 and Super. Ct. Civ. R. 5.2, and removed the following information from my brief:

1. All information listed in Super. Ct. Civ. R. 5.2(a); including:

   - An individual's social-security number
   - Taxpayer-identification number
   - Driver's license or non-driver's' license identification card number
   - Birth date
   - The name of an individual known to be a minor
   - Financial account numbers, except that a party or nonparty making the filing may include the following:

     (1) the acronym "SS#" where the individual's social-security number would have been included;
     (2) the acronym "TID#" where the individual's taxpayer-identification number would have been included;
     (3) the acronym "DL#" or "NDL#" where the individual's driver's license or non-driver's license identification card number would have been included;
     (4) the year of the individual's birth;
     (5) the minor's initials; and
     (6) the last four digits of the financial-account number.

2. Any information revealing the identity of an individual receiving mental-health services.

3. Any information revealing the identity of an individual receiving or under evaluation for substance-use-disorder services.

4. Information about protection orders, restraining orders, and injunctions that "would be likely to publicly reveal the identity or location of the protected party," 18 U.S.C. § 2265(d)(3) (prohibiting public disclosure on the internet of such information); *see also* 18 U.S.C. § 2266(5) (defining "protection order" to include, among other things, civil and criminal orders for the purpose of preventing violent or threatening acts, harassment, sexual violence, contact, communication, or proximity) (both provisions attached).

5. Any names of victims of sexual offenses except the brief may use initials when referring to victims of sexual offenses.

6. Any other information required by law to be kept confidential or protected from public disclosure.

/s/ Catherine M.A. Carroll
Signature

22-CV-0239
Case Number(s)

Catherine M.A. Carroll
Name

October 4, 2022
Date

catherine.carroll@wilmerhale.com
Email Address

ADDENDUM

ADDENDUM

TABLE OF CONTENTS

Title 18. Crimes and Criminal Procedure

Part I. Crimes

Chapter 121. Stored Wire and Electronic Communications and Transactional Records Access

18 U.S.C. § 2702

§ 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.--Except as provided in subsection (b) or (c)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.-- A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(7) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

[**(B)** Repealed. Pub.L. 108-21, Title V, § 508(b)(1)(A), Apr. 30, 2003, 117 Stat. 684]

(8) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency; or

(9) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(c) Exceptions for disclosure of customer records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

(1) as otherwise authorized in section 2703;

(2) with the lawful consent of the customer or subscriber;

(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(4) to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency;

(5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A;

(6) to any person other than a governmental entity; or

(7) to a foreign government pursuant to an order from a foreign government that is subject to an executive agreement that the Attorney General has determined and certified to Congress satisfies section 2523.

(d) Reporting of emergency disclosures.--On an annual basis, the Attorney General shall submit to the Committee on the Judiciary of the House of Representatives and the Committee on the Judiciary of the Senate a report containing--

(1) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (b)(8);

(2) a summary of the basis for disclosure in those instances where--

(A) voluntary disclosures under subsection (b)(8) were made to the Department of Justice; and

(B) the investigation pertaining to those disclosures was closed without the filing of criminal charges; and

(3) the number of accounts from which the Department of Justice has received voluntary disclosures under subsection (c)(4).

*** * ***

18 U.S.C. § 2703

§ 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.--
(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

> **(A)** without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction; or
>
> **(B)** with prior notice from the governmental entity to the subscriber or customer if the governmental entity--
>
> > **(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal** or State grand jury or trial subpoena; or
> >
> > **(ii)** obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure;

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

(h) Comity analysis and disclosure of information regarding legal process seeking contents of wire or electronic communication.--

(1) Definitions.--In this subsection--

(A) the term "qualifying foreign government" means a foreign government--

(i) with which the United States has an executive agreement that has entered into force under section 2523; and

(ii) the laws of which provide to electronic communication service providers and remote computing service providers substantive and procedural opportunities similar to those provided under paragraphs (2) and (5); and

(B) the term "United States person" has the meaning given the term in section 2523.

(2) Motions to quash or modify.--(A) A provider of electronic communication service to the public or remote computing service, including a foreign electronic communication service or remote computing service, that is being required to disclose pursuant to legal process issued under this section the contents of a wire or electronic communication of a subscriber or customer, may file a motion to modify or quash the legal process where the provider reasonably believes--

(i) that the customer or subscriber is not a United States person and does not reside in the United States; and

(ii) that the required disclosure would create a material risk that the provider would violate the laws of a qualifying foreign government.

Such a motion shall be filed not later than 14 days after the date on which the provider was served with the legal process, absent agreement with the government or permission from the court to extend the deadline based on an application made within the 14 days. The right to move to quash is without prejudice to any other grounds to move to quash or defenses thereto, but it shall be the sole basis for moving to quash on the grounds of a conflict of law related to a qualifying foreign government.

(B) Upon receipt of a motion filed pursuant to subparagraph (A), the court shall afford the governmental entity that applied for or issued the legal process under this section the opportunity to respond. The court may modify or quash the legal process, as appropriate, only if the court finds that--

(i) the required disclosure would cause the provider to violate the laws of a qualifying foreign government;

(ii) based on the totality of the circumstances, the interests of justice dictate that the legal process should be modified or quashed; and

(iii) the customer or subscriber is not a United States person and does not reside in the United States.

(3) Comity analysis.--For purposes of making a determination under paragraph (2)(B)(ii), the court shall take into account, as appropriate--

(A) the interests of the United States, including the investigative interests of the governmental entity seeking to require the disclosure;

(B) the interests of the qualifying foreign government in preventing any prohibited disclosure;

(C) the likelihood, extent, and nature of penalties to the provider or any employees of the provider as a result of inconsistent legal requirements imposed on the provider;

(D) the location and nationality of the subscriber or customer whose communications are being sought, if known, and the nature and extent of the subscriber or customer's connection to the United States, or if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the nature and extent of the subscriber or customer's connection to the foreign authority's country;

(E) the nature and extent of the provider's ties to and presence in the United States;

(F) the importance to the investigation of the information required to be disclosed;

(G) the likelihood of timely and effective access to the information required to be disclosed through means that would cause less serious negative consequences; and

(H) if the legal process has been sought on behalf of a foreign authority pursuant to section 3512, the investigative interests of the foreign authority making the request for assistance.

(4) Disclosure obligations during pendency of challenge.--A service provider shall preserve, but not be obligated to produce, information sought during the pendency of a motion brought under this subsection, unless the court finds that immediate production is necessary to prevent an adverse result identified in section 2705(a)(2).

(5) Disclosure to qualifying foreign government.--(A) It shall not constitute a violation of a protective order issued under section 2705 for a provider of electronic communication service to the public or remote computing service to disclose to the entity within a qualifying foreign government, designated in an executive agreement under section 2523, the fact of the existence of legal process issued under this section seeking the contents of a wire or electronic communication of a customer or subscriber who is a national or resident of the qualifying foreign government.

(B) Nothing in this paragraph shall be construed to modify or otherwise affect any other authority to make a motion to modify or quash a protective order issued under section 2705.

* * *

CERTIFICATE OF SERVICE

I hereby certify that on this 4th day of October, 2022, a copy of the foregoing brief has been served electronically, through the Appellate E-Filing system, upon Caroline Van Zile at caroline.vanzile@dc.gov.

/s/ Catherine M.A. Carroll

CATHERINE M.A. CARROLL
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
(202) 663-6000