No. 22-CV-0239

IN THE DISTRICT OF COLUMBIA COURT OF APPEALS

META PLATFORMS, INC.,

Petitioner,

v.

DISTRICT OF COLUMBIA,

Respondent.

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

APPELLANT'S REPLY BRIEF

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

December 19, 2022

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

Meta claims no immunity from investigation. It answered OAG's valid requests. Had OAG framed Request #2 to avoid implicating contents of communications and burdening protected expression, Meta would have answered it as well. Narrower options were readily available—*e.g.*, requesting aggregate data, de-identified information, or records specific to known "repeat offenders," to name a few. Instead, Request #2 demands a trove of granular details about the contents of user communications and Meta's exercise of editorial judgment in untold numbers of cases—effectively seeking to compile a database of identities of people who posted content that OAG disfavors and thinks Meta should have removed.

The Stored Communications Act (SCA) and First Amendment bar that request. Under § 2703 of the SCA, the government can compel disclosure of user contents "only" with a warrant. That requirement applies fully here and provides vital protection against unchecked government surveillance of people's online conversations—whether about COVID vaccines, elections, reproductive rights, or any other controversial topic the government might target for investigation. The First Amendment likewise forbids use of a sweeping subpoena that burdens the rights of both Meta and its users when far less intrusive means are available.

Having won below thanks to the Superior Court's rewriting of Request #2, OAG now raises new theories on appeal, ignores many of Meta's arguments while mischaracterizing others, and portrays Request #2 as if it sought nothing more than

inconsequential information about public communications. Those efforts fail. Request #2 is invalid, and the Superior Court erred in enforcing it.

ARGUMENT

I. REQUEST #2 VIOLATES THE SCA

To compel disclosure of stored communications, the government must satisfy § 2703. The SCA's text, structure, and history confirm that view. Meta Br. 21-29. And this Court has agreed that forced "[g]overnmental access" is subject to § 2703, not § 2702. *Facebook, Inc. v. Pepe*, 241 A.3d 248, 254 n.12 (D.C. 2020).

Leaving many of those points unaddressed, OAG claims for the first time on appeal that the SCA does not even apply here because Request #2 seeks public information. That argument is forfeited, and it is wrong. To the extent OAG defends the Superior Court's rationale that § 2702(b)'s consent exception excuses the government from complying with § 2703, that argument is equally unavailing.

A. OAG's Reliance On § 2511(2)(g)(i) Fails

Citing 18 U.S.C. § 2511(2)(g)(i), OAG mainly claims (at 23-27) the SCA "does not apply" because Request #2, as modified by the Superior Court, seeks only "public information." This argument is forfeited. OAG concedes (at 24 n.31) it never cited § 2511 below; nor did OAG ever dispute the SCA's applicability. OAG relied on the "publicly disclosed" nature of the communications at issue (*id.*) only in invoking § 2702's consent exception. OAG cites no "exceptional

circumstances" that would warrant considering the argument for the first time on appeal, and there are none. *Sewell v. Walker*, 278 A.3d 1175, 1177 (D.C. 2022).[1]

At any rate, OAG misreads the SCA. Section 2511(2)(g)(i) does not render the entire SCA inapplicable to public communications. It creates an exception to specific prohibitions the SCA (and Wiretap Act) would otherwise impose against unauthorized "access" or "interception." *See* 18 U.S.C. §§ 2511(1)(a), 2701. Because those prohibitions have no bearing here, neither does § 2511(2)(g)(i).

Section 2511(2)(g)(i) provides that "[i]t shall not be unlawful under [the Wiretap Act] or [the SCA] for any person … to *intercept* or *access* an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." (Emphasis added.) That plain text does not say the SCA "does not apply" to public communications, as OAG asserts, but simply exempts certain

[1] Indeed, there is ample reason not to entertain OAG's belated claim because Request #2 is not limited to "public" posts. As rewritten by the Superior Court, Request #2 covers public pages and "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. "[N]ominally private" posts are, "by definition, not accessible to the general public" under § 2511(2)(g)(i). *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 668 (D.N.J. 2013). If the user "took steps to limit access," *id.*—*e.g.*, by requiring a password or other conditions for access—the post is not "public" under § 2511(2)(g)(i), regardless of how many people are granted access, *e.g.*, *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1200 (9th Cir. 2022); *Ehling*, 961 F. Supp. 2d at 668 ("Privacy protection provided by the SCA does not depend on the number of Facebook friends a user has.").

communications from the prohibitions against "intercept[ion]" and "access" found in the Wiretap Act, 18 U.S.C. § 2511(1)(a), and the SCA, *id.* § 2701(a).

Statutory context and history confirm that § 2511(2)(g)(i) articulates a limitation specific to the SCA's statutory "access prohibition"—not the entire SCA. *Facebook, Inc. v. Superior Ct.*, 417 P.3d 725, 738 (Cal. 2018). When Congress enacted the Electronic Communications Privacy Act of 1986 ("ECPA"), which included the SCA, it updated the Wiretap Act to prohibit unauthorized "interception" of electronic communications and similarly protected electronic communications from unauthorized "access" while in storage. *See* S. Rep. No. 99-541, at 1, 13, 35-36 (1986) ("S. Rep."); H.R. Rep. No. 99-647, at 16, 62 (1986) ("H. Rep."). As amended, the Wiretap Act imposes liability on "any person" who "intercept[s]" an electronic communication without authorization, 18 U.S.C. § 2511(1)(a), while the SCA's § 2701 forbids anyone from "access[ing]" a communication in electronic storage without authorization.

Section 2701 addressed a "growing problem of unauthorized persons deliberately gaining access to, and sometimes tampering with," private communications. S. Rep. 35; *see* H. Rep. 62. It protects against "forms of electronic trespass," such as "'computer hack[ing].'" *Walker v. Coffey*, 956 F.3d 163, 167 (3d Cir. 2020). At the same time, Congress recognized that many nascent services, such as "electronic bulletin boards," were designed for the public to

communicate openly with others without restriction. S. Rep. 35-36; H. Rep. 62-63. To avoid stunting those services' growth, Congress adopted § 2511(2)(g)(i) to ensure § 2701's access prohibition (and the Wiretap Act interception analogue) would not reach services configured for public access. *Id.*

In doing so, Congress did not silently override the finely tuned rules it adopted in § 2703 to "limit[] the government's ability to compel providers to disclose their users' information." *Walker*, 956 F.3d at 167. Section 2511(2)(g)(i) has nothing to do with § 2703, which does not bar unauthorized "access"—*i.e.*, electronic trespass and hacking—but regulates compelled "disclosure" of user data to the government. *Id.*[2] In this case, for example, OAG does not seek to "access" Facebook posts by intruding on Meta's servers or logging in to visit users' Facebook pages; it seeks to compel Meta to disclose those posts. Because that request is not addressed by § 2701, the limitation in § 2511(2)(g)(i) is irrelevant.

The cases OAG cites (at 24-27) confirm OAG's error. Every case involves an alleged violation of § 2701. None suggests § 2511(2)(g)(i) alters the government's obligation to comply with § 2703 when it seeks to compel disclosure of communications. In *Ehling v. Monmouth-Ocean Hospital Services Corporation*, for example, the plaintiff sued her employer under § 2701 for

[2] Although § 2511(2)(g)(i) cross-references the SCA as a whole, *see* 18 U.S.C. § 2511(2)(g)(i) (referencing "chapter 121"), § 2701 is the only provision in the SCA that prohibits unauthorized "access" to stored electronic communications.

"improperly accessing" her Facebook post. 961 F. Supp. 2d 659, 665-667 (D.N.J. 2013). Contrary to OAG's characterization (at 26), the court did not say communications must be nonpublic to be protected in any way by the SCA; it said communications must be nonpublic to establish a violation of § 2701. *Id.* at 667.[3]

The legislative history OAG cites (at 25) also addresses § 2701—not § 2703 or the whole SCA. *See* S. Rep. 35-36 (discussing public facilities in relation to "[n]ew section 2701"); H. Rep. 62 (similar). No suggestion of any limitation to private content appears in the discussion of § 2703. S. Rep. 38-39; H. Rep. 67-69. And nothing in § 2703's text suggests its carefully calibrated procedures turn on the public or private nature of the communications. OAG's view would nullify § 2703 for huge swaths of content on social media. Had Congress intended such a vast exception to § 2703's intricate scheme, it surely would have said so expressly.

B. To Compel Disclosure, The Government Must Satisfy § 2703

Meta's opening brief showed at length (at 21-33) that a governmental entity can compel disclosure of communications only as provided in § 2703—regardless

---

[3] *See also Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1316, 1321 (11th Cir. 2006) ("[t]he provision at issue [is] § 2701(a)"); *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 969 (C.D. Cal. 2010) (motion to quash under § 2701); *Burke v. New Mexico*, 2018 WL 3054674, at *5 (D.N.M. June 20, 2018) (alleged violation of § 2701); *Facebook, Inc. v. Superior Court*, 417 P.3d at 739 (linking "focus[] on the public/private theme" to § 2701); *Combier v. Portelos*, 2018 WL 3302182, at *11, 13 (E.D.N.Y. July 5, 2018) (plaintiff claimed defendants "hacked" communications in violation of § 2701), *aff'd*, 788 F. App'x 774 (2d Cir. 2019).

of whether § 2702 would permit voluntary disclosure by the provider. OAG barely acknowledges most of Meta's arguments, much less rebuts them.

OAG instead says (at 28) this Court "already held" in *Pepe* that "a provider *must* comply with a subpoena if a Section 2702(b) exception applies." That misreads *Pepe*, which concerned a subpoena issued by a criminal defendant. Meta Br. 29-31. The Court stressed that distinction, emphasizing that "[g]overnmental access" is "addressed separately in § 2703." 241 A.3d at 254 n.12. OAG dismisses this distinction (at 31 n.34), noting *Pepe* "had no occasion to consider whether the government could compel production." But that is precisely the point. The Court understood that compelled disclosure to the government is addressed in § 2703 but was not at issue in the case before it, so the Court limited its holding accordingly. At the same time, the Court strongly signaled that the validity of legal process issued by the government is governed by § 2703. Meta Br. 30-31.

OAG nonetheless contends the Court should sweep § 2703 aside and simply follow the result in *Pepe* here despite the Court's reasoning and the crucial distinction between *Pepe* and this case. OAG's arguments are unpersuasive.

1. *Text and structure.* Section 2703 expressly states that a governmental entity may compel disclosure of contents of communications "only" pursuant to a warrant. 18 U.S.C. § 2703(a); Meta Br. 21-24. While acknowledging the import of that text, OAG asserts that this language "cannot possibly … mean[]" what it

says because many provisions in § 2702(b) "permit[] disclosure" to governmental entities and, as a result, § 2703 "cannot be the *sole* method by which the government can *obtain* information" under the SCA. OAG Br. 30 (second emphasis added). But in focusing on whether the government can "obtain" communications under § 2702, OAG repeats the Superior Court's error. Meta Br. 25. The issue is not whether OAG could "obtain" communications covered by a § 2702 exception if Meta voluntarily disclosed them; the issue is whether OAG can *compel* Meta to disclose them. *Id.* That question is answered by § 2703.

That § 2702(b)(2) permits voluntary disclosure "as otherwise authorized in" § 2703 supports Meta's analysis, not OAG's. *Cf.* OAG Br. 31. That provision confirms that the "authori[ty]" for legal process compelling disclosure must come from somewhere other than § 2702 itself. *Cf. Pepe*, 241 A.3d at 258 & n.30. And legal process that does not comply with § 2703 is not "authorized in" § 2703.

2. *Fourth Amendment.* The SCA's Fourth Amendment roots provide no basis to excuse OAG from complying with § 2703. *Cf.* OAG Br. 32-34.

To begin, OAG's blanket assertion that the Fourth Amendment "provides no protection to publicly available information" undervalues users' expectations of privacy. "A person does not surrender all Fourth Amendment protection by venturing into the public sphere." *Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018). Courts have "recognized the privacy interest inherent in the

nondisclosure of certain information even where the information may have been at one time public." *United States Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 767 (1989). A government rap sheet, for example, compiling a person's criminal history in one official dossier implicates substantial privacy interests even if each offense is a matter of public record. *Id.* at 762-771.[4]

Moreover, as new technologies and methods of surveillance evolve—"expand[ing] dramatically the opportunity" for "arbitrary use of Government power to maintain surveillance over citizens," S. Rep. 1-2—so do expectations of privacy even in information that is in some sense public, *Carpenter*, 138 S. Ct. at 2216-2220. A government demand compelling social-media platforms to create and provide databases of the identities of people who post content about controversial issues the government might wish to investigate—be it COVID, abortion, an election, and so on—raises obvious privacy implications, regardless of whether each individual post might have once been public.

Congress adopted the SCA's warrant requirement precisely because the existence of a reasonable expectation of privacy is "not always clear or obvious." S. Rep. 4 (brackets and quotation marks omitted). Given the state of case law at

---

[4] Moreover, Request #2 is not limited to content "'readily accessible to the general public.'" OAG Br. 33; *supra* note 2. Even when widely shared, posts "may be constitutionally protected" where the user applies more secure privacy settings. *United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012).

the time, Congress was concerned the Fourth Amendment alone might not offer "robust … protections … online." 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). Statutory protections would fill those gaps, resolve uncertainty, and guard against erosion of Fourth Amendment rights. S. Rep. 5.

The point of the SCA's warrant provision was thus to ensure a warrant would be required regardless of whether a court agreed the Fourth Amendment requires one. *See, e.g.*, *Graves v. Mahoning Cnty.*, 821 F.3d 772, 778 (6th Cir. 2016) ("Fourth Amendment … sets a national floor"; statutes "may (and frequently do) establish protections beyond that floor"); *United States v. Hammad*, 858 F.2d 834, 839 (2d Cir. 1988) (similar). OAG is not excused from complying merely because § 2703 might provide greater protections than the Fourth Amendment.

3. *Consequences*. It is not "absurd" to conclude the SCA imposes greater restrictions on the government's ability to compel disclosure than it imposes on private parties. OAG Br. 29-30. The plain text recites detailed restrictions unique to "governmental entit[ies]." 18 U.S.C. § 2703. Section 2702 likewise sets different rules for voluntary disclosures depending on whether disclosure is being made to the government. *Id.* § 2702(a)(3), (b)(8), (c)(4), (c)(6).

Legislative history confirms a different standard for the government is exactly what Congress intended. Congress set unique "[r]equirements for

governmental access," S. Rep. 38 (emphasis added), because the government's "enormous power … makes the potential consequences of its snooping far more ominous than those of … a private individual or firm." H. Rep. 19; *see* S. Rep. 1 (targeting "arbitrary use of Government power" to "surveil[] … citizens").

Finally, Meta's view does not "shield" ECS providers from investigation. *Cf.* OAG Br. 34. Meta complied with OAG's lawful requests, challenging only Request #2. Meta Br. 13. OAG has authority to investigate potential violations of the CPPA and other laws, and it could have requested relevant information without seeking contents of communications or users' identities. For example, OAG could have reframed Request #2 to reach only business records of aggregate data, such as the numbers of posts flagged for review, removed, or reviewed but not removed. As discussed below, such information would have given OAG all it needed to investigate Meta's content moderation. The SCA forecloses Request #2 only because OAG unnecessarily framed its request in a way that implicates contents of communications. The result is not immunity for service providers, but necessary protection for users. OAG's view would gut those protections—not only where the investigation targets a provider, but whenever the government targets Facebook users. Because it does not satisfy § 2703, Request #2 is unenforceable.[5]

[5] In another forfeited argument, OAG argues (at 36) for the first time that § 2703's warrant requirement does not apply because no "disclosure" occurs when

II. REQUEST #2 VIOLATES THE FIRST AMENDMENT

When a government investigative demand implicates protected expression, the First Amendment requires far more than the typical justification. *Cf.* OAG Br. 37 (citing *United States v. Morton Salt*, 338 U.S. 632 (1950)). Request #2 intrudes on Meta's and its users' First Amendment rights so it must meet exacting scrutiny. *See Americans for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2383 (2021) (plurality); *Buckley v. Valeo*, 424 U.S. 1, 64 (1976) (per curiam). Because OAG could achieve its goals through far less intrusive means, Request #2 fails that test.

A. Exacting Scrutiny Applies

1. Request #2 Burdens Meta's First Amendment Rights

OAG may investigate potentially unfair and deceptive practices, and Meta has cooperated with OAG's investigation here. But OAG must do so consistent with the First Amendment. OAG concedes (at 41) the First Amendment protects Meta's right to exercise editorial judgment over what content it publishes on the Facebook platform. And OAG does not dispute that an investigation intruding on

---

information has been previously disclosed. No authority supports this suggestion. *Cf. People v. Harris*, 949 N.Y.S.2d 590, 591, 596 (N.Y. Crim. Ct. 2012) (requiring warrant for "tweets that were publicly posted"). And it simply cannot be the case that anytime a user posts online, the SCA's disclosure prohibitions cease to apply. Such a rule would allow the government to obtain large swaths of content without a warrant regardless of whether a § 2702 exception applies. And redefining "disclosure" to reach only the very first disclosure would open a vast hole in other statutes that protect sensitive information from "disclosure," including FOIA, 5 U.S.C. § 552(a)(8)(A), and the Privacy Act, *id.* § 552a(b).

that right must meet exacting scrutiny. Request #2 presents such an intrusion.

An investigation triggers First Amendment scrutiny 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); Meta Br. 37. This is not a "heavy burden." OAG Br. 44. The test is objective, not subjective. *See Hartley v. Wilfert*, 918 F. Supp. 2d 45, 53 (D.D.C. 2013). Meta need not show its "speech was actually inhibited or suppressed." *Lacey v. Maricopa Cnty.*, 693 F.3d 896, 916 (9th Cir. 2012). Rather, the "*risk* of a chilling effect" is "enough 'because First Amendment freedoms need breathing space to survive.'" *Americans for Prosperity Found.*, 141 S. Ct. at 2389 (emphasis added).

OAG is wrong to suggest (at 21, 43) Meta's speech can be chilled only if OAG compels Meta to speak or directly restricts Meta's content moderation. Forcing Meta to disclose granular information about myriad specific content-moderation decisions threatens to chill Meta's exercise of editorial control—just as a subpoena demanding notes from an editorial board meeting would risk chilling a newspaper's editorial rights. Meta Br. 4, 47. The risk of chill is heightened because Request #2 purported to set a "continuing" obligation. App. 4. Knowing OAG has demanded information about content-moderation decisions and could take enforcement action if it concludes the decision was, *e.g.*, not sufficiently "aggressive," OAG Br. 10-11 nn.16-17 (quoting Meta statements), would lead any

person of "ordinary firmness" to feel chilled in their editorial decisions.

This is why courts have held that compelled production of information concerning a publisher's "editorial judgment[s]" would be "an obvious intrusion on the protections of the editorial function guaranteed by the First Amendment." *Maughan v. NL Industries*, 524 F. Supp. 93, 95 (D.D.C. 1981) (compelling production of reporter's notebook would intrude on "editorial processes"); *see also, e.g.*, *Robertson v. People Mag.*, 2015 WL 9077111, at *2-3 (S.D.N.Y. Dec. 16, 2015) (quashing request for "access to People's editorial files, including all documents covering the mental process of People staff concerning what would or would not be published in the magazine"); *Palandjian v. Pahlavi*, 103 F.R.D. 410, 412 (D.D.C. 1984) (quashing subpoena for reporters' notes as intruding on "editorial processes"); *United States v. Cuthbertson*, 630 F.2d 139, 147 (3d Cir. 1980) (First Amendment "prevent[s] intrusion" into "editorial process"). OAG's position cannot be squared with this case law.

That chill is not diminished just because OAG is investigating statements about content moderation rather than content-moderation decisions themselves. *Cf.* OAG Br. 39, 44. Even a legitimate inquiry "cannot be pursued by means that broadly stifle fundamental personal liberties." *Shelton v. Tucker*, 364 U.S. 479, 488 (1960). And here, it is OAG's "means"—demanding granular information about a huge number of moderation decisions so it can judge whether such

decisions were correct—that intrudes on Meta's rights.[6] Moreover, investigating the statements at issue here necessarily second-guesses Meta's decisions. A statement that Meta intends to take "aggressive" action, for example, cannot be false unless OAG concludes a truly "aggressive" moderator would have made a different editorial decision. OAG thus admits (at 49) it seeks to determine whether Meta "failed or refused" to remove or demote content.

The First Amendment burden exists regardless of whether OAG is acting in "bad faith" or for a "retaliatory motive." OAG Br. 40-41, 44. To be clear, Meta has never claimed bad faith or challenged Request #2 on these bases. But the cases OAG cites (at 40-41) regarding "bad faith" are inapposite. They all involve a bad-faith exception to the standard test for enforcing a run-of-the-mill investigatory subpoena.[7] None involve any impact on First Amendment rights. *See FEC v. Machinists Non-Partisan Pol. League*, 655 F.2d 380, 389 (D.C. Cir. 1981)

---

[6] The Ninth Circuit did not hold otherwise in *Twitter, Inc. v. Paxton*, in which Twitter challenged a document demand before enforcement. The Ninth Circuit has reconsidered the opinion cited by OAG (at 39, 44). *See* 2022 WL 17682769, at *3 (9th Cir. Dec. 14, 2022). Its new opinion emphasizes that Twitter "can raise its First Amendment defense if [the Attorney General] moves to enforce" his demand, *id.* at *6 & n.2—precisely as Meta does here. And unlike the "vague" and "indefinite" allegations the Ninth Circuit deemed insufficient, Meta here challenges "the chilling effect of the specific investigation at hand," *id.* at *4-5, by objecting to the intrusive information demanded in Request #2.

[7] *See United States v. LaSalle Nat'l Bank*, 437 U.S. 298 (1978) (no First Amendment issue); *Ngo v. United States*, 699 F. App'x 617 (9th Cir. 2017) (same); *NLRB v. American Med. Response, Inc.*, 438 F.3d 188, 192 (2d Cir. 2006) (same).

(rejecting application of *Morton Salt* in light of First Amendment concerns).

2. Request #2 Burdens Meta's Users' First Amendment Rights

OAG likewise errs in disputing the chilling effect on Meta's users of disclosing a list of speakers to the government whose speech OAG disfavors.

To start, OAG overstates the standard for establishing an intrusion on Meta's users' First Amendment rights. Meta was not required to present "evidence" that users actually faced threats in the past or that enforcing Request #2 "would" surely result in threats or harassment in the future. *Cf.* OAG Br. 45-46. A party asserting the right to speak need show only that the challenged conduct is "likely [to] deter a person of ordinary firmness from the exercise of First Amendment rights." *Benham*, 635 F.3d at 135. OAG's cited cases agree that a party challenging compelled disclosure "need show only a reasonable probability that the compelled disclosure ... will subject [contributors] to threats, harassment, or reprisals," or "other consequences which objectively suggest an impact on, or 'chilling' of, the members'" First Amendment rights. *Brock v. Local 375, Plumbers Int'l Union of Am.*, 860 F.2d 346, 350 & n.1 (9th Cir. 1988) (rejecting "'unduly strict requirements of proof'"); *see also In re Motor Fuel Temperature Sales Practices Litig.*, 641 F.3d 470, 491 (10th Cir. 2011) (disclaiming any "bright-line rule

delineating the minimum proof necessary").[8]

OAG is wrong (at 46-47) that compelling Meta to hand over a list of speakers whose speech the government disfavors raises no First Amendment concerns. As Meta explained (at 48-49), even a user who did not conceal her identity would face a chill from having her identity turned over to the government. *See Hartley*, 918 F. Supp. 2d at 54 (placing a person protesting in public on a Secret Service list of "crazies … in front of the White House" would chill a person of "ordinary firmness"). That is particularly true here because the Superior Court ordered Meta to disclose not only users who posted publicly but also those who posted in "private groups" to which OAG might not have access. App. 26; *supra* p. 3. As the Supreme Court recently reaffirmed, "*each* government demand for disclosure brings with it an *additional* risk of chill." *Americans for Prosperity*, 141 S. Ct. at 2389 (emphasis added). If speaking could land a person on a government

[8] OAG does not dispute Request #2 as written required Meta to unmask anonymous users. Request #2 demands information "sufficient to identify … the identity of any individuals or entities" who violated misinformation policies. App. 9. OAG now abandons (at 47-48) that demand in light of the Superior Court's indication that Meta should produce "only the identities that these users themselves employed in their public posts." App. 31. But as discussed, *supra* p. 3, even as rewritten, Request #2 threatens to chill protected speech by disclosing users to the government who identified themselves only to "private groups." App. 26. And to the extent OAG were to seek information beyond the name in a user's profile, such unmasking would alone trigger First Amendment scrutiny because an "'author's decision to remain anonymous'" is itself "'an aspect of the freedom of speech protected by the First Amendment.'" *Solers, Inc. v. Doe*, 977 A.2d 941, 951 (D.C. 2009) (quoting *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995)).

blacklist of people associated with content the government disfavors, then any user of "ordinary firmness" would be less likely to speak.

B. Request #2 Fails Exacting Scrutiny

OAG makes little attempt to pass exacting scrutiny. OAG in no way satisfies its burden to identify the statements it is investigating, establish that each statement is potentially actionable, and show that Request #2 sweeps up no more information than needed to determine whether the statements were false or misleading. Meta Br. 41-46; *see also Solers, Inc. v. Doe*, 977 A.2d 941, 955 (D.C. 2009) (plaintiff seeking to unmask defamation defendant had to "set forth as precisely as possible the statements," show that each supports a "viable" claim, and ensure the "information sought is important to the litigation").

OAG's asserted need for the identities of every user associated with any violation of COVID-19 vaccine-related misinformation policies is inadequate. If OAG is investigating only Meta, not its users, then de-identified information should suffice. Meta Br. 44-45. OAG's sole answer (at 50) is that it needs identifying information to assess how Meta addresses "repeat offenders" and those "publicly identified as responsible" for misinformation. But OAG ignores the mismatch between that explanation and the scope of Request #2. Meta explained (at 44), for example, that OAG has never identified any statement by Meta that could be rendered false or misleading based on Meta's treatment of "repeat

offenders." In response, OAG still identifies nothing. Nor could it. The statements OAG says it is investigating reflect Meta's assertion that it "may" take actions against repeat offenders; no amount of identifying information about users and the contents of their posts could make such statements actionably false.[9]

Moreover, to the extent any group, page, or account repeatedly violated Meta's misinformation policies, a unique but de-identified code would link those repeat violations together, allowing OAG to evaluate Meta's response. *See Lubin v. Agora, Inc*., 882 A.2d 833, 847 (Md. 2005) (rejecting "fishing expedition" for identifiable subscriber information). OAG also fails to explain why records for a far smaller subset of users would not suffice. If OAG believes (at 50) Meta failed to act against particular "publicly identified" users and can tie that failure to some potentially actionable statement, then it should ask for information about only those users.[10] None of OAG's explanations justify demanding identifying information for all of the thousands or possibly millions of users who Meta

---

[9] *See, e.g.*, Rosen, *An Update on Our Work to Keep People Informed and Limit Misinformation About COVID-19*, Meta (Apr. 16, 2020) (those that "repeatedly share these debunked claims *may* be removed altogether" (emphasis added), https://tinyurl.com/yck624s9), cited at OAG Br. 11 & n.20. OAG does not claim that it is investigating repeat offenders based on Meta's statements about enforcing its rules "aggressively" and the like. Nor could it, given that such statements are non-actionable puffery. Meta Br. 42-44.

[10] Similarly, if OAG means to test the truthfulness of Meta's statement that it had "removed over 3,000 accounts, pages, and groups for repeat violations," OAG Br. 11, OAG would need information only for those 3,000 accounts, and de-identified information should suffice.

determined violated its COVID-19 policy.

OAG fares no better in explaining why it needs even de-identified information about every violation Meta identified. OAG concedes (at 11-12) Meta has made no statements quantifying "how much COVID-19 vaccine misinformation it has removed or demoted," and OAG identifies no other reason it would need such granular information. Investigating whether Meta has "knowingly failed or refused" to restrict certain content, OAG Br. 49, likewise does not justify OAG's sweeping demands. If OAG could identify statements by Meta unequivocally pledging to always remove certain misinformation, then OAG could request de-identified information about Meta's non-removal of content in that category. But OAG identifies no such statements, and it nowhere explains what it could possibly learn about Meta's supposed refusal to enforce its rules from information about the occasions on which Meta did restrict misinformation.

Because Request #2 thus is not "narrowly tailored to the government's asserted interest," it fails to satisfy exacting scrutiny. *Americans for Prosperity Foundation*, 141 S. Ct. at 2383.

CONCLUSION

The Superior Court's order should be reversed.

Respectfully submitted,

/s/ Catherine M.A. Carroll

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

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

December 19, 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 20 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

December 19, 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

December 19, 2022
Date

catherine.carroll@wilmerhale.com
Email Address

CERTIFICATE OF SERVICE

I hereby certify that on this 19th day of December, 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