No. 22-CV-239

IN THE DISTRICT OF COLUMBIA COURT OF APPEALS

META PLATFORMS, INC.,
APPELLANT,

V.

DISTRICT OF COLUMBIA,
APPELLEE.

ON APPEAL FROM AN ORDER OF THE
SUPERIOR COURT OF THE DISTRICT OF COLUMBIA

BRIEF FOR APPELLEE THE DISTRICT OF COLUMBIA

KARL A. RACINE
Attorney General for the District of Columbia

CAROLINE S. VAN ZILE
Solicitor General

ASHWIN P. PHATAK
Principal Deputy Solicitor General

*STACY L. ANDERSON
Senior Assistant Attorney General
Office of the Solicitor General

Office of the Attorney General
400 6th Street, NW, Suite 8100
Washington, D.C. 20001
(202) 724-6625
stacy.anderson2@dc.gov

*Counsel expected to argue

TABLE OF CONTENTS

TABLE OF AUTHORITIES*

Cases

---

* Authorities upon which we chiefly rely are marked with asterisks.

Statutes

INTRODUCTION

Meta Platforms, Inc., formerly known as Facebook, Inc. ("Facebook"), appeals a Superior Court order granting the motion of the Office of the Attorney General ("OAG") to enforce an administrative subpoena. The subpoena arises from OAG's investigation into whether Facebook's well-publicized representations to consumers about its efforts to stem COVID-19 vaccine misinformation on its platform deceived its users. Deceptive representations to consumers are a classic violation of the D.C. Consumer Protection Procedures Act ("CPPA"), D.C. Code § 28-3901 *et seq.*, which OAG routinely enforces. To understand whether Facebook has complied with this Act, OAG sought information about Facebook groups, pages, and accounts that had violated Facebook's COVID-19 vaccine misinformation policy; nature of the violations; and Facebook's response. Appellant's Appendix ("App.") 4-5. The Superior Court enforced the subpoena, and it ordered Facebook to produce only content posted publicly and accessible to everyone. App. 25-27.

Facebook challenges OAG's subpoena as a violation of the Stored Communications Act ("SCA"), 18 U.S.C. § 2701, *et seq*., and the First Amendment. Neither contention has merit. The Superior Court's order does not implicate the SCA because that Act protects only *private* information, which the subpoenaed information plainly is not. Even if the Act did apply, the Superior Court correctly recognized that OAG could compel public information under the Section 2702(b)(3)

user-consent exception, which Facebook agrees applies to the public posts here. That reading comports with the SCA's text, which does not require the government to get a warrant every time it seeks content stored electronically. A contrary conclusion would undermine Congress's intent to extend Fourth Amendment protections—which apply only to private information—to the digital sphere. And it would lead to an absurd result, requiring the government to get a warrant for information that a private party could subpoena under a Section 2702(b) exception.

Facebook's First Amendment concerns are even more far-fetched. Facebook posits that OAG's investigation is intended to control Facebook's content moderation and to target Facebook users' disfavored speech. No fair reading of the subpoena suggests such bad-faith motivation. Rather, OAG is simply investigating whether Facebook's commercial speech is deceptive—that is, whether it is complying with its *own* claims to consumers about its vaccine-misinformation policies. Similarly, OAG is not targeting Facebook users, nor will its investigation have a chilling effect on their speech, for the simple reason that the posts at issue are *already public*, and no anonymous users will be unmasked. For those reasons, OAG's subpoena is not subject to "exacting scrutiny." But even if were, it would survive: OAG has a significant interest in consumer protection and its request for information bears a substantial relationship to this interest—indeed, it is the only

way that OAG can ensure Facebook's compliance with the CPPA. This Court should affirm.

STATEMENT OF THE ISSUES

1. Whether the Superior Court's enforcement of OAG's administrative subpoena against Facebook violated the SCA.

2. Whether the Superior Court's enforcement of OAG's administrative subpoena against Facebook violated the First Amendment.

STATEMENT OF THE CASE

In June 2021, OAG issued Facebook a subpoena for documents related to OAG's CPPA investigation. App. 1-5. When Facebook objected to producing some information as barred by the SCA, OAG petitioned the Superior Court to enforce its subpoena in November 2021. App. 7-12. The Superior Court granted the petition on March 9, 2022. App. 13-36. Facebook timely moved for reconsideration on April 6, and it filed a timely, protective notice of appeal on April 8. App. 37-40. The Superior Court denied Facebook's motion for reconsideration on May 23. App. 41-42. In July, with the District's consent, the Superior Court stayed its order pending the outcome of this expedited appeal. App. 43.

STATEMENT OF FACTS

1. The Stored Communications Act.

Three years before the advent of the World Wide Web in 1989, and two decades before Facebook widely launched in 2006, Congress passed the Electronic

Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848. In Title II, Congress adopted the SCA to address access to stored electronic communications and related records. 100 Stat. at 1860-68; S. Rep. No. 99-541 ("S. Rep."), at 3 (1986).

The purpose of the Act was to extend Fourth Amendment-like protections to private communications taking place through new technological mediums. S. Rep. 5; *see* H.R. Rep. No. 99-647 ("H.R. Rep."), at 19 (1986); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1214 (2004). This was necessary because "[h]istorically, the Fourth Amendment ha[d] not protected personal information revealed to third parties," like electronic communication providers. *Walker v. Coffey*, 956 F.3d 163, 166 (3d Cir. 2020); *see* S. Rep. 3. "To address this vulnerability, Congress crafted the SCA to protect information held by centralized communication providers." *Walker*, 956 F.3d at 167. In doing so, Congress sought to strike a balance between the "privacy expectations of American citizens and the legitimate needs of law enforcement." S. Rep. 5.

Although social media platforms like Facebook did not exist when Congress enacted the SCA, Congress did consider the law's impact on a precursor—electronic bulletin boards, which it defined as "communications networks created by computer users for the transfer of information among computers." *Id*. at 8. It explained that

these systems "may require special 'passwords' which restrict entry to the system," but may also "be public or semi-public . . . depending on the degree of privacy sought by users, operators or organizers." *Id*. at 9.

Congress did not intend to "hinder the development or use of 'electronic bulletin boards' or other similar services where . . . the readily accessible nature of the service [is] widely known and the service does not require any special access code or warning to indicate that the information is private." *Id*. at 36. In Congress's view, "[t]o access a communication in such a public system is not a violation of the [SCA], since the general public has been 'authorized' to do so." *Id*.; *see* H.R. Rep. 62. Thus, Congress provided that "[i]t shall not be unlawful under . . . [the SCA] for any person . . . to . . . 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." 18 U.S.C. § 2511(2)(g)(i).[1]

As for private stored communications, the SCA prohibits "a person or entity providing an electronic communication service to the public" to "knowingly divulge to any person or entity the contents of a communication while in electronic storage

[1] A communication is readily accessible to the public if the means of access are widely known and if a person encounters no warnings, encryptions, password requests, or other indicia of privacy when accessing the content. H.R. Rep. 62.

by that service." 18 U.S.C. § 2702(a)(1).[2] It imposes civil liability on providers that violate this provision. *Id*. § 2707(a). But there are many exceptions to the non-disclosure prohibition. Section 2702(b) identifies nine instances when "[a] provider . . . may divulge the contents of a communication" without violating the SCA. As relevant here, those exceptions include disclosures:

> (1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;[3]
>
> (2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of 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] . . .
>
> (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--

---

[2] An "electronic communication service" provides users with "the ability to send or receive . . . electronic communications." 18 U.S.C. § 2510(15). Facebook is such a service. The "content" of a communication is "any information concerning the substance, purport, or meaning of" the communication. *Id*. § 2510(8).

[3] "A person may be an 'intended recipient' of a communication . . . even if he is not individually identified by name or otherwise." H.R. Rep. 67. "[T]he service provider would not be liable for disclosure to any person who might reasonably be considered to fall in the class of intended recipients." *Id.*

[4] "[A] subscriber who places a communication on a computer 'electronic bulletin board,' with a reasonable basis for knowing that such communications are freely made available to the public, should be considered to have given consent to the disclosure or use of the information." H.R. Rep. 66.

> (i) were inadvertently obtained by the service provider; and
>
> (ii) appear to pertain to the commission of a crime; or
>
> (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.

Id. § 2702(b).

The SCA separately provides in Section 2703 that a "governmental entity may require the disclosure" by a service provider "of the contents of a[n] electronic communication . . . only pursuant to a warrant." *Id*. § 2703(a). With the warrant requirement, Congress intended to protect stored communications consistent with protections that the Fourth Amendment otherwise affords private information, like letters or papers in a home. *See* H.R. Rep. 22, 68 ("The 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."); *Vista Mktg., LLC v. Burkett*, 812 F.3d 954, 970 (11th Cir. 2016). The warrant requirement applies only to content that is in electronic storage for 180 days or less. 18 U.S.C. § 2703(a). For content held longer, the government may obtain content with a warrant or, after providing notice to the user, with an administrative subpoena or court order based on "specific and articulable facts showing . . . that the contents . . . are relevant and material to an ongoing criminal investigation." *Id*. § 2703(a), (d).

A provider may disclose consumer *records*—not contents—under Section 2702(c) in several scenarios: in response to a warrant, with user consent, as needed to provide services, to a governmental entity upon a dangerous emergency, in a report to the National Center for Missing and Exploited Children, to anyone other than a governmental entity, or under an approved order of a foreign government. Section 2703(c)(1) provides that a "governmental entity may require a provider . . . to disclose a record or other information pertaining to a subscriber . . . only when the governmental entity" secures a warrant, obtains a court order in certain circumstances, has the consent of the subscriber, seeks information as part of a telemarketing fraud investigation, or seeks limited information under subsection (c)(2). *Id*. § 2703(c)(1). Subsection 2703(c)(2) requires an electronic communication service provider to disclose basic subscriber information in response to an administrative subpoena. *Id*. § 2703(c)(2).

2. Facebook And COVID-19 Vaccine Misinformation.

Facebook operates a website and a companion mobile application that allow consumers to communicate and share content on its platform.[5] To begin using Facebook, a consumer first creates an account.[6] The consumer can then add other

---

[5] *What are the Meta Products?*, Help Ctr., https://tinyurl.com/3ha98brt (last visited Oct. 31, 2022).

[6] *Creating an Account*, Help Ctr., https://tinyurl.com/urvdawnh (last visited Oct. 31, 2022).

Facebook users as "friends," join (or form) public or private "groups," "tag" other users, and "like" public "pages."[7] In this process, consumers are exposed to content from other accounts, groups, and pages.[8]

Facebook users control who sees the content they post by choosing their "audience."[9] When a consumer elects to "share something with Public that means anyone including people off of Facebook can see it."[10] In addition, when the user shares private information with friends, those friends can choose to make it public or share it with others who can make it public.[11] Likewise, a Facebook user's comments made on another user's public post become public.[12] And Facebook Pages and public groups are public spaces where anyone who can see the Page or the group can see the consumer's posts and comments.[13]

---

[7] *Friending*, Help Ctr., https://tinyurl.com/mpccjpdx (last visited Oct. 31, 2022); *Join and Choose Your Settings*, Help Ctr., https://tinyurl.com/45yvsmzr (last visited Oct. 31, 2022); *Tagging*, Help Ctr., https://tinyurl.com/y25xt4c3 (last visited Oct. 31, 2022); *Interact with Pages*, Help Ctr., https://tinyurl.com/mtjpj52f (last visited Nov. 15, 2022).

[8] *Your Home Page*, Help Ctr., https://tinyurl.com/ycx5bny6 (last visited Oct. 31, 2022).

[9] *Select your audience on Facebook*, Help Ctr., https://tinyurl.com/349fvy4m (last visited Oct. 31, 2022).

[10] *Id*.

[11] *Control who can see what you share on Facebook, What is public information on Facebook?*, Help Ctr., https://tinyurl.com/3uuvw5tv (last visited Oct. 31, 2022).

[12] *Id*.

[13] *Id*.

Facebook is unique among social media platforms in prohibiting anonymous users. Instead, it requires users to "[u]se[] the name they go by in everyday life" on the platform.[14] Facebook's terms notify users that it may share their information in response to a legal request, like a subpoena.[15]

Since the beginning of the COVID-19 pandemic, Facebook has routinely made public statements about addressing COVID-19-related misinformation on its platforms. In April 2020, Facebook publicly committed to preventing the spread of COVID-19 misinformation and in May announced that it had placed warning labels on around 50 million pieces of false COVID-19-related content.[16] In December 2020, Facebook announced that it would be "removing" false claims about COVID-19 vaccines.[17] In February 2021, Facebook expanded its list of types of COVID-19

---

[14] *Names allowed on Facebook*, Help Ctr., https://tinyurl.com/y9dpn5d2 (last visited Oct. 31, 2022).

[15] *How do we respond to legal requests, comply with applicable law, and prevent harm?*, Privacy Ctr., https://tinyurl.com/yspt3hkp (last visited Nov. 3, 2022).

[16] Guy Rosen, *An Update on Our Work to Keep People Informed and Limit Misinformation About COVID-19*, Meta (Apr. 16, 2020), https://tinyurl.com/yck624s9; *id*. (May 12, 2020 update); *see* Nick Clegg, *Combating COVID-19 Misinformation Across Our Apps*, Meta (Mar. 25, 2020), https://tinyurl.com/y87hv7hz ("we've been . . . taking aggressive steps to stop misinformation and harmful content from spreading").

[17] Kang-Xing Jin, *Keeping People Safe and Informed About the Coronavirus*, Meta (Dec. 18, 2020), https://tinyurl.com/5yx9ew47 ("For example, we will remove false claims that COVID-19 vaccines contain microchips, or anything else that isn't

vaccine misinformation that it would remove and committed to "immediately" enforcing this policy change, "with a particular focus on Pages, groups, and accounts that violate these rules."[18] In the spring of 2021, Facebook enacted what it called "break the glass" measures to "demote the news feed ranking" of content that was sensationalist, alarmist, or that indirectly discouraged vaccines.[19] In August 2021, Facebook announced that it had removed 20 million items of content that violated its COVID-19 misinformation policies, removed over 3,000 accounts, pages, and groups for repeat violations, and displayed warnings on over 190 million pieces of COVID-related content for being "false, partly false, altered or missing context."[20]

---

on the official vaccine ingredient list. We will also remove conspiracy theories about COVID-19 vaccines that we know today are false."); Guy Rosen, *An Update on Our Work*, *supra* n.16 (Feb. 8, 2021 update) ("Since December, we've removed false claims about COVID-19 vaccines . . . . These new policies will help us continue to take aggressive action against misinformation about COVID-19 and vaccines. We will begin enforcing this policy immediately."); *see* Guy Rosen, *How We're Tackling Misinformation Across Our Apps*, Meta (Mar. 22, 2021), https://tinyurl.com/3cdyyw7n ("For the most serious kinds of misinformation, such as false claims about COVID-19 and vaccines . . . we will remove the content.").

[18] Guy Rosen, *An Update on Our Work*, *supra* n.16 (Feb. 8, 2021 update) (expanding Facebook's list of prohibited false claims); *see COVID-19 and Vaccine Policy Updates & Protections*, Help Ctr., https://tinyurl.com/mrk3hsnn (last visited Oct. 31, 2022) ("[W]e remove misinformation . . . that . . . is false. . . . [W]e remove false information about . . . COVID-19 vaccines that contribute to vaccine rejection."); Br. 10.

[19] Sam Schechner, Jeff Jorowitz & Emily Glazer, *How Facebook Hobbled Mark Zuckerberg's Bid to Get America Vaccinated*, Wall St. J. (Sept. 17, 2021), https://tinyurl.com/44tbm2d7.

[20] Guy Rosen, *Community Standards Enforcement Report, Second Quarter 2021*, Meta (Aug. 18, 2021), https://tinyurl.com/yc7wcuuu.

It has not, however, said how much COVID-19 vaccine misinformation it has removed or demoted, maintaining here that it does not know. Br. 13 n.15 (asserting that it "does not separately track COVID-19 misinformation specific to vaccines").

Despite its public pledges to remove and demote COVID-19 vaccine misinformation, Facebook's staff internally continued to report the proliferation of COVID-19 vaccine misinformation on the platform. Internal memos in early 2021 found that over two-thirds of sampled comments about COVID-19 and vaccines were anti-vaccination—a figure that staffers noted was much higher than the rate of anti-vaccine sentiment among the general U.S. population.[21] One staffer circulated a memo about an anti-vaccine Facebook post that had been viewed over three million times and reshared 53,000 times without being demoted or removed.[22] The staffer described the post's circulation, which said that vaccines "are all experimental & you are in the experiment," as "a bad miss for misinfo."[23] A July 2021 report by an advocacy group found that Facebook's "related pages" algorithm appeared to be accelerating COVID-19 vaccine misinformation by recommending pages that

---

21 Schechner, Jorowitz, & Glazer, *supra* n.19.

22 *Id*.

23 *Id*.

promoted misleading content to users.[24] In the same month, the Washington Post reported that anti-vaccination content was "still common" on Facebook, citing a study that identified hundreds of public and private anti-vaccine groups with hundreds of thousands of followers combined.[25] Internal Facebook memos suggested that anti-vaccine activists "used Facebook's own tools to sow doubt" about vaccine safety.[26] Another internal document found that "a relatively few number of actors" created a "large percentage of the content and growth" of COVID-19 vaccine misinformation on Facebook's platform.[27] The proliferation of vaccine misinformation on Facebook continues, despite its pledges to consumers about acting on its content removal and demotion policies.[28]

---

[24] Avaaz, *A Shot in the Dark: Researchers peer under the lid of Facebook's "black box," uncovering how its algorithm accelerates anti-vaccine content* (July 21, 2021), https://tinyurl.com/3urx84x4.

[25] Gerrit De Vynck & Rachel Lerman, *Facebook and YouTube spent a year fighting covid misinformation. It's still spreading.*, Wash. Post (July 22, 2021), https://tinyurl.com/3rajzn64.

[26] Schechner, Jorowitz & Glazer, *supra* n.19.

[27] *Id*.

[28] *See*, *e.g.*, Fergal Gallagher, *Facebook 'failing' to tackle COVID-19 misinformation posted by prominent anti-vaccine group, study claims*, ABC News (Dec. 3, 2021), https://tinyurl.com/bdf7j2pu; Daniel Zuidijk, *Emoji Help Anti-Vaccine Posts Avoid Moderation on Facebook*, Bloomberg, Oct. 19, 2022, https://tinyurl.com/yse8d9w8.

3. OAG's Investigation And Its Administrative Subpoena.

The CPPA grants OAG authority to file an action against any person who it has reason to believe is violating the CPPA or other consumer protection laws. D.C. Code § 28-3909(a). The CPPA prohibits unfair or deceptive trade practices. *Id.* § 28-3904. OAG has statutory authority to conduct "investigation[s] to determine whether to seek relief under [the CPPA]," *id.* § 28-3910, and it may issue subpoenas for the production of records as part of those investigations, *see id.* § 1-301.88d(a).

OAG is investigating whether Facebook has violated the CPPA by making unfair or deceptive statements to consumers about its efforts to reduce and remove COVID-19 vaccine misinformation on its social media platform—statements apparently made to curry public favor and quell scrutiny from its consumers. *See* App. 1. OAG requested that Facebook provide information about the sources of COVID-19-related misinformation on its platform, a request that Facebook refused. Thus, OAG issued a subpoena under D.C. Code § 28-3910. At issue is the subpoena's Request for Production No. 2 which seeks:

> Documents sufficient to identify all Facebook groups, pages, and accounts that have violated Facebook's COVID-19 misinformation policy with respect to content concerning vaccines, including the identi[t]y of any individuals or entities associated with the groups, pages, and accounts; the nature of the violation(s); and the consequences imposed by Facebook for the violation, including whether content was removed or banned from these sources.

App. 4-5.

4. OAG's Enforcement Action And The Superior Court's Decision.

Facebook declined to comply with OAG's subpoena on the asserted ground that the SCA required the District to seek a warrant, and OAG therefore brought an enforcement action in the Superior Court. App. 7-12. The Superior Court granted the petition for enforcement to the extent that it sought public content, concluding that OAG's request for "public posts is a reasonable and lawful exercise of the District's subpoena power and that it is consistent with the [SCA] and with the First Amendment." App. 13; *see* App. 17.[29]

With regard to the SCA, the Superior Court first found that the information that the District sought included the "content" of Facebook posts that were in electronic storage. App. 18-21. Because the District sought the identity of users who Facebook had determined provided false vaccine information, identifying them necessarily disclosed the content of their communications—misinformation about vaccines. App. 19-21. The Superior Court also found that Facebook posts, including the subset removed by Facebook but maintained on its servers, are in electronic storage for "backup protection" under 18 U.S.C. § 2510(17)(B). App. 21.

---

[29] The District defined "public posts" to include posts to "pages" or to "public" groups visible to the public no matter if the viewer has a Facebook account, and posts to nominally "private" groups which either have so many members that they are functionally public or otherwise reflected an intent to reach the public. OAG's Mem. in Support of Pet. for Enforcement 12 n.22 (filed Nov. 30, 2021).

Nevertheless, the Superior Court concluded that the user-consent exception to the SCA's protections in Section 2702(b)(3) covered publicly posted information on Facebook. App. 21-27. The court rejected Facebook's argument that the government could not obtain information by subpoena with the consent of a Facebook consumer. App. 21-24. It explained that nothing in the text of the SCA limits the consent exception to disclosures to non-governmental entities. App. 22. And it found that the warrant authorized by Section 2703 was not the exclusive way that the government could obtain information, given that Section 2702 authorizes disclosures to governmental entities without a search warrant. App. 23.

The court also noted that Facebook did "not suggest any reason why Congress would have prevented disclosure of content to government agencies with user consent," concluding that the SCA could not "reasonably be interpreted to prohibit [Facebook] from honoring this explicit authorization." App. 23. The court cited *Facebook, Inc. v. Pepe*, 241 A.3d 248 (D.C. 2020), where this Court upheld a subpoena from a criminal defendant that fit within a Section 2702 exception. Given that precedent, the Superior Court concluded that because Section 2702(b)(3) permitted Facebook to disclose the information OAG sought, Facebook could not refuse to comply with the otherwise valid subpoena. App. 23-24.

As for whether those who made public posts had consented to their release to OAG, the court found that they had implicitly done so. App. 24-27. Recognizing

that Congress intended the SCA to protect private, not public, information, the court held that "when a user posts content on Facebook that is generally accessible to the public, the user implicitly consents to disclosure." App. 25.[30]

As for Facebook's First Amendment arguments, regarding Facebook's assertion of its own First Amendment rights, the Superior Court rejected Facebook's suggestion that the District's subpoena infringed on its right to make content-moderation decisions. App. 27. Facebook did "not suggest that compliance with the subpoena would in fact inhibit it from exercising its right to control its content moderation policies." App. 28 n.4. Instead, the court found that Facebook's compliance with the subpoena would have "no effect whatsoever" on its content moderation or enforcement, nor would compliance require it to publish any preferred message. App. 27.

The Superior Court also rejected Facebook's First Amendment argument on behalf of its user, including the accusation that OAG was trying to target and unmask private citizens based on the District's disapproval of their speech. App. 13. The court found that *Facebook* was the subject of the District's investigation, which

---

[30] The Superior Court also rejected Facebook's Fourth Amendment challenges, reasoning that the Fourth Amendment "protects only privacy interests that society accepts as objectively reasonable, and Facebook users do not have an objectively reasonable expectation of privacy in information that they include in public posts about COVID-19 vaccines and their identities." App. 21 n.3 (citation omitted). Facebook has abandoned its Fourth Amendment arguments before this Court.

focused on whether Facebook made deceptive statements about its enforcement efforts. App. 13-14. In any event, the court noted that the users who publicly posted content about vaccines never masked themselves in the first place, as Facebook's terms required them to use their everyday names. App. 14, 31. But even then, "the District is seeking only the identities that these users themselves employed in their public posts." App. 31. If users did not comply with Facebook's requirement that they use their true names, Facebook is obligated only to "provide to the District the information about their identities that the users chose to include in their posts." App. 31. The Superior Court also rejected the contention that the District was trying to regulate or chill consumer speech. App. 14.

Finally, even assuming exacting scrutiny applied, the court first found that the District had a compelling interest in investigating whether Facebook made false statements that violated the CPPA. App. 28-30. Next, it determined that OAG's subpoena was narrowly tailored to its investigative goals. App. 30. Third, it found that the identities of the Facebook users, like content they posted, was information they chose to make public themselves. App. 31. Lastly, the court determined that providing user information would not lead to reprisals because the record does not support that OAG will disclose the information, and even if it did, any criticism the users might receive stems from the public nature of their posts, not any the District's

actions. App. 31-32. The court found that this case stood in "sharp contrast" to the First Amendment precedents Facebook cited. App. 32-34.

STANDARD OF REVIEW

This Court reviews questions of law like issues of statutory construction de novo. *Richardson v. Easterling*, 878 A.2d 1212, 1216 & n.5 (D.C. 2005).

SUMMARY OF ARGUMENT

1. The Court should affirm the Superior Court's determination that OAG can compel the content it seeks with a subpoena rather than a warrant under the SCA.

First, the SCA's protections do not apply to public content—and public content is all that Facebook has been ordered to produce here. The SCA expressly provides that its protections do not apply when an "electronic communication is readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i). The Act's legislative history confirms Congress's clear intent not to protect public content. And courts have recognized as much, concluding that there can be no violation of the SCA unless the content at issue is unavailable to the public.

Second, even if the SCA applies to public content, its warrant requirement does not. Section 2702(b) lists instances when providers may disclose otherwise protected information, and subsection (b)(3) covers information disclosed with a user's consent. Facebook agrees that the information OAG seeks falls within this exception. And this Court has already held in *Pepe* that a provider must turn over

information that falls within a Section 2702(b) exception in response to a subpoena by a private party.

There is no indication that the government is subject to a different, special rule. To be sure, Section 2703 generally requires the government to obtain a warrant. But this Court should read that provision in harmony with Section 2702(b), which explicitly permits disclosure to the government in certain circumstances. Moreover, reading the SCA to require a warrant here runs contrary to the Act's purposes and would lead to absurd results. The purpose of the SCA is to afford Fourth Amendment protections to electronic communications just as that Amendment otherwise would apply. But the Fourth Amendment does not protect public information, and consent is a well-settled exception to the warrant requirement. Moreover, Facebook's interpretation would create a special carve-out for the government that would require it to get a warrant for information that a private party could obtain by subpoena. It would also effectively insulate providers like Facebook and Twitter from most civil investigations concerning public representations about content on their platforms. Nothing in the SCA compels these incongruous results.

Third, if the warrant requirement applies, OAG's request did not trigger it because the subpoena does not "require the disclosure" of user content. Rather, the content OAG seeks has already been divulged to the public. In complying with the

subpoena, then, Facebook will not have to disclose any new content, but only acknowledge an earlier disclosure—something the SCA in no way forbids.

2. Facebook's First Amendment challenges also lack merit. Before a court subjects a subpoena to exacting scrutiny, the party claiming a privilege must make a prima facie showing that the subpoena infringes on its First Amendment rights. Facebook has not made that showing, either as to itself or its users.

Regarding itself, OAG is investigating Facebook's *commercial* speech—its own statements about its efforts to combat COVID-19 vaccine misinformation on its platform. Facebook never claims that OAG's investigation has a chilling effect on, or restrains, *this* speech. Instead, Facebook maintains that OAG is acting in bad faith to target its editorial control over its platform. Not so. A party alleging bad faith carries a heavy burden to prove that an agency, not just an employee, issued a subpoena for an improper reason. Facebook has presented no evidence, let alone sufficient evidence, to prove institutional bad faith. In any event, its claim that OAG's investigation infringes on its right to content moderation is baseless. Facebook relies on cases where the government either compelled speech, barred the exercise of editorial discretion, or targeted the speech for which protection was sought. OAG's investigation does none of these things; it simply seeks to confirm that Facebook is complying with *its own* public representations about its vaccine misinformation policy.

Facebook relies on another series of mischaracterizations when claiming that OAG's subpoena infringes on the First Amendment rights of its users, asserting that OAG is targeting its users based on disfavored speech and attempting to unmask those who wish to remain anonymous. Not so. OAG is not targeting Facebook users, nor could it under the CPPA. It is investigating Facebook and its statements about its vaccine misinformation policies. What is more, Facebook has offered no evidence, as it must, to show that OAG's investigation will have a chilling effect on users' speech. Nor could it. Because the users have spoken and identified themselves publicly, they have acted outside of any zone of protection, and OAG's investigation does not chill or abridge their First Amendment rights. Finally, no anonymous users will be "unmasked" because the Superior Court's order forbids it.

Even if Facebook had made a prima facie showing of a First Amendment infringement against itself or its users, OAG's subpoena survives exacting scrutiny. Facebook agrees that OAG has a legitimate interest in consumer protection, but claims it is not implicated here because it has made no statements about the *quantity* of COVID-19 vaccine misinformation it has removed. That is irrelevant. OAG's focus is not on the accuracy of Facebook's statements about the amount of content it has removed; its focus is on Facebook's statements about its enforcement of its vaccine misinformation policy, including the content it has *failed* to remove despite its pledges.

Finally, OAG's subpoena is narrowly tailored to its important interest in consumer protection. OAG needs the identity of Facebook users to assess Facebook's response to repeat offenders and those who have been publicly identified as responsible for much of the misinformation on its platform. Anonymized information will not permit OAG to make this assessment. Instead, the Superior Court correctly found that there is no less intrusive means for OAG to accomplish its investigative goals.

ARGUMENT

I. The SCA Does Not Preclude OAG From Compelling The Production Of Public Content With A Subpoena.

A. The SCA does not apply to protect public information, but only information the user intends to be private.

The plain text of the SCA, its legislative history, and case law make clear that the SCA does not apply to public information, which is all that the court ordered be produced here. When assessing the meaning of any statute, the Court begins with the text. *Peoples Drug Stores, Inc. v. District of Columbia*, 470 A.2d 751, 753 (D.C. 1983). If the language is clear and unambiguous, the Court should give effect to its plain meaning unless there are "persuasive reasons" to look beyond it. *Id*. at 755 (internal quotation marks omitted). Here the text of the SCA is unambiguous: it does not apply to preclude *anyone* access to public content. Federal law provides:

> (g) It shall not be unlawful under this chapter or chapter 121 of this title [(the SCA)] for any person—

> (i) 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*.

18 U.S.C. § 2511(2)(g)(i) (emphasis added). "The language of the statute makes clear that the statute's purpose is to protect information that the communicator took steps to keep private," not Facebook posts configured by users to be public. *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 668 (D.N.J. 2013); *see Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965, 981 (C.D. Cal. 2010) ("[A] completely public [bulletin board service] does not merit protection under the SCA.").[31]

---

[31] Although not citing to 18 U.S.C. § 2511(2)(g)(i) below, OAG has consistently argued throughout this litigation that the SCA does not apply to publicly disclosed communications. OAG's Mem. in Support of Pet. for Enforcement 12 ("[A]s case law and legislative history make clear, the SCA was not intended to protect publicly disclosed communications."); OAG's Reply ISO Pet. for Enforcement 10 (filed Feb. 22, 2022) (asserting that the SCA's purpose is to protect information that the consumer intended to keep private). This statutory argument, as well as arguments about the applicability of the SCA warrant requirement to public information, are simply further evidence of that claim regarding the SCA's scope. *See Tindle v. United States*, 778 A.2d 1077, 1082 (D.C. 2001) ("[T]he Supreme Court of the United States and this court have distinguished between 'claims' and 'arguments,' holding that although 'claims' not presented in the trial court will be forfeited (and thus subject to the plain error review standard), parties on appeal are not limited to the precise arguments they made in the trial court." (internal quotation marks omitted)).

The legislative history confirms what the statute plainly says. *See Facebook, Inc. v. Wint*, 199 A.3d 625, 628 (D.C. 2019) (looking to legislative history to confirm that an interpretation accords with legislative intent). In enacting the SCA, Congress "repeatedly focused on the public/private theme" when explaining the purpose of the legislation. *Facebook, Inc. v. Superior Ct.*, 417 P.3d 725, 739-40 (Cal. 2018). In Congress's view, "[t]o access a communication in such a public [electronic bulletin board] system is not a violation of the Act, since the general public has been 'authorized' to do so by the facility provider." S. Rep. 36; *see* H.R. Rep. 62 (same). Congress intended that "[t]hose wire or electronic communications which the service provider attempts to keep confidential would be protected, while the statute would impose no liability for access to features configured to be readily accessible to the general public." H.R. Rep. 63; *see* S. Rep. 35 (addressing the "problem of unauthorized persons deliberately gaining access to . . . electronic . . . communications that are not intended to be available to the public.").

Thus, for *public* information, it is simply incorrect to say—as Facebook does—that "Section 2703(a) 'provides requirements for the government to obtain the contents of an electronic communication" or that "[a] government entity can *only gain access* to the contents of such an electronic communication pursuant to a warrant." Br. 26 (quoting S. Rep. 38); *see* Br. 3 (asserting that the government may only "access" consumer communications with a warrant). Instead, the SCA puts a

governmental entity on par with the public when it comes to accessing public communications in electronic storage. That is, the SCA imposes no restriction on its ability to do so.

Case law confirms this understanding of the SCA. Courts have recognized that "the requirement that the electronic communication *not be* readily accessible by the general public is *material and essential* to recovery under the SCA." *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir. 2006) (emphasis added). Thus, "the SCA covers: (1) electronic communications, (2) that were transmitted via an electronic communication service, (3) that are in electronic storage, and (4) *that are not public*." *Ehling*, 961 F. Supp. 2d at 667 (emphasis added). There can be no violation of the SCA for disclosing content configured to be publicly available. *See Combier v. Portelos*, No. 17-CV-2239 (MKB), 2018 WL 3302182, at *13 (E.D.N.Y. July 5, 2018) ("Courts have held that information is protected by the SCA only if the plaintiff restricts access to the electronic communication."), *R. & R. adopted*, 2018 WL 4678577 (E.D.N.Y. Sept. 29, 2018), *aff'd*, 788 F. App'x 774 (2d Cir. 2019); *Burke v. New Mexico*, No. 16-CV-0470 MCA/SMV, 2018 WL 3054674, at *8

(D.N.M. June 20, 2018) ("[A]n SCA violation cannot flow from accessing a stored communication that was not made private.").[32]

Because OAG seeks only public content, the SCA neither subjects Facebook to liability nor imposes a barrier to it being compelled to produce user and corrective-action information in response to an administrative subpoena. *See Airbnb, Inc. v. City of Bos.*, 386 F. Supp. 3d 113, 124 (D. Mass. 2019) (SCA does not prohibit compelling "Airbnb to provide . . . information appearing in its public listings for Boston rental properties—specifically, the location description a host has provided in the listing, and whether the listed accommodation is a room or an entire unit"); *Louis Vuitton Malletier, S.A. v. Akanoc Sols., Inc.*, No. C 07-03952 JW, 2008 WL 3200822, at *1 (N.D. Cal. Aug. 7, 2008) ("Defendants . . . are only required to disclose information that the third-parties have made available to the public.").[33]

---

[32] Notably, courts that have disagreed with this interpretation of the SCA have nevertheless permitted the disclosure of public information under Section 2702(b). *See Facebook, Inc.*, 417 P.3d at 743-44 ("Under this view, which appears to have been endorsed by some commentators, the Act simply would not cover or protect communications that have been configured to be public. We do not endorse this reading of the Act, however. Instead, we conclude that, by virtue of section 2702(a), the Act generally and initially prohibits the disclosure of *all* (even public) communications—but that section 2702(b)(3)'s subsequent lawful consent exception allows providers to disclose communications configured by the user to be public." (footnote omitted)).

[33] The Superior Court's order covers both information that remains publicly available on Facebook and information configured to be publicly available by users, but that Facebook has subsequently removed. Facebook has not suggested, let alone

B. Even if the SCA applies to public content, Congress intended the warrant requirement to apply only to private information.

Assuming that the SCA applies to public content, OAG can obtain the information it seeks without a warrant because the warrant requirement is not the exclusive path for the government to obtain information. Rather, Section 2702(b)(3) permits a provider to divulge the contents of a communication "with the lawful consent of the originator or an addressee or intended recipient of such communication." The information OAG seeks falls within this exception. Because it was publicly posted with user consent, OAG necessarily has the "lawful consent" of the "originator." At the very least, it has the "lawful consent" of the "intended recipient of such communication"; because the posts were public, "recipient" refers to everyone, OAG included. Facebook agrees, conceding that it could "voluntarily" produce this information if it chose without a warrant. Br. 25 & n.21.

Despite Section 2702(b)'s use of the term "may," 18 U.S.C. § 2702(b) ("a provider . . . *may* divulge" (emphasis added)), this Court has already held that a provider *must* comply with a subpoena if a Section 2702(b) exception applies. In

---

argued, that the public information it deleted but maintains on its servers should be treated as any more private than the public information that remains on its platform today. In both instances, the *user* configured the information to be public, Facebook disclosed it to the public, and there is no reason to think that by removing the posts, Facebook wiped it from the public domain. *See*, *e.g.*, Trump Twitter Archive, https://www.thetrumparchive.com (archiving former President Donald Trump's tweets, although Twitter deleted his account) (last visited Nov. 7, 2022).

Pepe, a criminal defendant subpoenaed Facebook to produce content from his own account, including communications from others, that was no longer available to him. 241 A.3d at 251-52. Noting the "weighty and well-settled presumption against inferring that Congress silently intended to foreclose or restrict the availability of a core component of the judicial process such as the subpoena power," the Court found no congressional intent to prohibit a subpoena where the (b)(3) consent exception applied to expressly permit disclosure. *Id*. at 257 (emphasis omitted). Instead, the Section 2702(b) exceptions "remove th[e] barrier to subpoena compliance and enable service providers to comply with compulsory process." *Id*.; *cf. Wint*, 199 A.3d at 629 (holding conversely that a criminal defendant cannot subpoena content where none of the Section 2702(b) exceptions applies). Said another way, Section 2702 does "not purport to authorize providers to refuse to [disclose communications] at their own option, let alone to vest them with a novel privilege to withhold evidence from discovery for any or no reason." *Pepe*, 241 A.3d at 257.

Pepe's reasoning applies with equal force here. OAG issued a valid administrative subpoena for information that Facebook concedes satisfies a Section 2702 exception. As the Court in *Pepe* held, nothing about Section 2702 makes compliance with that subpoena optional.

Seeking to distinguish *Pepe*, Facebook envisions a special rule precluding only *governmental* subpoenas and requiring the government to get a warrant in every

instance it seeks stored communications under the SCA. But that special carve out for the government does not appear in the SCA's text, defies Congress's intent when it passed the Act, and leads to absurd results.

First, regarding the text, Facebook hinges its argument on Section 2703(a)'s admonition that "[a] governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication . . . *only* pursuant to a warrant." 18 U.S.C. § 2703(a) (emphasis added). Read in isolation, that provision might suggest that Section 2703's warrant requirement is the exclusive means for the government to obtain the contents of communications. But reading the SCA holistically, that cannot possibly be what it means. That is because many provisions of Section 2702 unambiguously and exclusively apply to disclosures to government entities. For instance, subsection (b)(7) permits disclosure to "a law enforcement agency . . . if the contents—(i) were inadvertently obtained by the service provider; and (ii) appear to pertain to the commission of a crime." *Id.* § 2702(b)(7); *see also id*. § 2702(b)(8) (permitting disclosure to a governmental entity if the provider "believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay").

Given this, Section 2703 cannot be the *sole* method by which the government can obtain information under the Act. The better reading, which harmonizes

Sections 2702 and 2703, is that Section 2703's warrant requirement is the exclusive option for the government to obtain information *where a Section 2702 exception does not apply*. That interpretation is supported by Section 2702(b)'s express incorporation by reference of the disclosures "authorized in . . . [section] 2703." *Id.* § 2702(b)(2). If a Section 2703 warrant is one instance when a provider may disclose information under Section 2702, so too is a subpoena for information that falls within another Section 2702 exception. This construction also comports with this Court's clarification that "[r]ead together, §§ 2702 and 2703 appear to comprehensively address the circumstances in which providers may disclose covered communications." *Wint*, 199 A.3d at 628; *see Walker*, 956 F.3d at 167 ("sections 2702 and 2703 regulate the information given to the government"). Rather than "blur[] the distinction between Sections 2702 and 2703," Br. 25, then, the Superior Court's interpretation harmonizes those provisions.[34]

Were there any doubt about the meaning of the SCA's text, the purpose of the SCA confirms that the government need not obtain a warrant to acquire a stored communication that falls within a Section 2702(b) exception. "The literal words of a statute are not the sole index to legislative intent, but rather, are to be read in the

---

[34] Facebook contends that this outcome is inconsistent with language from a footnote in *Pepe*, Br. 30, but in that case, the Court had no occasion to consider whether the government could compel the production of public communications that fall within a Section 2702(b) exception by subpoena.

light of the statute taken as a whole and are to be given a sensible construction." *Washington v. United States*, 206 A.3d 864, 867-68 (D.C. 2019) (brackets and ellipses omitted). Moreover, the Court may also look beyond the plain meaning of a statute where the literal meaning would produce an absurd result or undermine the legislative purpose of the statute as a whole. *See Dobyns v. United States*, 30 A.3d 155, 159 (D.C. 2011). Taken as a whole, the SCA does not reflect a legislative intent that the government obtain *public* content only with a warrant.

As Facebook agrees, Congress's purpose in enacting the SCA was to extend Fourth Amendment-like privacy protections to electronic communications. *See* Br. 6, 22, 27; S. Rep. 5 ("[T]he law must advance with the technology to ensure the continued vitality of the [F]ourth [A]mendment."); H.R. Rep. 19 (same); Kerr, 72 Geo. Wash. L. Rev. at 1214. Thus, Facebook understands that Congress imposed the warrant requirement because Congress concluded that the Fourth Amendment should protect private content in stored communications. *See* Br. 6, 22, 27.

The Fourth Amendment, however, provides no protection to publicly available information because there can be no reasonable expectation of privacy in it. *See United States v. Knotts*, 460 U.S. 276, 281 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). Thus, a government agent's "viewing of what a private party had freely made available for his inspection d[oes] not violate

the Fourth Amendment." *United States v. Jacobsen*, 466 U.S. 109, 119 (1984). Simply put, "[w]hen a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment." *United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) (citing *Katz v. United States*, 389 U.S. 347, 351 (1967)); *see Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Users would logically lack a legitimate expectation of privacy in the materials intended for publication or public posting."). It follows that "[i]f electronic content (be it text, photos or videos) is readily accessible to the general public there is absolutely no need for the government to obtain a search warrant to view this content." *Facebook, Inc. v. Superior Ct.*, 223 Cal. Rptr. 3d 660, 665 (Cal. Ct. App. 2017).

Similarly, it is "well settled that one of the specifically established exceptions to the requirements of both a warrant and probable cause is a search that is conducted pursuant to consent." *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973). "'Consent searches are part of the standard investigatory techniques of law enforcement agencies' and are 'a constitutionally permissible and wholly legitimate aspect of effective police activity.'" *Fernandez v. California*, 571 U.S. 292, 298 (2014) (quoting *Schneckloth*, 412 U.S. at 228, 231-32). "It would be unreasonable—indeed, absurd—to require police officers to obtain a warrant when the sole owner or occupant of a house or apartment voluntarily consents to a search." *Id*.

Setting aside the third-party exception, there is no indication that Congress intended to afford *more* protections to information than the Fourth Amendment would otherwise. To the contrary, the plain text of the SCA establishes that Congress provided *less*, including by permitting a governmental entity to obtain content older than 180 days with a court order based on something less than probable cause with notice to, but without consent from, a user—a procedure that falls beneath the protections afforded by the Fourth Amendment. *United States v. Warshak*, 631 F.3d 266, 287-88 (6th Cir. 2010). Given Congress's intent to (at most) mirror the Fourth Amendment's protections for stored electronic communications, the only sensible construction of the warrant requirement is that it applies to content the user intended to be private, not the public information at issue here. Indeed, requiring a warrant where OAG seeks public user content would place the government in a less favorable position than a private citizen subpoenaing that same information. *See Pepe*, 241 A.3d at 256-59. That is an absurd result that Congress could not have intended.

Facebook's interpretation would also perversely shield internet providers from civil investigations to which companies in other industries are routinely subject. Notably, OAG could not obtain a warrant for the information it seeks here (and Facebook does not suggest it could). "Unlike a subpoena, . . . an SCA warrant is not civil by nature." *In re 381 Search Warrants Directed to Facebook, Inc.*, 78

N.E.3d 141, 147 (N.Y. 2017) (internal quotation marks omitted). But OAG is admittedly not investigating a crime, nor does the CPPA subject Facebook to possible criminal penalties. Instead, OAG is seeking Facebook's business records related to a consumer-protection investigation—the quintessential function of a statutorily authorized civil subpoena. If the warrant requirement applied here, the SCA would effectively shield providers like Facebook and Twitter from civil investigations into their representations about the content on their platform, a protection that no other industry enjoys.

Thus, the Superior Court's interpretation would hardly lead to a "dramatic expansion" of OAG's ability to access user content, Br. 3, nor will it "gut" the SCA, Br. 27. Rather, the Superior Court's interpretation simply mirrors the Fourth Amendment's protections for public electronic communications, permitting the government to subpoena that information if the user has consented to its public dissemination. It is *Facebook's* interpretation that would yield dramatic consequences, placing tech companies in a category of their own and immune to most civil investigations about the content on their platforms.[35]

---

[35] While Facebook contends that the Superior Court's decision "stands alone," Br. 3-4, 29, this is only because no other court has been asked to consider anything close to the precise question presented here—whether the government can compel *public* content under a Section 2702(b) exception with an administrative subpoena.

C. If the warrant requirement applies, OAG's subpoena did not trigger it because responding to the subpoena does not "require the disclosure" of user content.

Even if Facebook were correct that OAG's only recourse is to obtain a warrant to disclose content, Section 2703 would still not apply. Section 2703 mandates that the government obtain a warrant before "requir[ing] the disclosure by a provider . . . of the contents" of an electronic communication. 18 U.S.C. § 2703(a). But OAG's subpoena will not "require the disclosure" of the contents of an electronic communication. Any disclosure of content here occurred when Facebook voluntarily divulged the information in its users' public posts on its social media platform, delivering them to the intended recipients—the public writ large, including OAG—upon the users' request and with their consent. Thus, Facebook has already let the metaphorical "cat out of the bag." With the information disclosed to the public, Facebook would not have to divulge any additional content when responding to OAG's subpoena. Nothing in Section 2703 precludes Facebook from simply acknowledging a past disclosure.

II. Enforcing OAG's Subpoena Will Not Infringe On The First Amendment Rights Of Facebook Or Its Users.

Having failed to show a violation of the SCA, Facebook is left to suggest that OAG's routine investigatory subpoena violates the First Amendment. That argument is flawed at the outset because it is built on mischaracterizations of OAG's investigation, which concerns Facebook's own public representations about the

content on its platform, not any disagreement with the messages it publishes. Facebook therefore has not shown that OAG's investigation implicates either its First Amendment rights or those of its users. Thus, OAG's subpoena is not subject to exacting scrutiny. Even if it were, OAG has identified a significant governmental interest in enforcing the District's consumer protection laws, and its request is substantially related to this important interest.

A. Facebook has not made the prima facie showing of a First Amendment violation required to trigger exacting scrutiny.

Ordinarily, a court will enforce an investigative subpoena with little scrutiny if it meets the three-prong test from *United States v. Morton Salt Co.*, 338 U.S. 632 (1950): (1) the investigation and issuing the subpoena are within the authority of the agency; (2) the demands sought are not too indefinite and are reasonably related to the inquiry; and (3) the demands are not unduly burdensome or unreasonably broad. *Id.* at 652; *Okla. Press Pub. Co. v. Walling*, 327 U.S. 186, 208-09 (1946); *EEOC v. Kloster Cruise Ltd.*, 939 F.2d 920, 922 (11th Cir. 1991). Facebook does not suggest on appeal that OAG's subpoena lacks these attributes.

Rather, Facebook argues that OAG's subpoena violates the First Amendment. "[A] higher degree of scrutiny must attach before courts can compel disclosure of information that may impinge upon" First Amendment rights. *Fed. Election Comm'n v. Fla. for Kennedy Comm.*, 681 F.2d 1281, 1284 (11th Cir. 1982); *see Sweezy v. New Hampshire*, 354 U.S. 234, 245 (1957). A party claiming a First

Amendment privilege "always bears the initial burden of establishing the factual predicate for the privilege." *In re Motor Fuel Temperature Sales Pracs. Litig.*, 641 F.3d 470, 488 (10th Cir. 2011). "Bare allegations of possible [F]irst [A]mendment violations are insufficient to justify judicial intervention into a pending investigation." *McLaughlin v. Serv. Emps. Union, AFL-CIO, Loc. 280*, 880 F.2d 170, 175 (9th Cir. 1989). If the party asserting the privilege makes its prima facie case, the burden shifts to the government to satisfy "exacting scrutiny" by showing that there is a substantial relationship between its request and an important governmental interest. *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2383 (2021); *see Solers, Inc. v. Doe*, 977 A.2d 941, 957 n.15 (D.C. 2009).

1. Facebook has not made a prima facie case that the subpoena infringes on its First Amendment Rights.

OAG's subpoena does not violate Facebook's First Amendment rights because the subpoena is not based on the government's disagreement with any particular viewpoint. Rather, it is simply part of an investigation into whether Facebook is complying with *its own* representations about the content on its platform—that is, Facebook's commercial speech.

"[T]he Constitution accords less protection to commercial speech than to other constitutionally safeguarded forms of expression." *Bolger v. Youngs Drug Prod. Corp.*, 463 U.S. 60, 64-65 (1983). Indeed, commercial speech that is false or misleading garners no First Amendment protection and "may be prohibited

entirely." *In re R.M.J.*, 455 U.S. 191, 203 (1982); *Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557, 566 (1980) (To be protected, commercial speech "must . . . not be misleading."); *Bates v. State Bar of Ariz.*, 433 U.S. 350, 383 (1977) ("[T]he leeway for untruthful or misleading expression that has been allowed in other contexts has little force in the commercial arena.").

Here, OAG issued its subpoena under the authority of the CPPA, which prohibits unfair or deceptive trade practices. D.C. Code §§ 28-3904, 28-3910(a). As OAG explained in its subpoena, and to the court below, it is investigating whether Facebook has violated the CPPA with its representations about its efforts to prevent vaccine misinformation on its platform, including claims that it "prohibits" and "removes" this content. App. 1, 8. OAG's subpoena thus fits squarely within First Amendment guardrails: it is an effort to ensure that Facebook's commercial speech—its guarantees about the content on its platform—are not false or misleading to consumers. "Even if content moderation is protected speech, making misrepresentations about content moderation policies is not." *Twitter, Inc. v. Paxton*, 26 F.4th 1119, 1125 (9th Cir. 2022).

Notably, Facebook has never claimed that OAG's investigation burdens this speech by impermissible restraint or chilling effect. Mem. of Opposing P. & A. in Opp'n To the D.C.'s Pet. for Enforcement ("Opp.") 15-25 (filed Jan. 31, 2022). Nor could it. Facebook's "right to impart truthful and accurate information concerning

its services [i]s not threatened by the Attorney General's investigation." *Scott v. Ass'n for Childbirth at Home, Int'l*, 430 N.E.2d 1012, 1016 (Ill. 1981); *see Bates*, 433 U.S. at 383 ("Since the advertiser knows his product and has a commercial interest in its dissemination, we have little worry that regulation to assure truthfulness will discourage protected speech.").

Instead, to concoct a First Amendment violation, Facebook accuses OAG of a bad-faith effort to exercise editorial control over its content moderation. Br. 1, 34-38. Ignoring its own representations about its vaccine-misinformation policies, Facebook asserts that OAG's subpoena "probes and penalizes" its right to control its platform's content, and that OAG is using its investigative power to "scrutinize and pressure" it into changing how it exercises editorial control, with a chilling effect on it content-moderating decisions. Br. 34-38.

Facebook's bald and unsubstantiated assertions of OAG's bad faith lack merit. Of course, a court may not enforce a subpoena issued in bad faith. *See United States v. Powell,* 379 U.S. 48, 58 (1964). But an assertion of bad faith must be based on evidence that the agency—as an institution as opposed to an individual employee—acted with an improper motive when it served the subpoena. *See United States v. LaSalle Nat'l Bank,* 437 U.S. 298, 314-16 (1978). Once an agency satisfies the *Morton Salt* standard—which OAG indisputably has—the burden is on the challenger to prove bad faith, and this burden is "heavy." *Ngo v. United States*, 699

F. App'x 617, 619 (9th Cir. 2017) ("When the Government sets forth a prima facie case, the petitioner bears the heavy burden of alleging specific facts and evidence supporting its allegations of bad faith." (internal quotation marks omitted)); *NLRB v. Am. Med. Response, Inc.*, 438 F.3d 188, 192 (2d Cir. 2006) ("A subpoena that satisfies [the *Morton Salt*] criteria will be enforced unless the party opposing enforcement demonstrates that the subpoena is . . . issued in bad faith or for other improper purposes.").

Facebook has not met its heavy burden to prove institutional bad faith: that the real reason for the subpoena is to control its editorial content. As the Superior Court correctly found, Facebook offers the Court "no reason," and certainly no evidence, to question OAG's representations. App. 27-28. Beyond failing to show bad faith, Facebook has not even articulated how OAG's subpoena infringes its editorial right of freedom of expression, let alone made a prima facie showing. Indeed, the Superior Court reasonably found that "the subpoena would have no effect *whatsoever* on [Facebook's] content moderation polices or how it applies and enforces them." App. 27 (emphasis added). This is a finding that Facebook neither acknowledges nor meaningfully challenges.

To be sure, Facebook devotes pages of its brief to establishing what no one disputes—that the First Amendment protects its right to decide what to publish or not publish on its platform. Br. 34-37. But it is strikingly silent as to how OAG's

subpoena infringes on this right, merely asserting in a conclusory fashion that OAG's demand "interfere[s] with" or "intrudes on" its First Amendment right. Br. 2, 38. Courts demand more to make a showing of the government's bad faith.

The authorities Facebook cites only underscore the correctness of the Superior Court's holding. Facebook's main authorities involve actual infringement on editorial discretion. For example, in *Miami Herald Publishing Company v. Tornillo*, 418 U.S. 241 (1974), a Florida statute required newspapers to print, free of cost, a political candidate's reply when newspapers assailed their character or record. *Id.* at 244. Noncompliance with the statute was a misdemeanor. *Id*. Understandably, the Supreme Court found that the penalty provision would chill political and electoral coverage and that compulsory candidate access was incompatible with editorial decision-making. *Id*. at 257-258. Similarly, *NetChoice, LLC v. Attorney General*, 34 F.4th 1196 (11th Cir. 2022), involved a challenge to another Florida law that "prohibit[ed] certain social-media companies from 'deplatforming' political candidates under any circumstances, prioritizing or deprioritizing any post or message 'by or about' a candidate, and, more broadly, removing anything posted by a 'journalistic enterprise' based on its content." *Id.* at 1203. The court found this law "clearly restrict[ed] platforms' editorial judgment by preventing them from removing or deprioritizing content or users and forcing them to disseminate messages that they find objectionable," violating the First Amendment. *Id*. at 1222;

see also O'Handley v. Padilla, 579 F. Supp. 3d 1163, 1188 (N.D. Cal. 2022) ("Twitter has important First Amendment rights that would be jeopardized by a Court order telling Twitter what content-moderation policies to adopt and how to enforce those policies.").

These cases are inapposite here. OAG's investigation does not compel Facebook to say anything, nor does it require Facebook to adopt any particular content moderation policy or procedure. And OAG has certainly not warned Facebook to "stop doing" anything, let alone suggested there would a "consequence" if Facebook "fail[ed] to heed that warning." Br. 37.

Nor is there any reasonable basis to conclude that OAG's investigation will have a chilling effect on Facebook's content moderation. OAG's investigation is nothing like the investigations cited by Facebook. Br. 37. In *White v. Lee*, 227 F.3d 1214 (9th Cir. 2000), for instance, the challenged investigation lasted longer than statutorily authorized, the investigators' conciliation proposal precluded plaintiffs from engaging in certain speech, the plaintiffs were interrogated and threatened with subpoenas, and the investigators told a major metropolitan newspaper that plaintiffs had broken the law with their speech. *Id.* at 1228-29. The court concluded "that these actions would have chilled or silenced a person of ordinary firmness from engaging in future First Amendment activities." *Id*. at 1229. OAG's lawful subpoena has none of these attributes.

More fundamentally, unlike every case cited by Facebook, OAG's investigation does not target the speech for which Facebook seeks protection—its right to content moderation. Br. 37 & n.24; *see Parkhouse v. Stringer*, 863 N.Y.S.2d 400, 405 (N.Y. App. Div. 2008) ("[W]e do not find that the nature or extent of DOI's investigation amounts to the chilling of petitioner's speech rights inasmuch as the investigation is not aimed at the content of petitioner's speech."), *aff'd*, 912 N.E.2d 48 (N.Y. 2009). Instead, OAG has directed its investigation at Facebook's potentially deceptive or false statements *about* its content moderation policies. *See Twitter, Inc.*, 26 F.4th at 1125 ("[I]f Twitter's statements are misleading commercial speech, and thus unprotected, then Twitter's content moderation decisions would be a proper cause for the investigation, because they would be the very acts that make its speech misleading.").

Finally, there is no evidence that OAG's investigation is to retaliate against Facebook for its content-moderation decisions. Instead, as the Superior Court found, "[t]he District's investigation is not targeted at [Facebook's] exercise of any First Amendment right and in any event, [Facebook] does not suggest that compliance with the subpoena would in fact inhibit it from exercising its right to control its content moderation policies." App. 28 n.4. Considering all of this, Facebook has not carried its heavy burden to make a prima facie showing that OAG's investigation infringes upon Facebook's First Amendment rights.

2. Facebook has not made a prima facie case that the subpoena infringes on its users' First Amendment rights.

In another series of mischaracterizations, Facebook maintains that OAG's investigation infringes on the First Amendment rights of its users by "unmask[ing] those who engage in speech that is disfavored by OAG," with an intent to "blacklist" them. Br. 33, 49; *see* Br. 4, 38. These bald assertions cannot support a prima facie showing that OAG's subpoena infringes on users' First Amendment rights. To do so, Facebook would have had to present the Superior Court with some evidence that enforcement of the subpoena would result in harassment or other consequences which objectively suggest a "chilling" of its users' speech. *See Brock v. Loc. 375, Plumbers Int'l Union of Am.*, 860 F.2d 346, 349-50 (9th Cir. 1988); *Motor Fuel Temperature Sales*, 641 F.3d at 491. "A subjective fear of reprisal is insufficient to invoke [F]irst [A]mendment protection against a disclosure requirement." *Dole v. Loc. Union 375, Plumbers Int'l Union of Am.*, 921 F.2d 969, 973 (9th Cir. 1990).

However, as the Superior Court found, Facebook presented "*no evidence*" that those "who publicly posted positive or negative content that [Facebook] later determined violated its content moderation policies (a) were in the past subjected to threats or worse or (b) are any more likely in the future to be subjected to any response other than verbal criticism." App. 32-33. Instead, Facebook's "concerns about a chilling effect on Facebook users who want to post content that is negative

or positive about COVID-19 vaccines is speculative." App. 32. This speculation cannot trigger exacting scrutiny.

Even if they were not speculative, Facebook's arguments are baseless in many other respects. *First*, as the Superior Court found, OAG is not targeting Facebook users or their speech with its subpoena, but only Facebook itself. App. 13, 35. Facebook never suggests otherwise.

Second, OAG is not seeking to "identify potentially millions of users 'associated with' speech it views as undesirable," Br. 38; *see* Br. 12, 44, but only those users who Facebook has determined have violated its COVID-19 vaccine misinformation policy, and then only to assess the truthfulness of Facebook's claims, App. 35.[36] Indeed, Facebook presented no evidence to support its claim that OAG's subpoena implicates "millions" of users. Instead, it represents here that it "does not separately track COVID-19 misinformation specific to vaccines," and thus cannot even guess about how many users have violated its content policy. Br. 13 n.15.

Third, Facebook ignores the fact that the Superior Court limited its order to public content by persons who have identified themselves publicly. This is

---

[36] Notably, the Superior Court left Facebook considerable discretion in identifying those users, providing that Facebook "may adopt any reasonable interpretation of the term ['associated'] that minimizes its burden in responding to the subpoena and protects users who have not given explicit or implicit consent to disclosure of their identities by making public posts." App. 35.

significant. When Facebook users post publicly, "[n]o interest legitimately protected by the First and Fifth Amendments is involved." *Reps. Comm. for Freedom of Press v. Am. Tel. & Tel. Co.*, 593 F.2d 1030, 1058 (D.C. Cir. 1978). As the D.C. Circuit has explained,

> [t]o the extent individuals desire to exercise their First Amendment rights in private, free from possible good faith law enforcement investigation, they must operate within the zone of privacy secured by the Fourth Amendment. When individuals expose their activities to third parties, they similarly expose these activities to possible Government scrutiny. The mere prospect that such investigation may occur or, indeed, the actual conduct of such investigation does not "chill" or otherwise abridge First Amendment rights, even though it may give rise to subjective inhibitions for those who desire to avoid the prospect of investigation altogether.

Id. at 1058-59. This would be especially true where, as here, Facebook's users are on notice that Facebook could turn over their information in response to a subpoena. *See supra* n.15.

Facebook's authority is not to the contrary. Instead, as the Superior Court found, the cases on which it relies involve only the disclosure of confidential, private, and anonymous member information—not information already in the public domain. App. 32-33; *see*, *e.g.*, Br. 48 (citing *Ams. for Prosperity*, 141 S. Ct. at 2381-84, 2386-89 (involving private donor information)).

Fourth, Facebook is simply wrong to claim that OAG is seeking to unmask users who have chosen to remain anonymous. Br. 47-48. The Superior Court was clear that Facebook need only provide users' *public-facing* identities. App. 31.

Those who choose to remain anonymous by using fictitious identities in violation of Facebook's terms of use will remain anonymous under this subpoena. *See* App. 31 ("Meta's terms of use require users to identify themselves using the same name that they use in everyday life, . . . but even if users did not comply . . . , Meta will provide to the District the information about their identities *that the users chose to include in their posts*." (emphasis added)). Thus, upholding OAG's subpoena will not enable it to "target" groups "under the guise of consumer protection" to "demand the identities" of those who want to remain anonymous. Br. 4-5, 34, 38.

As for user information that OAG obtains, the Superior Court found no reason to believe that OAG would disclose it to others, and Facebook offers no basis for thinking otherwise. App. 31. In any event, because OAG is not compelling the identity of speakers who wish to remain anonymous, its subpoena will not "chill" anyone's speech even if the subpoenaed information became public. Br. 39; *Reps. Comm. for Freedom of Press*, 593 F.2d at 1058-59.

B. OAG's subpoena survives exacting scrutiny.

Even if OAG's subpoena were subject to "exacting scrutiny," it readily survives this standard. Facebook agrees that OAG has a legitimate interest in consumer protection and enforcing the CPPA. Br. 41. But Facebook argues that this interest is not implicated here because it has made no public claims about the quantity of COVID-19 vaccine misinformation it has removed or demoted. Br. 12,

18, 41, 45. That is beside the point. OAG is investigating whether Facebook has adhered to its COVID-19 vaccine misinformation policy and public statements assuring consumers in concrete and possibly misleading terms that it "prohibits" and "will remove" certain content. OAG's investigation therefore implicates not only what misinformation Facebook has demoted or removed, but also what it has knowingly failed or refused to demote or remove despite its pledges, including whether it is promoting, rather than "prohibit[ing]," this content. *See supra* pp. 10-13 & nn.16-28. The question is therefore not simply whether Facebook made truthful statements about the *quantity* of misinformation it has demoted or removed.

On appeal, Facebook suggests that its claim about its "aggressive" content moderation policy, Br. 42 (quoting OAG's Reply ISO Pet. for Enforcement 2 n.1), is mere "puffery" and too "vague" to support a CPPA violation, Br. 42 (quoting *Prager Univ. v. Google LLC*, 951 F.3d 991, 1000 (9th Cir. 2020)). Facebook never made that argument in Superior Court, and it is therefore forfeited. *See Johnson v. D.C. Dep't of Health*, 162 A.3d 808, 812 (D.C. 2017); App. 14 ("Meta does not dispute . . . that its public statements about its content moderation policies are within the scope of the CPPA"). In any event, it makes no similar claim about its actual COVID-19 vaccine misinformation policy and its many other statements that OAG cited. Br. 9-10, 42-43; *see supra* pp. 10-13 & nn.16-28. There is therefore little

doubt that at least some of its claims regarding its vaccine-misinformation policy are subject to the CPPA and can support OAG's legitimate interest.

Finally, OAG's subpoena is narrowly tailored to achieve its important interest in consumer protection. There is no "dramatic mismatch" between OAG's investigation and the information it seeks. Br. 44 (quoting *Ams. For Prosperity*, 141 S. Ct. at 2389). OAG seeks the identity of Facebook users who have posted COVID-19 vaccine misinformation as identified by Facebook to assess, among other things, how it addresses repeat offenders and those that have been publicly identified as responsible for much of the misinformation. Anonymized data will not permit OAG to make this assessment. Nor is it enough that Facebook has provided some information about content it has removed. Br. 13, 45. This information says little about Facebook's efforts where it refuses to disclose how much public content it has *failed to* demote or remove. Instead, as the Superior Court found, there is no "less intrusive means" for OAG to accomplish its investigative goals other than the subpoena at issue. App. 30.

CONCLUSION

The Court should affirm.

Respectfully submitted,

KARL A. RACINE
Attorney General for the District of Columbia

CAROLINE S. VAN ZILE
Solicitor General

ASHWIN P. PHATAK
Principal Deputy Solicitor General

/s/ Stacy L. Anderson
STACY L. ANDERSON
Senior Assistant Attorney General
Bar Number 475805
Office of the Solicitor General

Office of the Attorney General
400 6th Street, NW, Suite 8100
Washington, D.C. 20001
(202) 724-6625
(202) 741-5922 (fax)
stacy.anderson2@dc.gov

November 2022

REDACTION CERTIFICATE DISCLOSURE FORM

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 taxpayeridentification 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/ Stacy L. Anderson
Signature

22-CV-239
Case Number

Stacy L. Anderson
Name

November 17, 2022
Date

stacy.anderson2@dc.gov
Email Address

CERTIFICATE OF SERVICE

I certify that on November 17, 2022, this brief was served through this Court's electronic filing system to:

Catherine M.A. Carroll

Joshua S. Lipshutz

Keisha Stanford

Brian Hauck

/s/ Stacy L. Anderson
STACY L. ANDERSON