DISTRICT OF COLUMBIA COURT OF APPEALS

No. 22-CV-0239

META PLATFORMS, INC., APPELLANT,

v.

DISTRICT OF COLUMBIA, APPELLEE.

Appeal from the Superior Court
of the District of Columbia
(2021-CA-004450-2)

(Hon. Anthony C. Epstein, Trial Judge)

(Argued January 31, 2023 Decided September 14, 2023)

Catherine M.A. Carroll, with whom *Ronald C. Machen*, *George P. Varghese*, *Ari Holtzblatt*, and *Joshua S. Lipshutz* were on the brief, for appellant.

Ashwin P. Phatak, Principal Deputy Solicitor General, with whom *Karl A. Racine*, Attorney General for the District of Columbia at the time, *Caroline S. Van Zile*, Solicitor General, and *Stacy L. Anderson*, Senior Assistant Attorney General, were on the brief, for appellee.

Before BLACKBURNE-RIGSBY, *Chief Judge*, DEAHL, *Associate Judge*, and STEADMAN, *Senior Judge*.

Opinion for the court by *Associate Judge* DEAHL.

Concurring opinion by *Associate Judge* DEAHL at page 42.

DEAHL, *Associate Judge*: The District has subpoenaed Meta Platforms, the operator of the social media site Facebook, for documents related to Meta's enforcement of its COVID-19 misinformation policies. The District is investigating potential violations of the Consumer Protection Procedures Act, or CPPA, D.C. Code §§ 28-3901 to -3913, alleging that Meta has misrepresented to the District's consumers the degree to which it polices misinformation posted to its platform about the COVID-19 vaccine. Meta refused to comply with the subpoena, and the Superior Court issued an order enforcing the subpoena. Meta now appeals that order.

Meta raises two arguments in support of its view that the District's subpoena is unenforceable. Its first argument concerns the Stored Communications Act, or SCA, 18 U.S.C. §§ 2701 to 2711. Meta argues that § 2703 of the SCA requires the District to procure a warrant in order to compel the disclosure of the documents it seeks. Its second argument is grounded in the Constitution. Meta argues that the District's subpoena infringes on both its and its users' First Amendment rights to free speech and free association. Like the trial court, we disagree with Meta as to both points, and affirm.

I.

Superior Court Proceedings

This case arises from an ongoing investigation by Attorney General for the District of Columbia into Meta's content moderation practices. Throughout the COVID-19 pandemic, Meta made various public statements about its efforts to police the spread of misinformation on its platform. In December 2020, for example, the company announced that it would be "remov[ing] false claims that COVID-19 vaccines contain microchips, or anything else that isn't on the official vaccine ingredient list." Several months later, Meta unveiled an expansion of this policy, noting "a particular focus on pages, groups, and accounts that violate these rules." By August 2021, Meta reported that these efforts had led to the removal of 20 million items of content and over 3,000 accounts, pages, and groups for repeat violations.

The District, perceiving a mismatch between these public statements and the widespread dissemination of vaccine misinformation on Facebook, is investigating Meta's potential violations of the CPPA. That statute, which prohibits unfair and deceptive trade practices, authorizes the District to conduct "investigation[s] to determine whether to seek relief under" its provisions, including by issuing subpoenas to "compel production of records, books, papers, contracts, and other

documents." D.C. Code § 28-3910(a). Relying on this authority, the District issued a subpoena demanding the production of the following:

> 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.

This demand was eventually narrowed to only those documents related to public posts, or posts that were so widely accessible as to be functionally public.[1]

Meta refused to comply with the subpoena, and so the District brought an enforcement action in Superior Court. In that litigation, Meta principally argued that the government may compel the production of electronic communications only by procuring a warrant, citing to a provision of the SCA, 18 U.S.C. § 2703(a). The trial court disagreed with that reading of the statute. It instead reasoned that because the

[1] It is difficult to say exactly when a post to a nominally private Facebook group or Page has been so broadly disseminated that it is effectively public. The trial court charged Meta and the District with reaching an "agreement on an approach that identifies public posts in a way that protects non-public posts from disclosure and that does not impose an undue burden on Meta." Neither party challenges that aspect of the trial court's order, so we do not opine on any theoretical threshold for when a post on the internet becomes functionally public.

District is targeting only public posts, the SCA's "consent exception," § 2702(b)(3), permitted Meta to make the disclosures, and Meta was therefore required to comply with the District's valid subpoena (more on these provisions in a moment). Meta also raised a First Amendment challenge to the subpoena, arguing that compelling it to disclose the targeted documents would chill both its and its users' First Amendment rights of free speech and association. The court again disagreed, concluding that the subpoena did not infringe upon either Meta's or its users' First Amendment rights.

Meta now appeals, pressing the same two arguments that it raised before the trial court. First, it argues that the SCA precludes the government from compelling disclosure of the targeted documents via subpoena, as the SCA requires it to instead procure a warrant. Second, it argues that the subpoena violates its and its users' First Amendment rights of free speech and association. We address Meta's statutory argument concerning the proper interpretation of the SCA first, and then turn to its First Amendment challenges.

II.

The proper interpretation of the SCA is a question of law we review de novo. *Facebook, Inc. v. Wint*, 199 A.3d 625, 628 (D.C. 2019).

A. Background of the Stored Communications Act

Congress passed the SCA in 1986 to fill a perceived hole that technological advances had poked in the Fourth Amendment's protections of private communications and records. For most of our country's history, people typically kept their private communications and records in their homes or places of business, and the government generally needed a warrant supported by probable cause to seize those materials. *See Coolidge v. New Hampshire*, 403 U.S. 443, 455 (1971) (the Fourth Amendment's warrant requirement is "subject only to a few specifically established and well delineated exceptions").

The advent of email and other forms of electronic communications and storage changed that, and raised serious questions about the Fourth Amendment's applications to these new technologies. Electronic communications typically must be disclosed to third-party service providers, who then transmit messages to their intended recipients. Those third-party service providers might themselves disclose the communications to the government, offering a potentially massive end run on the Fourth Amendment's protections of private materials. *See United States v. Miller*, 425 U.S. 435, 443 (1976) ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [them] to

Government authorities."). *But see Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (declining to extend *Miller* to cell-site location information a person reveals to their wireless carrier).[2]

The SCA sought to fill that potential gap by providing "a set of Fourth Amendment-like privacy protections by statute," limiting "the ability of [service providers] to voluntarily disclose information about their customers and subscribers to the government." 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, 1212-13 (2004). Two of the SCA's provisions are particularly crucial to this appeal.

First is § 2702, which precludes service providers from disclosing their users' communications or records, subject to certain exceptions. Section 2702 states that the provider of an "electronic communication service" may not knowingly divulge "the contents of a communication while in electronic storage by that service." 18

[2] To be clear, we do not express any view about whether there is in fact any gap in the Fourth Amendment's protections of electronic communications. Courts are capable of adapting doctrinal rules to fit technological advances, but are often slow to do so. The SCA was simply Congress's attempt to address the gap it perceived.

U.S.C. § 2702(a)(1).[3] The provision then lists nine exceptions to that general prohibition, including: disclosures "to an addressee or intended recipient of" the communication, *id.* § 2702(b)(1); disclosures "with the lawful consent of the originator or an addressee or intended recipient of" the message, *id.* § 2702(b)(3); and disclosures "as otherwise authorized in [§ 2703]," discussed immediately below. *Id.* § 2702(b)(2). Section 2702(a) "broadly prohibits providers from disclosing the contents of covered communications." *Wint*, 199 A.3d at 628. But when one or more of the nine § 2702(b) exceptions apply, we have held that "the SCA is no obstacle" to compelling disclosure of communications via ordinary legal process, like subpoenas. *Facebook, Inc. v. Pepe*, 241 A.3d 248, 253 (D.C. 2020).

Second is § 2703, which confers on government entities alone the power to compel disclosure of electronic communications and records, even when no § 2702(b) exception applies. The SCA grants private parties no similar authority. Under § 2703, the government may compel via court order a narrow set of non-

[3] The SCA's strictures apply to both providers of "electronic communication services" and "remote computing services." *See* 18 U.S.C. § 2510(15) (defining "electronic communication service"), and § 2711(2) (defining "remote computing service"); *see also id.* § 2702(a)(2) (directed at remote computing services). For our purposes, the differences between these types of services are immaterial, and we refer generally to "service providers." *Cf.* Kerr, *User's Guide*, 72 Geo. Wash. L. Rev. at 1209 (advocating for "eliminating the[se] confusing categories").

content records, including a subscriber or customer's name, address, and means of payment. 18 U.S.C. § 2703(c)(2), (d). As for the contents of electronic communications, like the text of an email, the statutorily required process for government-compelled disclosure depends on how long the communication has been in electronic storage. When it has been in storage for more than 180 days, § 2703(b) permits the government to compel its disclosure so long as it provides prior notice to the user and obtains an administrative subpoena or court order provided for in § 2703(d). But when the communication has been in storage for 180 days or less, the SCA authorizes the government to compel disclosure "only pursuant to a warrant." *Id.* § 2703(a).[4]

B. *Wint*, *Pepe*, and the Parties' Competing Readings of the SCA

We have interpreted these provisions twice before, and both cases are important here. We first addressed them in *Facebook v. Wint*, where we held that

[4] The District does not invoke the SCA's more permissive processes for obtaining communications that are "more than one hundred and eighty days" old, 18 U.S.C. § 2703(b), (d), and Meta suggests that is because the 180-day line has effectively been abandoned through practice and case law. Whatever the reason, we proceed here as if the District is seeking materials that have been electronically stored for 180 days or less, even though that would seem not to be true of the vast bulk of materials that the District seeks.

§ 2702(a)'s "broad prohibition" on disclosure precludes a service provider from complying with a criminal defendant's subpoena seeking protected communications. 199 A.3d at 629-30. None of the statutory exceptions permitting disclosure applied in that case, and we concluded that "barring an applicable statutory exception, the SCA prohibits providers from disclosing covered communications," even when subpoenaed by a private party. *Id.* at 629.

We next addressed these provisions in *Facebook v. Pepe*, where unlike *Wint*, statutory exceptions did apply to permit the service provider to disclose the subpoenaed communications. 241 A.3d 248, 256 (D.C. 2020). Nonetheless, Facebook opted not to comply with the criminal defendant's subpoena in that case, highlighting statutory language providing only that it "*may* divulge" electronic communications when such an exception applies, rather than requiring it to do so. *Id.* at 257-58 (emphasis added). We disagreed and held that Facebook was required to comply with the subpoena where nothing in the SCA precluded it from doing so. *Id.* at 258. In short, because "the SCA did not authorize Facebook's refusal to comply with Mr. Pepe's subpoena," Facebook was subject to "disclosure requirements imposed by other law." *Id.* at 258.

The present case, like *Pepe*, involves communications that are exempted from the SCA's broad prohibition on disclosure. Meta does not dispute that the SCA *permits* it to comply with the District's subpoena, because the District seeks only publicly posted messages, which the parties agree fit within the SCA's consent exception to overcome the general bar on disclosure. 18 U.S.C. § 2702(b)(3). *But see infra* at 42-44 (Deahl, J., concurring) (questioning exception's application).

The parties offer competing theories about how §§ 2702 and 2703 should be read together and applied in this case. The District contends that *Pepe*'s reasoning applies with full force here, and the same result—that Meta must comply with the subpoena—follows. Recall that *Pepe* held that so long as some § 2702(b) exception to § 2702(a)'s general bar on disclosure applies, private parties can avail themselves of whatever avenues of compulsory process they have available to them, and service providers must comply with such valid process. 241 A.3d at 258. The District maintains that the same is true when a government actor subpoenas documents. In its view, § 2702(a)'s general prohibition on disclosure does not bar compliance with its subpoena because the users have consented to the disclosure of their communications by publicly posting them. *See* 18 U.S.C. § 2702(b)(3). And as in *Pepe*, the District has authority independent of the SCA to "compel production of records" that it seeks: the CPPA. *See* D.C. Code § 28-3910. Thus, Meta must

comply with the subpoena. The Superior Court adopted essentially this reasoning, positing that "[n]othing in the text of § 2702(b)(3) limits the consent exception to disclosure to non-governmental entities."

Meta counters that *Pepe* is inapplicable because the SCA applies an entirely different set of restrictions when it is the government, rather than a private party, seeking to compel disclosures. Meta contends that *Pepe* and the § 2702 exceptions are inapposite in light of § 2703's directive that "[a] governmental entity may require the disclosure . . . of the contents of a wire or electronic communication . . . *only* pursuant to a warrant." 18 U.S.C. § 2703(a) (emphasis added). This portion of the statute, it argues, imposes additional hurdles on government entities seeking electronic communications beyond those found in § 2702, and the trial court blurred the distinction between the two provisions when it granted the District's petition to enforce its subpoena. If the District or any other government entity wants access to these records, Meta concludes, it has no option but to comply with § 2703's warrant requirement.

We agree with the District's reading of the statute. The text and structure of the SCA support the District's interpretation, as we explain in Part II.C. The Act's legislative history also supports that interpretation, as we explain in Part II.D.

C. The SCA's Text and Structure

We begin with the text of the statute, which is "generally the best indication of the legislative intent." *In re B.B.P.*, 753 A.2d 1019, 1021 (D.C. 2000). As an initial matter, the District argues that the SCA does not apply to public posts at all, but instead applies only "to protect information that the communicator took steps to keep private." *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 668 (D.N.J. 2013). It might be right about that.[5] *See infra* at 44-47 (Deahl, J., concurring). *But see Facebook, Inc. v. Superior Court (Hunter)*, 417 P.3d 725, 743-44 (Cal. 2018) (concluding that the SCA "initially prohibits the disclosure of *all* (even public) communications—but that section 2702(b)(3)'s subsequent lawful

[5] As the District points out, the SCA's proscriptions of the unauthorized access and interception of electronic communications do not extend to "electronic communication[s that are] readily accessible to the general public." 18 U.S.C. § 2511(2)(g)(i); *see id.* § 2701. Meta counters that we are not concerned here with the unauthorized access or interception of electronic communications, but with disclosures of electronic communications, which are covered by different provisions: §§ 2702 and 2703. Meta's response is well-taken, but it is not wholly satisfactory. It would be a rather strange statutory regime if the SCA permitted the government (and anybody else) to "intercept" and "access" any and all public posts, while prohibiting the government from compelling disclosure of the exact same material absent a warrant (as Meta's reading of the statute would dictate). And at a broader level, it would be odd if a statutory regime meant to mimic the Fourth Amendment's protections swept so much more broadly than the Fourth Amendment itself, and protected communications that had been broadcast to the world. *See infra* at Part II.D.2. We ultimately do not resolve this broader dispute between the parties, and will assume, without deciding, that the SCA applies to public posts.

consent exception allows providers to disclose communications configured by the user to be public"). We ultimately bypass that question, though, because even assuming, as the trial court concluded, that the SCA applies to the public posts at issue here, we agree that the District's subpoena is enforceable.

As the trial court recognized, our holding in *Pepe* applies with equal force when it is the government, rather than a private party, seeking to compel disclosure of communications that fall within one of the § 2702(b) exceptions. Nothing in the text of § 2702 suggests a different result. Section 2702's consent exception to the general bar on disclosure instructs that a service provider "may divulge the contents of a communication . . . 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," drawing no distinctions based on the nature of the recipient. 18 U.S.C. § 2702(b)(3). The parties agree that this exception applies here, and as we held in *Pepe*, when the SCA permits the disclosure of electronic communications to a third party, a service provider must comply with a valid subpoena requiring such disclosure. 241 A.3d at 258.

Meta counters that Congress enshrined an entirely different set of rules for government actors seeking to compel disclosure in § 2703. In particular, it

highlights the provision's directive that "[a] governmental entity may require the disclosure" of electronic communications "only pursuant to a warrant." 18 U.S.C. § 2703(a). Thus, it claims, "a warrant is the sole—exclusive—means by which the government 'may require' disclosure of content." This textual argument gets off to a bad start because the plain text of § 2703 does not, in fact, require the government to obtain a warrant whenever it seeks to compel electronic communications. The statute requires a warrant only when communications are held in "electronic storage" by an electronic communication service provider for 180 days or less. 18 U.S.C. § 2703(a). Meta ducks this nuance by asserting "the SCA's original distinction between communications in storage for more or less than 180 days has largely been abandoned." Maybe so, but to the extent that distinction has been abandoned, it was for constitutional rather than statutory reasons. *See, e.g.*, *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir. 2010) ("[T]o the extent that the SCA purports to permit the government to obtain" emails older than 180 days "warrantlessly, the SCA is unconstitutional."); H.R. Rep. No. 114-528, at 9 (2016) (citing *Warshak* and questioning "constitutional validity" of distinction). So those authorities are no fix to the initial textual problem with Meta's statutory interpretation argument.

But the far bigger textual problem with Meta's interpretation of § 2703 is that it reads this provision in isolation, whereas "[s]tatutory interpretation is a holistic

endeavor." *Grayson v. AT&T Corp.*, 15 A.3d 219, 238 (D.C. 2011) (en banc) (citation omitted). When viewed in its broader statutory context, it becomes clear that § 2703 is an additional grant of authority permitting government actors alone to compel disclosures even when no exception to § 2702(a)'s broad prohibition on disclosure applies, not a unique restriction on government actors when a § 2702(b) exception does apply, as Meta reads it.[6]

Start with the fact that government entities are the only actors that the SCA affirmatively authorizes to compel disclosures of communications covered by § 2702(a)'s general prohibition, even when no § 2702(b) exception applies. There is no similar authorization for private parties to compel disclosures in the face of a § 2702(a) bar. So when a § 2702(b) exception applies to lift the bar on disclosure, it would make no sense if the government's additional grant of authority could be weaponized against it, and read to preclude the government from availing itself of

[6] We add a reminder that where no § 2702(b) exception applies to exempt the service provider from § 2702(a)'s general prohibitions against disclosure, then compliance with § 2703 really is the government's exclusive option for compelling disclosures. *See Wint*, 199 A.3d at 628. And even compliance with the SCA might not be good enough, as the Constitution may provide added protections, for instance, by protecting communications that are held in storage for more than 180 days in a way the SCA's plain text does not. *See Warshak*, 631 F.3d at 291 ("[T]o the extent that the SCA purports to permit the government to obtain [emails older than 180] days warrantlessly, the SCA is unconstitutional.").

the same external legal processes that private parties can avail themselves of when a § 2702(b) exception applies. Through § 2703 Congress provided the government with an additional tool to compel disclosures that no private party has; it did not erect an obstacle to disadvantage the government from compelling information that a private party could obtain. In arguing otherwise, Meta seeks to invert the asymmetry that the SCA assigns to governmental and private actors' respective abilities to compel communications, contrary to the SCA's overall scheme.

And there are further textual indications that the SCA grants the government a greater ability to compel protected communications than the average Joe, rather than less as Meta would have it. For instance, several of the § 2702(b) exceptions permit the disclosure of otherwise protected communications *only* to government entities. Service providers must disclose to the National Center for Missing and Exploited Children any communications that they become aware of which indicate a violation of various laws against child pornography. 18 U.S.C. § 2702(b)(6) (referencing 18 U.S.C. § 2258A's mandatory reporting requirements). Those disclosures are required by law, whether or not the government has a warrant. Providers also may disclose, but only to "a law enforcement agency," any communications "inadvertently obtained by the service provider" that "appear to pertain to the commission of a crime." *Id.* § 2702(b)(7). They may disclose only

"to a governmental entity" communications that trigger a good faith belief "that an emergency involving danger of death or serious physical injury" is afoot and requires "disclosure without delay" to avoid hazardous results. *Id.* § 2702(b)(8).[7]

When §§ 2702 and 2703 are read together, their import is clear: § 2702(a) broadly precludes service providers from disclosing the contents of their users' communications, and unless some § 2702(b) exception applies, the government alone can compel the disclosure of those communications, and can do so only by complying with § 2703's strictures. But where a § 2702(b) exception does apply to remove § 2702(a)'s bar on disclosure, then the government and private parties alike can avail themselves of the "mandatory disclosure requirements imposed by other law," *Pepe*, 241 A.3d at 258, like the CPPA's subpoena powers the District invokes in this case. Section 2703(a) cannot sensibly be read as a bar on the government's ability to compel disclosures that private parties could compel, when it is instead an additional grant of authority to the government that private parties lack. *See id.* at

[7] We have not surveyed the field to examine whether there are some compulsory reporting requirements in state or federal laws that might require disclosure of materials that fall within these §§ 2702(b)(7) or (b)(8) exceptions. If there are, then our reasoning in *Pepe* would apply there as well, so that service providers are not only permitted to, but must, comply with those requirements (barring some constitutional hurdle to disclosure).

257 (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").

Meta protests that § 2703 has its own consent exception (applicable only to non-content records), which it argues would be "wholly superfluous" under our reading of the statute, as § 2702 also has a consent exception for non-content records. *Compare* 18 U.S.C. § 2703(c)(1)(C) *with id.* § 2702(c)(2). That's wrong. The § 2702(c)(2) consent exception removes a bar or disability on the service provider that would otherwise preclude them from disclosing such records, whereas § 2703(c)(1)(C) is an affirmative authorization permitting the government to compel disclosure when the user consents to it. Put another way, when a § 2702 exception applies, the government—like any other party—can compel disclosure only if they can point to some authority that allows them to do so; here the District points to its authority to subpoena records and compel disclosures in furtherance of a CPPA investigation. *See* D.C. Code § 28-3910. Whereas when § 2703(c)(1)(C) authority applies, the government need not point to some external source of authority that permits it to compel disclosure of non-content records—the provision itself provides that. There is no superfluity.

Meta next counters that our reading of the SCA's text would make us "the sole outlier" among courts to have considered this issue. That is a rhetorical sleight of hand. Meta points to just two decisions from trial courts that it suggests support its view, and only one of them even arguably does. In truth, Meta's position here is so novel that there are simply not any appellate court decisions addressing it, and the trial court decisions that Meta cites give us no pause.

Meta first points to *FTC v. Netscape Communications Corp.*, 196 F.R.D. 559 (N.D. Cal. 2000). That case is inapposite because there was no suggestion in it that a § 2702(b) exception applied to the communication sought to be compelled via agency subpoena. *Netscape* thus stands for the unremarkable position that where no § 2702(b) exception applies, the government's sole recourse for compelling disclosure is to comply with § 2703's strictures. We agree with that—we held likewise in *Wint*, 199 A.3d at 629—but it is not the issue before us.

Meta's other authority is closer to the mark, but unpersuasive. *See People v. Harris*, 949 N.Y.S.2d 590 (N.Y. Crim. Ct. 2012). *Harris* involved a subpoena issued by a District Attorney's Office seeking tweets publicly posted from a Twitter account, allegedly operated by a criminal defendant, over the course of more than 100 days. *Id.* at 591. The trial court enforced that subpoena as to all but a single

day's tweets, because only that day's tweets were "less than 180 days old," and therefore the court concluded they could be compelled only by a search warrant. *Id.* at 596, 598. The court did not address whether the tweets fell within any § 2702(b) exception to the SCA's general bar on disclosure, and there is no indication that any party raised that point. It did not grapple with the statutory structure of the SCA, as discussed above. And unsurprisingly the parties and the court alike were more focused on (1) the 100-plus days of tweets that fell outside the 180-day window and therefore did not require a warrant than they were with the single day of tweets that fell within it, and (2) the attendant question of whether Twitter users' themselves had standing to quash the subpoena served on Twitter. *Id.* at 593. As to the remaining single day's tweets, the court offered nothing resembling persuasive statutory analysis, stating only that "the government must obtain a search warrant for the December 31, 2011 tweets." *Id*. at 596. That conclusion is some support for Meta's view here, but it is anemic, and it gives us no cause to reconsider our own statutory analysis.

D. The SCA's Legislative History

The legislative history supports our reading of the SCA as well. As previously explained, the SCA is roughly meant to extend Fourth Amendment protections to

electronic communications and the like. It seeks to neutralize the incident of technology that things like emails are typically disclosed to third-party service providers—thereby calling the Fourth Amendment's protections into doubt—for purposes of transmission. There are two features of Meta's proposed interpretation of the SCA that do not square with this history: (1) it would extend Fourth Amendment-like protections to public disclosures, which would ordinarily receive slim-to-no Fourth Amendment protections; and (2) the protections it extends would not actually belong to the individual users themselves, but instead would belong to the service providers. We elaborate below on why neither feature aligns with the legislative history, then we respond to Meta's counterpoints to it, but before all of that, we detail the legislative history itself.

1. The Legislative History in Broad Strokes

The SCA was enacted as part of the Electronic Communications Privacy Act (ECPA) of 1986, Pub. L. No. 99-508, which predates the World Wide Web by several years. As one might expect, applying the SCA to modern technology is often like cramming a square peg into a round hole. *See generally* Orin Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 378, 390-410

(2014) (detailing a variety of reasons "why the [ECPA] is based on outdated assumptions").

As the Senate Report accompanying the legislation explained: "When the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the 'houses, papers, and effects' protected by the fourth amendment." S. Rep. No. 99-541, at 1-2 (1986). Because of technological developments, however, Congress believed that the Constitution's protections had become "hopelessly out of date." *Id.* at 2. Unlike one's physical property, electronic records and communications are frequently in the possession and control of third-party service providers, which arguably renders them "subject to no constitutional privacy protections." *Id.* at 3 (citing *Miller*, 425 U.S. 435). "Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities as well as unauthorized private parties." *Id.* The SCA sought to fill this perceived gap in the Fourth Amendment's protections:

> [T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

Id. at 5; *see also* H.R. Rep. 99-647, at 19 ("Additional legal protection is necessary to ensure the continued vitality of the Fourth Amendment.").

2. Meta Would Expand the SCA Far Beyond the Fourth Amendment

This Congressional intent—to eliminate an instance of legal arbitrage by applying the Fourth Amendment's protections to a new technology via statute—comports with our reading of the SCA's disclosure provisions. Communications blasted in public fora, for all to see or hear, generally are not protected by the Fourth Amendment, putting the nicety of third-party electronic transmitters of communications aside. "What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." *Katz v. United States*, 389 U.S. 347, 351 (1967); *accord Biles v. United States*, 101 A.3d 1012, 1024 (D.C. 2014). So it would make little sense to extend the SCA's protections to such communications.

Meta's interpretation would do just that, despite the fact that publicly broadcast communications have no shelter in the Fourth Amendment itself. That would expand the SCA far beyond the Fourth Amendment protections that Congress sought to mimic. To the contrary, the House and Senate Reports affirmatively indicate that Congress did not intend for the SCA's protections to cover content that

the user took no steps to keep private. For example, both reports include extended discussions of electronic bulletin board systems (BBS)—"early analogues to the social media platforms at issue here." *Hunter*, 417 P.3d at 739. As one article describes this archaic technology, dialing into a BBS was akin to "visit[ing] the private residence of a fellow computer fan electronically. BBS hosts had converted a PC . . . into a digital playground for strangers' amusement." Benj Edwards, *The Lost Civilization of Dial-Up Bulletin Board Systems*, The Atlantic (Nov. 4, 2016). These early (now anachronistic) digital meeting spaces could be configured as either "public or semi-public in nature, depending on the degree of privacy sought by users." S. Rep. 99-541, at 9. Only the latter, non-publicly accessible BBSs were intended to fall within the SCA's protections. As the Senate Report puts it, the SCA's protections do not apply where a BBS "does not require any special access code or warning to indicate that the information is private. To access a communication in such a public system is not a violation of the Act, since the general public has been 'authorized' to do so by the facility provider." *Id.* at 36; *see also Snow v. DirectTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir. 2006) ("[T]he requirement that the electronic communication not be readily accessible by the general public is material and essential to" the SCA's scope of protections).

Meta counters that this discussion of BBSs relates only to the SCA's provisions prohibiting the unauthorized access and interception of electronic communications, or what is effectively the SCA's anti-hacking provision, 18 U.S.C. § 2701. That is not quite right. BBSs feature heavily in the House Report's discussion of § 2702, one of the two disclosure provisions we are concerned with here. Specifically, after noting that a user can waive the SCA's protections by consenting to their communications' disclosure, the report states that "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 communication." H.R. Rep. 99-647, at 66; *see also* 18 U.S.C. § 2702(b)(3). In other words, Congress clearly contemplated that publicly broadcast communications would not be protected under § 2702's broad prohibition on disclosure. While Meta is correct that BBSs were not specifically discussed in relation to § 2703, what is missing from the legislative history is any indication whatsoever that Congress intended to preclude the government from obtaining, via subpoena or other compulsory process, materials that were not protected under § 2702 in the first place.

3. Meta Would Leave the SCA's Protections to Service Providers' Discretion

There is another feature of Meta's statutory interpretation that is at odds with the SCA's legislative history. That history evinces Congress's intent to confer upon individual users of electronic services Fourth Amendment-like protections. But recall that Meta's view is not that its users have any right to prevent it from complying with the subpoena in this case—because a § 2702(b) exception applies, Meta acknowledges that it is free to comply with the subpoena. Meta's view is instead that it alone decides whether it will comply with, or defy, the subpoena, entirely at its own discretion. Under that view, the SCA in fact confers no protections to Meta's users when a § 2702(b) exception applies, save for those that their service provider's good graces—and maybe the terms of service—afford them. There is simply nothing in the SCA's legislative history that suggests Congress meant to enshrine such service-provider-centric protections.[8] To the contrary, by

[8] We do not mean to overstate the point, because users could enter into private agreements with their service providers—like agreeing to a social media site's terms of service—that preclude disclosure of their private information. It might be a sensible enough regime to leave users' privacy interests to such agreements, and we do not opine on that. *Cf.* Orin Kerr, *Terms of Service and Fourth Amendment Rights* (Jan. 29, 2023), U. Penn. L. Rev. (forthcoming), *available* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4342122; https://perma.cc/7MDY-RJ7B (arguing that terms of service do not generally alter Fourth Amendment rights). We conclude only that there is no indication in the

seeking to mirror the Fourth Amendment's protections, the legislative history evinces Congress's intent to protect individual users *from* the discretionary disclosure choices that their service providers might otherwise make.

It is true that when a § 2702(b) exception applies to permit the disclosure of otherwise protected communications, the statutory text itself says only that the provider "*may* divulge the contents of a communication," which would generally connote some degree of discretion, consistent with Meta's view. But we have already explained in *Pepe* why that generally permissive statutory language is a bit of a mirage: "[T]he subdivisions in § 2702 where 'may' appears are framed not as a grant of discretionary power but as a special exception to a general prohibition. In such a context all 'may' means is that the actor is excused from a duty, liability, or disability," it does not "suggest unlimited discretion." 241 A.3d at 258 (cleaned up) (first quoting *Hunter*, 417 P.3d at 751, then quoting *Zadvydas v. Davis*, 533 U.S. 678, 697 (2001)). And once the § 2702(a)'s general prohibition on disclosure is lifted, via a § 2702(b) exception, the provider's discretion is subject to "disclosure requirements imposed by other law." *Id.*

---

legislative history that this is the regime that Congress had in mind when passing the SCA.

4. Meta's Counterpoints Are Unpersuasive

Meta offers two counterpoints from the legislative history, but neither is persuasive. First, it notes that when discussing § 2703, the Senate Report states that "[a] government entity *can only* gain access to the contents of such an electronic communication pursuant to a warrant." S. Rep. 99-541, at 38 (emphasis added). Similarly, the House Report describes § 2703 as providing "the procedures the government *must use* before it can obtain access to the contents of any electronic communication held by a provider of a remote computing service." H.R. Rep. 99-647, at 67 (emphasis added). But while Meta argues that these statements "could not be more clear," they in fact do not contemplate communications that are unprotected by § 2702 in the first place (owing to the applicability of § 2702(b) exception). Quite the opposite. The premise underlying these discussions was "that the contents of [the] message in storage were protected by the Fourth Amendment," H.R. Rep. 99-647 at 68, and Congress was of the correct understanding that publicly disclosed communications received no such Fourth Amendment protections, as the history detailed above makes clear. This history thus supports our view, that where communications are not protected by § 2702's anti-disclosure provisions in the first place, § 2703's warrant requirement does not apply.

Next, Meta argues that applying § 2702's exceptions to cases involving government subpoenas ignores Congress's stated intent to "guard against the arbitrary use of Government power to maintain surveillance over citizens." S. Rep. 99-541, at 1. That was certainly Congress's intent, but our reading of the statute comports with rather than ignoring it. As discussed, it was well established at the time of the SCA's enactment that the Fourth Amendment generally does not protect the privacy of information that an individual has broadcast to the public. *Katz*, 389 U.S. at 351. That describes the electronic communications at issue in this case. There is nothing arbitrary about giving the government the ability to compel the disclosure of such publicly broadcast communications in much the same way that a private citizen might do. *Pepe*, 241 A.3d at 258. It would seem far more arbitrary to preclude the government from compelling disclosures that any private citizen might extract. Meta points us to nothing in the legislative history to suggest that Congress meant to put the government in an inferior position, vis-à-vis private parties, to compel such disclosures. And we detect no hint of that notion in the legislative history ourselves.

* * *

In summary, the SCA does not authorize a service provider's refusal to comply with valid legal process seeking material that a § 2702(b) exception permits it to divulge. *Pepe*, 241 A.3d at 258. Because the SCA permits Meta's compliance with the District's valid subpoena, it must comply, as there "is no reason to think the SCA . . . preempts laws that require disclosures the SCA expressly permits." *Id*. Section 2703 cannot sensibly be read to uniquely inhibit the government's ability to compel disclosures that any private party could compel, as Meta contends. The SCA's text, structure, and legislative history point to the opposite conclusion: § 2703 was a unique grant of authority to the government—one granted to no private party—to override § 2702(a)'s broad prohibition in certain circumstances, not a unique disability on the government when a § 2702(b) exception already applies to lift that broad prohibition. Meta's contrary view would stand that statutory scheme on its head.

III.

We now turn to Meta's argument that the District's subpoena impermissibly intrudes on both its and its users' First Amendment rights of free speech and association.

We begin by laying some legal groundwork. A court will ordinarily enforce an investigative subpoena so long as it meets the three-prong test announced in *United States v. Morton Salt Co.*, 338 U.S. 632, 652-53 (1950). Under that test, "[w]e consider only whether [1] 'the inquiry is within the authority of the agency, [2] the demand is not too indefinite and [3] the information sought is reasonably relevant.'" *Resol. Tr. Corp. v. Thornton*, 41 F.3d 1539, 1544 (D.C. Cir. 1994) (quoting *Morton Salt*, 338 U.S. at 652). There is no dispute, and we agree, that this test is satisfied here: (1) the District, through its Office of the Attorney General, is charged with enforcing the CPPA and may "subpoena witnesses" and "compel production of records" under its investigative authority to do so, D.C. Code § 28-3910(a); (2) its demands are not indefinite; and (3) the information it seeks to compel is reasonably relevant to its investigation.

But Meta argues that *Morton Salt* does not apply here, because where compelled disclosures seriously implicate First Amendment interests, government subpoenas may face more exacting judicial scrutiny. The seminal case for this proposition is *NAACP v. Alabama ex rel. Patterson*, 357 U.S. 449 (1958), which involved an attempt by Alabama's attorney general to compel the disclosure of the NAACP's membership lists. *Id.* at 452. The NAACP refused to comply, and it was held in civil contempt and fined $100,000. *Id.* at 453-54. The Supreme Court of the

United States reversed, reasoning that Alabama's investigation into the NAACP "entail[ed] the likelihood of a substantial restraint upon the exercise by petitioner's members of their right to freedom of association," and that Alabama had failed to demonstrate an interest "which is sufficient to justify the deterrent effect." *Id.* at 462-63. The Court more recently described this "exacting scrutiny" standard as requiring "a substantial relation between the disclosure requirement and a sufficiently important governmental interest." *Ams. for Prosperity Found. v. Bonta*, 141 S. Ct. 2373, 2383 (2021) ("*AFPF*") (quoting *Doe v. Reed*, 561 U.S. 186, 196 (2010)).[9]

But that more recent decision in *AFPF* did not suggest that all government subpoenas are doomed under the exacting scrutiny standard, regardless of the nature of the information sought. Rather, the Supreme Court indicated that compelled disclosures need only satisfy this standard when "First Amendment activity is chilled—even if indirectly." *Id.* at 2384. When it is not, the far more deferential

[9] Meta suggests in a single footnoted sentence that because the District's subpoena seeks a "content-based disclosure," it should be subject to strict, rather than merely exacting, judicial scrutiny. But a majority of the Supreme Court recently rejected that more demanding standard in *AFPF*. *See* 141 S. Ct. at 2383 (Roberts, C.J.) (three justice plurality employing exacting scrutiny); *see id.* at 2396 (Sotomayor, J., dissenting) (agreeing with the plurality that exacting scrutiny applies). Meta makes no actual argument as to why that majority view should not control here, so we apply it.

Morton Salt standard continues to govern our review. A party such as Meta claiming a First Amendment privilege bears the burden of "demonstrat[ing] that enforcement of the discovery requests will result in . . . consequences which objectively suggest an impact on, or 'chilling' of, the members' associational rights." *Perry v. Schwarzenegger*, 591 F.3d 1147, 1160 (9th Cir. 2010) (citation omitted). Only after this prima facie showing do we consider if a subpoena satisfies exacting scrutiny. *Id.* at 1161; *accord In re Motor Fuel Temperature Sales Pracs. Litig.*, 641 F.3d 470, 488 (10th Cir. 2011) ("[T]he party claiming a privilege always bears the initial burden of establishing the factual predicate for the privilege.").

For the reasons that follow, we conclude that Meta has not shown that the District's subpoena, which seeks information related to publicly accessible content generated by its users, will result in chilling Meta's free speech or associational rights. As to Meta's users, we assume the exacting scrutiny standard applies, but conclude that the District has demonstrated that its subpoena is "narrowly tailored to the government's asserted interest." *AFPF*, 141 S. Ct. at 2383. We therefore hold that enforcing the District's subpoena does not violate the First Amendment.

A. Meta's Own First Amendment Rights

We begin with Meta's claim that the District's subpoena impermissibly intrudes upon its own First Amendment rights by "prob[ing] and penaliz[ing]" its ability to exercise editorial control over the content that is disseminated through its platform. The trial court disagreed, concluding that even if the First Amendment protects the ability of a private social media company to make unfettered content moderation decisions,[10] enforcing the District's subpoena would not chill Meta from engaging in that activity, so that exacting scrutiny is unwarranted. We agree.

At its core, Meta's argument boils down to two assertions: that the District's investigation (1) is really just an attempt to "pressure Meta into changing how it exercises [its] protected editorial control over its platform"; and (2) that government scrutiny of its practices more generally will lead to a chilling of the company's speech.

---

[10] It is far from clear that it does. Federal courts are sharply divided—in multiple senses of the phrase—on the point. *Compare NetChoice, LLC v. Attorney General*, 34 F.4th 1196, 1210 (11th Cir. 2022) (holding that the First Amendment protects a social media platform's right to moderate user-generated content as it sees fit), *with NetChoice, LLC v. Paxton*, 49 F.4th 439, 445 (5th Cir. 2022) (holding that it does not, "reject[ing] the idea that corporations have a freewheeling First Amendment right to censor what people say"). The District does not press the issue, however, so we assume without deciding that this First Amendment right does exist.

On the first point, we disagree with Meta's characterization of the District's investigation. As the subpoena itself states, the District is investigating only whether Meta's "*representations* regarding efforts to prevent and remove vaccine misinformation from the Facebook platform" violate the District's consumer protection statute, the CPPA. There is no suggestion that the District is investigating whether Meta's moderation policies or efforts to police them were unlawful or insufficient in themselves (except to the extent that they belie Meta's representations). The District has disclaimed any interest in regulating Meta's editorial judgment when it comes to its content moderation, and Meta's reply brief expressly denies accusing the District of acting in bad faith. This was a prudent concession. While it is certainly possible for an otherwise valid government investigation to be launched on pretexutal grounds, Meta points to no evidence that this is the case here. *See Dep't of Com. v. New York*, 139 S. Ct. 2551, 2573–74 (2019) (emphasizing that a "strong showing of bad faith or improper behavior" is required before inquiring whether an agency is acting pretextually (citation omitted)).

As to Meta's argument that the District's subpoena (even if issued as part of a legitimate investigation) nonetheless chills its speech, we again disagree. To reiterate, the only speech that is being targeted by the District's investigation are

Meta's public statements regarding the company's content moderation practices, which the District alleges were deceptive and in violation of the CPPA. If those allegations are true, then an enforcement action under the CPPA would pose no constitutional problem at all, as the First Amendment "does not prohibit the State from insuring that the stream of commercial information flow cleanly as well as freely." *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.*, 425 U.S. 748, 772 (1976). In other words, even if content moderation is itself protected speech, fraudulent misrepresentations regarding a company's moderation practices is not.

Meta tries to take this argument a step further, claiming an investigation into its statements about its content moderation practices might indirectly chill those practices themselves. "[J]ust as a subpoena demanding notes from an editorial board meeting would risk chilling a newspaper's editorial rights," Meta argues, so too does the subpoena here threaten its "exercise of editorial control." The problem with that analogy is that Meta not only made its content moderation policies publicly available, it then widely touted the actions that were supposedly taken pursuant to those policies; indeed, those public statements were the basis for the District's investigation. To piggyback on the editorial board analogy, if the newspaper itself had published an account of its editorial policies and decisions, and it turned out to

be potentially fraudulent in some way, it would not chill the newspaper's exercise of editorial control to investigate whether the newspaper's public statements on that topic were false. Meta offers no theory for how a subpoena targeting documents that tangentially relate to this entirely public information risks any chilling of its speech, and we likewise discern none.

B. Meta's Users' First Amendment Rights

Meta also argues that enforcing the District's subpoena would chill the First Amendment rights of its users. In essence, its theory is that forcing Meta to identify the users whose posts were removed under the company's COVID-19 misinformation policy "associate[s]" those users with "speech that [the District] views as undesirable." That association, Meta argues, risks deterring these users from engaging in future online discussions of controversial topics. *See Talley v. California*, 362 U.S. 60, 65 (1960) ("[I]dentification and fear of reprisal might deter perfectly peaceful discussions of public matters of importance."). We seriously doubt that. The District seeks disclosures related to public posts, and the users who made those posts have already openly associated themselves with their espoused views by publicly posting them to Facebook. While we doubt exacting scrutiny

should apply here, we will assume that it does for the sake of argument, and conclude that the District's subpoena nonetheless passes constitutional muster.

Recall that exacting scrutiny examines the fit between the importance of the government's interest and the means used to realize that interest. "To withstand this scrutiny, the strength of the governmental interest must reflect the seriousness of the actual burden on First Amendment rights." *AFPF*, 141 S. Ct. at 2383 (quoting *Doe*, 561 U.S. at 196). More concretely, there must be "a substantial relation between the disclosure requirement and a sufficiently important governmental interest, and . . . the disclosure requirement [must] be narrowly tailored to the interest it promotes." *Id.* at 2385 (citations omitted).

The District's subpoena satisfies both of these requirements. The CPPA "establishes an enforceable right to truthful information from merchants about consumer goods and services that are or would be purchased, leased, or received in the District of Columbia." D.C. Code § 28-3901(c). And its list of prohibited trade practices includes instances where a company "misrepresent[s] . . . a material fact which has a tendency to mislead." *Id.* § 28-3904(e). While the merits of the District's investigation are not presently before us, it seems plausible at first blush that false or misleading statements regarding a social media company's attempts to

control the spread of COVID-19 misinformation might run afoul of this statute. As a result, we are satisfied that any First Amendment impact resulting from the District's investigation is in service of a sufficiently important government interest. Indeed, as *AFPF* itself held, "[i]t goes without saying that there is a 'substantial governmental interest[] in protecting the public from fraud.'" 141 S. Ct. at 2386 (quoting *Vill. of Schaumburg v. Citizens for a Better Env't*, 444 U.S. 620, 636 (1980)).

Meta acknowledges that the District has a "legitimate interest in consumer protection in general." It nonetheless argues that such an interest is not implicated here, where Meta's public statements about content moderation were mere "puffery" and therefore non-actionable under the CPPA. But commercial puffery is non-actionable because it consists of statements whose "truth or falsity . . . cannot be precisely determined," such as a sign in a storefront window promising "Satisfaction Guaranteed." *Pearson v. Chung*, 961 A.2d 1067, 1076 (D.C. 2008) (quoting *Tietsworth v. Harley-Davidson, Inc.*, 677 N.W.2d 233, 245 (Wis. 2004)). This sort of general assertion, incapable of measurement, is unlikely to lead reasonable consumers astray and therefore cannot be the basis for a CPPA violation. *Id.* But that does not describe Meta's public statements about its COVID-19 misinformation policy. Meta claimed that it removed 20 million items of content and over 3,000

user accounts as a result of enforcing that policy. These are not the "[l]ofty but vague" statements that can be chalked up to puffery. *See Prager Univ. v. Google LLC*, 951 F.3d 991, 1000 (9th Cir. 2020). They are instead quite detailed, quantifiable, and capable of verification.

As to the fit between that government's interest and the scope of the District's investigation, we likewise conclude that the subpoena—now that it has been limited to documents relating to publicly accessible posts—is sufficiently tailored. Though Meta claims that the District's subpoena could have pursued "less intrusive alternatives," such as aggregated or anonymized data,[11] some of the statements that are the target of the District's investigation concern the company's actions regarding repeat offenders and individuals publicly identified as major purveyors of COVID-19 misinformation. The investigation focuses not on the users spreading misinformation or the specific content of their public posts, but on Meta's statements

[11] The trial court's order does not require Meta to "unmask" any anonymous users, as it requires Meta to produce "only the identities that these users themselves employed in public posts." Meta counters that even that order might "chill protected speech by disclosing users to the government who identified themselves only to 'private groups.'" But recall that these groups are only nominally private, and the trial court's order targets information regarding posts that were spread so widely as to be functionally public. It is hard to see how a user who broadcasts their posts so widely would be chilled by disclosure here (when any recipient of the broadcast could have disclosed the posts to the government themselves).

about its regulation of that misinformation. The Superior Court found there is not a "less intrusive means" for the District to carry out this investigation than the subpoena at issue, and we likewise see none. Accordingly, because the subpoena is appropriately tailored to serve the government's interest, and that interest is sufficiently important, it satisfies exacting scrutiny.

IV.

For the foregoing reasons, the judgment of the Superior Court is affirmed.

So ordered.

DEAHL, *Associate Judge*, concurring: I am in full agreement with the court's opinion and write separately to address two issues it rightly bypasses. First is whether § 2702(b)(3)'s consent exception actually applies on the facts of this case. Second, taking a step back, is whether the SCA's protections apply to publicly posted messages at all. I think both of those questions should be answered in the negative, which would lead to the same result the court reaches: Meta must comply with the District's subpoena.

First, on the question of consent, I adhere to a general rule of thumb when trying to figure out if somebody consents to something: You ask them. Here, the users whose posts are targeted by the District's subpoena have not been asked whether they consent to disclosure to the government, and so I find it artificial to say they have consented to such disclosure. The trial court reasoned to the contrary, that "when a user posts content on Facebook that is generally accessible to the public, the user implicitly consents to disclosure." While that might be a fair inference if the posts remained public, the posts at issue here have all been removed, so I see no reason to conclude that any consent to disclosure endures. People are generally free to withdraw consent and might do so by, for instance, removing or restricting access to a once-public post. *See Ford v. United States*, 245 A.3d 977, 984-85 (D.C. 2021) (recognizing ability to withdraw or revoke consent to a search). The fact that the posts at issue here are no longer public would preclude me from inferring any present consent to disclosure. Nonetheless, Meta does not challenge this aspect of the trial court's ruling, and so I agree with the opinion for the court that this point has been conceded. *Supra* at 11-13.

To be sure, a person who publicly posts something opens themselves up to the risk—really, the high likelihood when it comes to popular social media sites—that some third party will save their post for posterity and render any attempt to delete it

from public viewing futile. But that is just to say that third parties generally may do what they will with publicly disclosed communications, which is quite different from saying the user consents to whatever they do. And a service provider is not free to do what they want with the communication if the SCA's protections apply to it (an important caveat discussed next): they are constrained by the statute, and where the statute requires the user's consent to disclosure, I do not think that eternal consent can be fairly inferred from the fact that a person once publicly posted something.

Second, I agree with the District that the SCA does not apply to public posts in the first place,[1] so my above concern with the consent exception's application is an entirely academic point here. The SCA was enacted to "protect electronic communications that are configured to be private." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002). When read as a whole, and in light of the legislative history discussed extensively in the court's opinion, the SCA's apparent

[1] The court correctly does not reach this weighty issue because it is obviated by Meta's concession that the consent exception applies. I note that, in advancing its view that the SCA does not protect public posts, the District places too much weight on 18 U.S.C. § 2511(2)(g)(i), which it suggests is an unambiguous standalone textual basis for concluding that the SCA does not apply to public posts. It is not. Meta correctly counters that this provision concerns the intercept or access of electronic communications, not their disclosure. Still, the provision is some evidence that the SCA was not meant to reach public posts, and the Act's overall structure and legislative history provide much more evidence for that conclusion.

"purpose is to protect information that the communicator took steps to keep private." *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 668 (D.N.J. 2013); *Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir. 2006) ("[T]he requirement that the electronic communication not be readily accessible by the general public is material and essential to" the scope of the SCA's protections.).

When a person publicly posts a message for the world to see, it falls outside of the SCA's protections altogether. In that case, the service provider is best seen as providing a public platform for a user to broadcast a message, rather than acting as an "electronic communication service," a phrase the statute seems to use to refer to a third-party transmitter of otherwise private communications.

This reading of the SCA makes sense. The SCA was meant to effectively neutralize the undesired but necessary disclosure of private communications to third-party service providers; it is not as if the user wants to share their communications with service providers, so much as they are necessary conduits for relaying messages to their intended recipients. The SCA steps into that relationship to dictate that the disclosure to a third-party service provider merely for the purposes of transmitting the message is a non-event, and should not affect the user's privacy interests in their communications that might otherwise be deemed private. But when a user blasts a

message for the world to see, the service provider does not act merely as a necessary transmitter of that communication, but can itself be seen as a recipient of it (just like everybody else). The third-party transmittal problem that is the SCA's raison d'être no longer exists. In that situation there is no Fourth Amendment gap for the SCA to fill, so it makes little sense to extend the SCA's protections to it.

My view admittedly faces a textual hurdle, which is that nothing in the statutory definitions of "electronic communication" or "electronic communication service" expressly says that the communication at issue must be a private one. *See* 18 U.S.C. § 2510(12), (15). Those capacious definitions in fact suggest otherwise. But that is unsurprising given that the SCA was passed in 1986 and there simply were no platforms for publicly posting electronic messages for the world to see, at least not on anywhere near the scale of what is available today. The issue was not on the forefront of legislators' minds. The closest analogues to social media platforms at the time were fairly obscure electronic bulletin board systems, which were analogous in only the barest of ways, and the limited legislative history on those suggests that Congress did not mean for the SCA's protections to extend to publicly configured posts. *See* S. Rep. 99-541, at 36 ("To access a communication in such a public system is not a violation of the Act, since the general public has been 'authorized' to do so.").

The SCA is antiquated and could no doubt use a legislative update, but in the meantime courts should read its provisions in a way that makes sense of the entire statutory scheme, while cognizant of just how much has changed in the nearly-four decades since it was passed. Doing that leads me to conclude that the SCA's protections do not extend to public posts, and the court should say so if a more appropriate occasion ever arises.