No. 20-727

In the Supreme Court of the United States

FACEBOOK, INC.,
Petitioner,

v.

PERRIN AIKENS DAVIS, ET AL.,
Respondents.

On Petition for Writ of Certiorari to the United States Court of Appeals for the Ninth Circuit

RESPONDENTS' BRIEF IN OPPOSITION

NEIL K. SAWHNEY
GUPTA WESSLER PLLC
100 Pine St., Suite 1250
San Francisco, CA 94111
(415) 573-0336
neil@guptawessler.com

MATTHEW W.H. WESSLER
Counsel of Record
GUPTA WESSLER PLLC
1900 L St. NW, Suite 312
Washington, DC 20036
(202) 888-1741
matt@guptawessler.com

Counsel for Respondents
(additional counsel listed on inside cover)

February 11, 2021

STEPHEN G. GRYGIEL
GRYGIEL LAW, LLC
301 Warren Ave., # 405
Baltimore, MD 21230
(410) 617-8945
sgrygiel@silvermanthompson.com

JAY BARNES
SIMMONS HANLY CONROY
One Court St.
Alton, IL 62002
(618) 693-3104
jaybarnes@simmonsfirm.com

DAVID A. STRAITE
KAPLAN FOX &
KISHEIMER LLP
850 Third Ave.
New York, NY 10022
(212) 687-1980
dstraite@kaplanfox.com

QUESTION PRESENTED

Whether an entity that secretly, and without consent, duplicates and redirects to itself an internet user's communication with a website is a "party to the communication" under the Wiretap Act, 18 U.S.C. § 2511(2)(d).

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and legislative materials

Other authorities

INTRODUCTION

This case involves secret, nonconsensual tracking practices that Facebook discontinued a decade ago, and that have been outstripped by intervening technological and legal developments. It is, in short, a relic of a previous internet age.

As it does now, in 2010, Facebook made money by tracking and collecting information about its billions of subscribers and then charging advertisers to target those subscribers based on their individualized profiles and sophisticated, proprietary inferences about their personalities and preferences. Facebook promised its subscribers that it would not track their personally identifiable data unless they were logged into their Facebook accounts.

That was a lie. Starting in April 2010, the company installed hidden source code on other, non-Facebook websites to duplicate and acquire subscribers' communications with those websites—even when the subscribers were *logged out* of their Facebook accounts. And Facebook did so without their knowledge or consent.

Facebook kept up the deception until September 2011, when the Wall Street Journal published the results of an investigation revealing that, even when "you are logged out, Facebook still knows and can track every page you visit." The public uproar was immediate. So was Facebook's retreat: Soon after the revelations of its secret tracking, Facebook ended its unlawful practices and changed its disclosures to better inform subscribers about its data collection when they are logged out of their Facebook accounts. The internet did not break when users were given back this limited control over their privacy, and Facebook continued to grow.

This action was filed by Facebook subscribers who were illegally surveilled during that 18-month period almost a decade ago. The Ninth Circuit eventually allowed eight of the plaintiffs' claims to proceed past the pleading stage. Facebook's petition here involves only one of these claims, arising under the Wiretap Act. That law prohibits the nonconsensual interception of an electronic communication by someone who is not a "party to the communication." 18 U.S.C. § 2511(2)(d). The plaintiffs' allegations that Facebook secretly installed source code that duplicated their communications to other websites and transmitted them to Facebook's servers without their knowledge or consent, the Ninth Circuit held, plausibly stated a claim for liability under the statute.

Facebook urges that this Court grant review to address what it says are the "sweeping practical consequences" of the decision below. Facebook claims that the Ninth Circuit's conclusion that Facebook is not a "party" within the meaning of the Wiretap Act here will "upend common internet practices," "stifle future innovation," and "chill the creativity that allows the internet to flourish." It will, in Facebook's telling, all but end the internet as we know it.

Nothing could be further from the truth. Despite Facebook's hyperbole, the decision below will have little practical significance outside this case. Although barely mentioned in Facebook's petition, the Wiretap Act also exempts from liability any interception made with a party's "prior consent." Nearly all of Facebook's peers attempt to seek consent before tracking their users. Indeed, *Facebook itself* takes the position that it currently obtains sufficient consent to track its subscribers when they are logged out. And, starting last year, California

state law requires every internet company to get consent from users before collecting personal information.

In light of these developments, whether Facebook (or any other company) is a "party" under the Wiretap Act is effectively an academic question. In fact, the Ninth Circuit has dismissed other Wiretap Act claims against Facebook based on the company's changed practices requiring consent before tracking subscribers. So the claimed "importance" of the question presented is no reason at all to grant Facebook's petition.

Nor is the purported split. Facebook attempts to manufacture a "general" circuit conflict over the Act's party exemption. But several decisions that it cites as generating this conflict did not interpret that provision at all. And, as Facebook admits, several others involved entirely different facts (*e.g.*, *oral* communications), thus giving little indication as to how the circuits would apply the statute to the type of electronic communications at issue here. Facebook is left only with some weak tension between the decision below and a decision from the Third Circuit. But later cases from the Third Circuit itself suggest even that is disappearing on its own accord.

The interpretation adopted below is also correct. The statute's text, history, and purpose all support the conclusion that a "party to the communication" under the Wiretap Act must be someone whose presence is, at the very least, *known* to the other parties. Facebook's contrary interpretation would sabotage the statute's core prohibitions. Even if this Court wishes to address the Act's applicability to the internet, it should wait for a better vehicle. Doing so for the first time in this unusual context—a private action challenging long-abandoned social-media tracking practices—could have unintended

consequences for criminal prosecutions and law enforcement alike. The petition should be denied.

STATEMENT

1. Congress's longstanding effort to provide protection from wiretapping. The federal government's effort to prohibit wiretapping dates back more than a century. Congress enacted the first federal wiretapping prohibition "as a temporary measure to prevent disclosure of government secrets during World War I." Stevens & Doyle, *Privacy: An Overview of Federal Statutes Governing Wiretapping and Electronic Eavesdropping*, Cong. Res. Servs. (October 9, 2012) at 2. That law provided that no person "shall, without authority and without the knowledge and consent of the other users thereof . . . tap any telegraph or telephone line." 40 Stat. 1017-18 (1918).

Then, a decade later in the Radio Act of 1927, Congress made it a crime for any "person not being authorized by the sender [to] intercept any message and divulge or publish the contents, substance, purpose, effect, or meaning of such intercepted message to any person." 44 Stat. 1172 (1927). And in 1934, Congress enacted Section 605 of the Communications Act to expand federal prohibitions against intercepting radio communications to include wire communications. *See* 48 Stat. 1103-04 (1934) (codified at 47 U.S.C. § 605). Like the earlier laws, Section 605 provided: "No person not being authorized by the sender shall intercept any radio communication." *Id.*

Following these early efforts, Congress sought to expand and update federal wiretapping prohibitions "to protect the privacy of wire and oral communications" from "unauthorized interception." S. Rep. 90-1097 (1968), *reprinted in* 1968 U.S.C.C.A.N. 21112, at 2177, 2178. The result was Title III of the Omnibus Crime Control and Safe

Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, also known as the Wiretap Act—"the first comprehensive federal legislation in the area of wiretapping and electronic surveillance." *United States v. Cox*, 449 F.2d 679, 683 (10th Cir. 1971); *see also* 18 U.S.C. § 2510 *et seq.*

As surveillance and tracking technologies changed, Congress sought to keep up. In the decades after the Wiretap Act's enactment, Congress found, "tremendous advances in telecommunications and computer technologies have carried with them comparable technological advances in surveillance devices and techniques." S. Rep. 99-541 at 3 (1986). Given this rise in electronic communications, Congress was concerned that information that was subject to control of "third party computer operator[s]" could "be open to possible wrongful use and public disclosure by . . . unauthorized private parties." *Id.* Thus, as part of the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (ECPA), Congress amended the statute to cover electronic communications in addition to wire and oral communications.

Today, the Wiretap Act, as amended by the ECPA, prohibits anyone from "intentionally intercept[ing]" any "electronic communication." 18 U.S.C. § 2511(1)(a). But, consistent with its predecessor statutes, the Act also establishes several exemptions from liability. One of those creates a safe harbor for any interception by "a party to the communication" or where "one of the parties . . . has given prior consent to such interception." *Id.* § 2511(2)(d). Although the term "party" is not defined, Congress made clear (as it had in the earlier statutes) that the "use of wiretapping or electronic surveillance techniques by private unauthorized hands has little justification where communications are intercepted without the consent of

one of the parties." S. Rep. No. 90-1097, 1968 U.S.C.C.A.N. at 2156.

2. Facebook's surreptitious tracking. Facebook is not free. Although it does not charge users to sign up for an account, Facebook hoovers up everything users do when logged in and then leverages that information to generate billions in revenue. Allowing the company to construct an individualized profile based on one's Facebook activity and sophisticated inferences is the price subscribers pay for using the social-media network. But what subscribers did not agree to, back in 2010, was being tracked across the internet—outside of Facebook—without their consent.

In 2010, Facebook created its first social plugin—a "Like" button that a non-Facebook developer could add to a website. C.A. E.R. 1079. Subscribers could share on Facebook that they "liked" a website or business by clicking the button. But they did not know that the plugin was able to capture a significant amount of their personal information and the precise content of their communications with other websites—regardless of whether they clicked on it or even noticed it. *See* C.A. E.R. 1092-95.

For instance, let's say a logged-off Facebook user, Alex, is suffering from depression, having suicidal thoughts, and wants to find help. Alex goes to the website for the Suicide Prevention Lifeline. She looks through the website, and eventually clicks on the link for "Talk to Someone Now." A few hours later, Alex logs back into Facebook and notices something new: advertisements for antidepressants. Shocked, Alex wonders: Why is she getting these ads?

The answer is Facebook's plugin. Although Alex didn't know it, Facebook's plugin was secretly redirecting her private interaction with the Suicide Prevention website to Facebook. When Alex pulled up the address https://suicidepreventionlifeline.org/talk-to-someone-now/, her browser sent the Suicide Prevention website what is called a "GET" request—essentially a request to get the web page. C.A. E.R. 1201. In turn, the website sent her information specific to "Suicide Prevention —Talk to Someone Now." *See* C.A. E.R. 1202. By embedding invisible Facebook computer-source code on the webpage Alex visited, Facebook was able to commandeer her communications device (through her web-browser) and cause the device to send a real-time duplicate of her communication to Facebook. Pet. App. 31a.

The duplicated transmission redirected to Facebook servers contains personal information about Alex that Facebook could then add to her Facebook profile. Pet. App. 6a-7a, 31a. To match Alex's communication with her profile, Facebook uses what are known as "cookies"—small text files that can capture information about a person browsing the internet. Pet. App. 7a-8a. Whenever a user creates a Facebook profile, Facebook attaches cookies to the user's web browser that are unique to her. C.A. E.R. 1079. Every time a user visits a website with a Facebook plugin, the plugin records the visit and through the identifying cookie updates the user's profile at Facebook. C.A. E.R. 1086.

What all this means is that, when Alex visited the Suicide Prevention Lifeline website, Facebook could immediately know and record that Alex had just exchanged a communication there seeking to "Talk to Someone Right Now." Within a year of its rollout, millions

of websites like the one Alex visited had Facebook's social plugins. C.A. E.R. 1079.

The company banked on being able to use its plugins to compile a robust personalized history of each user's internet browsing history. C.A. E.R. 1086. By tracking users across millions of websites, the company could obtain unparalleled access to its users' information which, in turn, could be used to extract billions from advertisers for ads targeting every individual user. Statista, *Facebook's Advertising Revenue Worldwide from 2009 to 2019* (Jan. 27, 2021), https://perma.cc/F255-NQUB. That is why a digital cry for help, for example, is answered with an ad for antidepressants.

Facebook, however, had a problem. Many users were logging off of Facebook before visiting other websites. C.A. E.R. 1091. If the company couldn't track those users' post-Facebook interactions and create a complete personalized profile, "the value of the Like button would diminish substantially." *Id.* Facebook's solution to the logged-off-user problem was "easy"—it simply decided to "track users post-logout." *Id.*

Back in 2010, however, Facebook's subscribers were unaware that Facebook was tracking their online movements using its plugins even when they were not logged into their Facebook accounts. Pet. App. 99a; C.A. E.R. 1236. In fact, the company told users the opposite—after they logged out, Facebook promised to "remove the cookies that identify [a user's] particular account" C.A. E.R. 1199. The company expressly represented that it had a "policy of not building profiles based on data from logged out users." Protalinski, *Facebook: Cookie Tracking Issue is Limited, Fix Coming Today*, ZDNet (Oct. 4, 2011), https://perma.cc/89RA-AKEV. And Facebook knew that

it could not "do [so] without some form of consent and disclosure." C.A. E.R. 1097. The company, in other words, understood that its secret tracking practices posed a serious privacy violation. *See id.* But it did so anyway.

It took more than a year before even technologically sophisticated investigators noticed Facebook's surreptitious tracking. In 2011, an Australian "technologist" and blogger discovered that Facebook was tracking logged-out users. Pet. App. 8a. The news triggered a "global stir" as Facebook's more than 800 million users learned, for the first time, that Facebook had been tracking and monetizing their personal information even after they had logged out. Valentino-DeVries, *Facebook Defends Getting Data from Logged Out Users*, Wall Street Journal (Sept. 26, 2011), https://perma.cc/3YZX-DMB7. Fierce criticism followed. C.A. E.R. 1098. Congress demanded an investigation because "tracking user behavior without their consent or knowledge raises serious privacy concerns." Protalinksi, *US Congressmen Ask FTC to Investigate Facebook Cookies*, ZDNet (Sept. 28, 2011), https://perma.cc/ZH8X-86PC; *see* C.A. E.R. 1100-01.

Yet Facebook continued to stonewall. Responding to the flood of criticism, it told the public that it was only using its cookies for users' safety and that "no information" Facebook received "when [a user] see[s] a social plugin[] is used to target ads." Protalinski, *Facebook Denies Cookie Tracking Allegations*, ZDNet (Sept. 25, 2011), https://perma.cc/L9DG-QJ9J. But internally, Facebook continued to tout its widespread tracking capability as a profitable feature. Pet. App. 17a; C.A. E.R. 1079. Only after further public outcry—and an FTC investigation into its privacy practices—did Facebook

finally stop tracking its logged-off users without their consent. Pet. App. 8a. Facebook now informs its users that "social plug-ins" provide "information about your device, websites you visit, purchases you make, the ads you see, and how you use [third-party] services—whether or not you have a Facebook account or are logged into Facebook." Facebook, *Data Policy* (Jan. 11, 2021), https://perma.cc/4KTK-B8MZ.

3. This case. Facebook subscribers who used the network between April 2010 and September 2011 filed this private action against Facebook for its clandestine and nonconsensual tracking, acquisition, and packaging of their personally identifiable data and communications. Pet. App. 74a-75a. They brought eleven claims seeking damages for the economic and privacy harms they suffered as a result of Facebook's violation of numerous state and federal laws, including the Wiretap Act. Pet. App. 55a-56a.

The district court granted Facebook's motions to dismiss the complaint. Pet. App. 53a, 72a-73a. On the Wiretap Act claim, the court found that Facebook's plugin made it a "party" to the communications between the subscriber and the website and thus exempt from liability. Pet. App. 63a. As a result, even though users had no knowledge that Facebook had rigged its code to "automatically" send it information subscribers provided to websites, the district court believed they could not demonstrate that Facebook had "intercepted the user's communication" in violation of the statute. Pet. App. 64a.

The Ninth Circuit reversed and reinstated eight of the plaintiffs' claims. As relevant here, the court recognized that, although the Wiretap Act "contain[s] an exemption from liability for a person who is a 'party' to the

communication," the statute "does not define the term 'party.'" Pet. App. 31a (quoting § 2511(2)(d)). So, the court explained, the party exemption's text "must be considered in the technical context of this case." Pet. App. 30a-31a. Here, Facebook employed software that "automatically duplicate[s] part of the communication" and "directs the user's browser to . . . send a separate but identical GET request . . . to Facebook's server"—all without the user's knowledge or consent. Pet. App. 31a. And "entities that surreptitiously duplicate transmissions between two parties," the court reasoned, "are not parties to communications within the meaning of the Act." *Id.* Accordingly, the Ninth Circuit held, Facebook's "simultaneous, unknown duplication and communication of GET requests" could not exempt the company from liability. Pet. App. 33a.

The Ninth Circuit reinforced its interpretation of the statute's text by considering the Act's purpose. The "paramount objective" of the Wiretap Act was "to protect effectively the privacy of communication." Pet. App. 33a (internal quotations omitted). And Congress enacted the Act "to prevent the acquisition of the contents of a message by an unauthorized third-party." *Id.* If Facebook were permitted to use plugins to "duplicat[e] and forward[]" its logged-out users' information without their knowledge, the Ninth Circuit observed, then the party exemption "would render permissible the most common methods of intrusion, allowing the exception to swallow the rule." *Id.*

REASONS FOR DENYING THE WRIT

I. There is no circuit split warranting this Court's review.

Facebook argues that this Court should grant review to resolve two purported conflicts: "a wider disagreement in the circuits over the scope of the Wiretap Act's 'party' provision" and a more specific split between the decision below and the Third Circuit over the Wiretap Act's application to internet tracking. Pet. 15. But neither justifies this Court's intervention. The former conflict is illusory—it merely consists of decisions applying the provision differently to different sets of facts. And the latter, to the extent it ever existed, is disappearing on its own. Facebook's petition should, therefore, be denied.

A. Facebook contends (at 21) that the decision below deepened a "general conflict over the Wiretap Act's 'party' provision." In its telling, the First, Seventh, and Ninth Circuits have held that a person whose participation in a communication is unknown or unauthorized is not a "party" to that communication under section 2511(2)(d), while the Second, Third, Fifth, and Sixth Circuits explicitly disagree. *See* Pet. 16-20. But on closer scrutiny, this so-called "wider" conflict falls apart at multiple levels.

1. The First and Seventh Circuit decisions that Facebook places on the Ninth Circuit's side of the split don't discuss section 2511(2)(d)'s "party" language at all. Contrary to the company's suggestion (at 18-19) that they involved the statute's "party exception," those decisions interpreted section 2511*(1)(a)*'s use of the term "intercept." *See United States v. Szymuszkiewicz*, 622 F.3d 701, 703-06 (7th Cir. 2010), *as amended* (Nov. 29, 2010); *In re Pharmatrak, Inc.*, 329 F.3d 9, 18, 21-22 (1st Cir. 2003). Facebook itself told the Ninth Circuit that

these decisions were irrelevant to whether Facebook is a "party" under section 2511(2)(d) because "[n]either case addressed the Wiretap Act's 'party' exception, which was not before either court." Facebook C.A. Br. 42-43.

Facebook was right the first time. The First and Seventh Circuits have never decided whether a "party to the communication" includes an entity, like Facebook here, who surreptitiously duplicates communications between two other parties and then transmits them to itself. Nor were they asked to weigh in on that question. Instead, the First and Seventh Circuits held only that "acquisition" of a communication—whether by GET request or email—that "occur[s] at the same time as the transmission" is "contemporaneous" and thus constitutes an "interception" under the Wiretap Act. *Pharmatrak*, 329 F.3d at 22; *see Szymuszkiewicz*, 622 F.3d at 705-06.

2. The other side of the purported split fares even worse. As Facebook admits (at 19), the Second, Fifth, and Sixth Circuit decisions it cites arose "outside the context of computer-to-computer communications." None considered whether a person's unknown, unauthorized acquisition of a secondary, duplicated, and redirected GET request—or, for that matter, any other type of electronic communication—should give rise to Wiretap Act liability. Not one of these circuits has even hinted at how it would apply the Act's party exception to the facts presented here.

For starters, the Fifth and Sixth Circuit's decisions—two criminal cases over 30 years old—involved police officers who answered phone calls while searching a suspect's home. *See United States v. Passarella*, 788 F.2d 377, 378 (6th Cir. 1986); *United States v. Campagnuolo*, 592 F.2d 852, 855 (5th Cir. 1979). In both cases, the caller

knowingly initiated the communication with another party—they just didn't realize that an officer, rather than their intended recipient, answered the call. As the Sixth Circuit explained, such "consensual interceptions" do not violate the Wiretap Act. *Passarella*, 788 F.2d at 379; *see also Campagnuolo*, 592 F.2d at 862-63. That conclusion is consistent with case law predating the current version of the statute, which held that "impersonation of the intended receiver is not an interception within the meaning of the statute." *United States v. Pasha*, 332 F.2d 193, 198 (7th Cir. 1964); *see* S. Rep. No. 90-1097, at 93-94 (1968) (referencing *Pasha* in Wiretap Act amendment). In short, these cases turned entirely on the purported interceptor's "impersonation" of the caller's intended recipient.

But here, Facebook does not impersonate the intended receiver of a communication, or otherwise deceive the internet user (the "caller") about its identity. The user does not initiate a communication with anyone other than the website she visited—it's *Facebook's* code, hidden on the website without the user's knowledge, that triggers a separate, unauthorized communication from the user's browser. Facebook is thus wrong when it asserts (at 19) that "the rationale of [these] decisions would have required ruling for Facebook here." This case's facts are more analogous to a situation in which an officer implants software or a device on a person's phone that triggers a separate, unknown call to the police station whenever the person dials a call—so that the police can listen to the conversation between the caller and recipient. Fairly read, *Passarella* and *Campagnuolo* shed no light on this situation.

Facebook's reliance on *Caro v. Weintraub*, 618 F.3d 94 (2d Cir. 2010), is even further off the mark. Pet. 20. *Caro* involved an in-person conversation between relatives about a person's wishes for her will and estate, during which one of her sons recorded part of that conversation on his iPhone. *See* 618 F.3d at 96. After the woman died, the son tried to introduce that recording at the probate court; her husband then sued the son for violating the Wiretap Act. *Id.* at 9697. The Second Circuit held that the son was a "party" under section 2511(2)(d) even though he was not "invited" to take part in the conversation among family members. *Id.* at 97. There was no question in *Caro* that the son actually "t[ook] part" in the conversation: the other participants *knew* that he "was present at the table during the conversation in the kitchen and . . . [he] spoke up a few times" in support of other participants. *Id.* at 97-98. Nothing in the Second Circuit's reasoning remotely suggests how the court would apply the Wiretap Act's party exception to *unknown* transmissions of duplicated electronic communications.

3. To the extent that these decisions are relevant, they suggest that, faced with similar facts as those here, the above circuits would arrive at the same outcome as the decision below.

The Fifth and Sixth Circuits, for instance, emphasized the fact that the officers "*directly* answered" calls that the caller *intended* to make. *Passarella*, 788 F.2d at 379 (emphasis added). As the Fifth Circuit explained: "[T]he officer was the *immediate party* to the call. The bettor *intended* his words to reach the officer, albeit the bettor thought he was someone else. Thus the officer did not 'intercept' a message while it was en route to another; *there was no other* on the line." *Campagnuolo*, 592 F.2d at

862 (quoting *Pasha*, 332 F.2d at 198) (emphasis added). And it explicitly compared the "impersonating officer" situation—which didn't violate the Wiretap Act—with "a situation in which by surreptitious means a third party overhears a telephone conversation between two persons"—which would. *Id.* Given this reasoning, it is likely that the Fifth and the Sixth Circuits would hold that Facebook is *not* a "party" under the Wiretap Act if presented with the company's "surreptitious" tracking practices.

Same with the Second Circuit. In *Caro*, the court explicitly held that the son was a "party" because the other participants were aware of the son's "presen[ce] . . . during the conversation." 618 F.3d at 97. But here, Facebook cannot dispute that the internet user—who has no idea that her browser has been hijacked—is unaware of Facebook's "presence" in the conversation. Given this key distinction, the Second Circuit, too, would likely agree with the decision below.

B. Having cleared away Facebook's claims of a "general" conflict over the Wiretap Act's party exception, all that remains is the Third Circuit's decision in *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125 (3d Cir. 2015). But more recent case law suggests that the Third Circuit is walking back its interpretation of section 2511(2)(d) to more closely align with that of the Ninth Circuit.

In a decision issued the year after *Google*, the Third Circuit affirmed a conviction under the Wiretap Act where the defendant had used an online web service to surreptitiously redirect and record phone conversations between labor-union officials and a website operator without their knowledge or consent. *United States v.*

Eady, 648 F. App'x 188, 189-90 (3d Cir. 2016). Eady argued that he was a "party" to the calls under section 2511(2)(d) because he "initiated the calls" and "could have participated in the communication." *Id.* at 191-92 & n.3.

The Third Circuit rejected that argument, holding that a "party" within the meaning of the Wiretap Act is "a participant *whose presence is known* to the other parties contemporaneously with the communication." *Id.* at 191 (emphasis added). That was so because "Congress intended to require actual participation in the conversation at issue to be considered a 'party,'" and "a defendant does not actually participate in a conversation unless his presence is known to the other participants." *Id.* at 192. The Third Circuit also made clear in *Eady* that it viewed its holding as consistent with its prior decision in *Google*. *See id.*; *see also Allen v. Quicken Loans Inc.*, 2018 WL 5874088, at *5 (D.N.J. Nov. 9, 2018) (reading *Google* and *Eady* together to hold that "surreptitiously record[ing] conversations between two other individuals without the knowledge or consent of *any* party to that communication" would fall outside § 2511(2)(d)).

The Third Circuit's interpretation of the party exception in *Eady*—which the petition fails to mention—is consistent with the Ninth Circuit's reasoning below. And it indicates that, contrary to Facebook's claims, the Third Circuit does not view its holding in *Google* to categorically allow "unknown or unauthorized participants [to] be 'parties' under the Act." Pet. 21.

Bottom line: Any weak tension that might exist between *Google* and the decision below does not warrant this Court's review. At the very least, the Third Circuit's evolving case law suggests it would be unwise to grant review without allowing further percolation. And that is

especially true given that the Third Circuit is fully capable of resolving any potential existing tension on its own.

II. The question presented has limited practical significance and is unlikely to recur.

Facebook claims that review is warranted because the decision below has "sweeping practical consequences" that will expose "ubiquitous," "prevalent," and "routine" internet practices to "massive" liability under the Wiretap Act and "stifle future innovation." Pet. 1-2, 4. But repeating that refrain does not make it so.

The practices at issue here—Facebook's nonconsensual, secret, and invasive tracking of individuals' internet browsing after they had logged out of their accounts—are anything but "prevalent" or "ubiquitous." In fact, Facebook itself admits that it no longer uses these practices. Instead, it now seeks (or at least claims to seek) users' consent before tracking them—a total defense to liability. And obtaining consent before transmitting personal information is now required by California's Consumer Privacy Act, meaning that technology companies that comply with state law should not be subject to Wiretap Act claims. The effect of the decision below is, therefore, unlikely to extend beyond a largely abandoned set of historic, outlier tracking practices—it has no potential to upend "common business practices integral to the internet's basic operation." Pet. 15. It is, in other words, essentially academic. This Court's intervention is thus unnecessary.

A. Facebook's hyperbolic speculation about the consequences of the decision below is grounded in Facebook's erasure of the second half of the key statutory provision. Pet. 27-31; *see* Internet Ass'n et al. Amici Br. 10-20. The Wiretap Act does not just exempt from liability any person who "is a party to the communication" at issue. 18

U.S.C. § 2511(2)(d). It also *permits* interception "where one of the parties to the communication has given *prior consent* to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." *Id.* (emphasis added).

Although Facebook barely mentions it, this "prior consent" exemption is central to understanding how the statute applies to modern internet communications. It means that a company like Facebook—whether "party to a communication" or not—may lawfully duplicate, record, or otherwise acquire that communication so long as one of the parties (here, the user or non-Facebook website) consents. *See, e.g.*, *Pharmatrak*, 329 F.3d at 19-21 (discussing § 2511(2)(d)'s prior-consent exception); *United States v. Amen*, 831 F.2d 373, 378 (2d Cir. 1987) ("Congress intended the consent requirement to be construed broadly."). The question presented, therefore, has no significance *at all* in cases involving consent. Indeed, Facebook recognizes as much, admitting that "[h]ost websites or third-party content providers may obtain consent to communicate with users' browsers and employ cookies, precluding Wiretap Act liability." Pet. 31 n.15.

Of course, the problem for Facebook is that, in 2010 and 2011, it didn't obtain its subscribers' consent to track their web browsing even after they logged out. Instead, it misled the public to believe that it did not acquire such information at all. C.A. E.R. 1210. Only after public scrutiny and federal investigation did Facebook change its tracking practices and its disclosures to the public about the information it obtained about its users. Pet. App. 8a; *see* Pet. 30 (acknowledging that Facebook "no longer engages in the practice that plaintiffs challenge in this case");

Facebook, *Cookies & other storage technologies* (last visited Feb. 3, 2021), https://perma.cc/Z9R2-R5MG; Facebook, *What information does Facebook get when I visit a site with the Like button?* (last visited Feb. 3, 2021), https://perma.cc/E7QM-PLXR.

Notably, after these changes, the Ninth Circuit—in a decision by Chief Judge Thomas, the author of the decision below—affirmed dismissal of a Wiretap Act claim against Facebook where the district court found "that Plaintiffs consented to Facebook's data tracking and collection practices" by agreeing to the company's reformed "Terms and Policies." *Smith v. Facebook, Inc.*, 745 F. App'x 8, 8-9 (9th Cir. 2018). That Facebook could escape liability simply by changing its own terms and policies demonstrates why the question presented has little, if any, practical effect. *Consent*, not "party" status, is what matters in the vast majority of cases privately enforcing the Wiretap Act.

Facebook's amici similarly speculate that the decision below will subject a "vast universe of communications to significant civil and criminal liability" by ensnaring companies in who engage in innocuous practices like "simple analytics." Amici Br. 15-17, 20. But these warnings, like Facebook's, overstate the extent to which the success of a plaintiff's Wiretap Act claim turns on "party" status. As amici and their cited authorities recognize, the website-performance data sent by web-analytics tools is meaningfully different from the detailed personal information about logged-out users that Facebook acquired through its secret tracking. *See id.* at 19; GSA Tech. Transformation Servs., *Guide To The Digital Analytics Program: Common Questions*, https://digital.gov/guides/dap/common-questions-about-dap/ (noting that "agencies are

forbidden" to collect personally identifiable information and that its "code is set to anonymize IP addresses at the earliest available point"). Web analytics, in other words, largely involve "basic identification and address information," which some courts have suggested cannot give rise to Wiretap Act liability because it does not qualify as "contents of a communication." *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1109 (9th Cir. 2014); *see United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010).

Consequently, the decision below does not undermine "the functions that characterize the modern web" or subject a "vast universe of communications to significant civil and criminal liability." Amici Br. 20. It just holds that a company, like Facebook, that secretly duplicates an internet user's communications with other websites and redirects those communications along with highly personal information about the user to itself—all in violation of the company's privacy policies and promises—may face a claim under the Wiretap Act. That narrow holding does not warrant this Court's review.

B. For similar reasons, the question presented is unlikely to recur. Like Facebook, most internet companies have adopted privacy terms and policies that seek to obtain users' consent to track them, provide them with targeted advertising, or otherwise acquire their personal information. Take Google. It also reached a settlement in 2012 with the FTC and numerous state attorneys general to address the very tracking practices that prompted the litigation that reached the Third Circuit. *See In re Google*, 806 F.3d at 132-33 & nn. 10-12. These settlements—among the largest ever obtained by the FTC—reasonably put other companies on notice that tracking individuals' browsing without their knowledge and consent violates

federal law. And any company that responsibly reformed their policies to address these legal concerns (just like Facebook and Google did) would not be exposed to Wiretap Act liability for engaging in these practices under the law's "prior consent" exception—particularly given the two-year statute of limitations. *See* 18 U.S.C. § 2520(e). In short, to avoid liability, a company must simply gain consent before tracking communications.

Facebook nevertheless contends (at 30) that Wiretap Act suits "will only proliferate" in the Ninth Circuit after the decision below. That is provably wrong, for at least two reasons.

First, according to Facebook, the First and Seventh Circuits have permitted Wiretap Act claims to proceed against "unknown" and "unauthorized" duplications and transmissions of electronic communications for more than a decade. Pet. 18-19. Yet Facebook points to no increase in private Wiretap Act litigation in those circuits—home to major technology hubs like Boston and Chicago. Nor does the company identify a single criminal prosecution in those circuits (or elsewhere) of a company employing practices similar to those here, despite Facebook's repeated concerns (at 4, 16, 28) that accepting the Ninth Circuit's interpretation of the party exception would expose it to criminal liability under the Wiretap Act.

Second, California recently enacted legislation that requires companies like Facebook to seek consent from users before collecting their personal information. The California Consumer Privacy Act, which became effective on January 1, 2020, provides that "[a] business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the

purposes for which the categories of personal information shall be used." Cal. Civ. Code § 1798.100(b). So Facebook and other technology companies operating in California should now, as a matter of state law, be obtaining consent from every user to collect personal information. And, as the Ninth Circuit's *Smith* decision illustrates, that "prior consent" should allow companies to avoid Wiretap Act liability. 745 F. App'x at 9; *see* 18 U.S.C. § 2511(2)(d).[1]

In the end, Facebook puts too much weight on the thin reed of the statute's party exception. Given the state of the law and the prevalent market and technological practices, Wiretap Act liability will realistically turn on companies' consent and disclosure policies, not on whether they are "parties" to users' communications with third-party websites. Far from "provid[ing] much-needed guidance to lower courts," Pet. 32, the question presented will likely have no practical impact on companies like Facebook aside from this case, and perhaps a handful of others that similarly involve long-abandoned practices. This Court should therefore deny review.

---

[1] Facebook points (at 28-29) to a couple recent lawsuits as evidence that the decision below will lead to an increase in litigation. But they actually demonstrate why the question presented will have little practical effect. For instance, in the Google case the petition cites, Google moved to dismiss the Wiretap Act claim based on section 2511(2)(d)'s "prior consent" exception. ECF No. 62 at 12-13, *Rodriguez v. Google*, No. 3:20-cv-4688 (N.D. Cal. Dec. 17, 2020). Google emphasized that its policies—just like Facebook's more recent ones at issue in *Smith*—require mobile apps using Google tracking tools to disclose that fact to users and "obtain their consent" for data collection. *Id.* at 11. Thus, whether Google is a "party" is immaterial to that case's resolution. And so it will be for nearly every case to come.

III. This case is an unsuitable vehicle for interpreting the Wiretap Act's "party" exception.

Even if this Court believes that the Wiretap Act's party exception merits further consideration, it should still deny review and wait for a better vehicle.

A. Facebook accurately states (at 32) that "this Court has not yet decided a case addressing the Wiretap Act's application to internet communications." But that is reason *not* to grant review here. If Facebook is correct (at 31) that "the question presented has immense doctrinal significance," it would be especially odd for this Court to address it in a private consumer action against outdated social-media-advertising practices that Facebook itself has cast aside.

Instead, if this Court wishes to grant review, it should do so in a case arising in the criminal context. After all, the Wiretap Act provision at issue here was enacted as part of Title III of the Omnibus *Crime* Control and Safe Streets Act of 1968, and thus is "primarily a criminal provision." *DIRECTV, Inc. v. Bennett*, 470 F.3d 565, 566 (5th Cir. 2006); *see Alderman v. United States*, 394 U.S. 165, 175 (1969). The Act's party exception is equally applicable to criminal prosecutions and wiretap applications as it is to private actions. And the provision also applies in cases involving *non-electronic* "oral" and "wire" communications. 18 U.S.C. § 2511(1)(a). So this Court's interpretation could have unanticipated and profound consequences for federal prosecutors and law-enforcement officers alike.

Facebook's reading of section 2511(2)(d), for instance, could conceivably immunize from criminal liability under the Wiretap Act a hacker who installs "spyware" software that commands a browser to duplicate and redirect a web user's communications with her financial

institutions, allowing the hacker to acquire the user's confidential information, such as bank accounts and credit-card details. *See, e.g.*, *United States v. Barrington*, 648 F.3d 1178, 1203 (11th Cir. 2011) (observing that "keylogger software . . . could be used to contemporaneously capture information or signals being transmitted beyond the user's computer"). Facebook's interpretation could even have national-security and civil-liberties implications: Would federal agents no longer need to follow the precise rules and procedures that the statute sets out for wiretap applications so long as they use code that triggers a separate communication whenever their subject communicates with another person? And what would the implications of accepting such an interpretation be for criminal defendants' Fourth Amendment rights?

These weighty legal and practical issues are not presented here. The plaintiffs' Wiretap Act claim turns on a specific factual context: their allegations that Facebook secretly tracked logged-out users' web browsing without their consent in violation of its own privacy promises. These unique facts would constrain the Court's ability to provide meaningful guidance to lower courts on how to apply the Act's party exception to the primary situations with which the law is concerned—a criminal prosecution of someone accused of wiretapping or a criminal defendant's motion to suppress evidence obtained by unlawful wiretapping. If this Court wishes to address the Act's application to electronic communications for the first time, it should grant review of a vehicle that provides the opportunity to interpret the statute in light of its core purposes.

B. This case suffers from an additional vehicle defect. Facebook's success on the merits of the Wiretap Act claim here does not actually turn on whether it is a "party to the

communication" under section 2511(2)(d). The question presented, in other words, is not outcome-dispositive even in this specific case.

Even if Facebook is a party to the "secondary GET request" between the user's browser and the company's servers (and it is not), it cannot possibly claim to be a party to the initial GET request between the user and the non-Facebook website. And it is *that* initial communication, the plaintiffs allege, that Facebook "intentionally intercept[ed]" in violation of the Wiretap Act. 18 U.S.C. § 2511(1)(a); *see* C.A. E.R. 566-67. The fact that Facebook may be a party to the *non*-intercepted communication—its plugin's duplication and redirection of the contents of the intercepted communication between the user and the other website—is irrelevant.

That is presumably why Facebook argued to the Ninth Circuit that it "never 'intercepted' a communication" at all. Facebook C.A. Br. 40. The company admitted that it "did not receive the first communication" and so was not a "party" to the initial GET request. *Id.* at 42. But it insisted that, under Ninth Circuit precedent, its "simultaneous, identical transmission" of the initial GET request to its own servers did not qualify as "interception" under the statute. *Id.* at 42-43.

The problem is that Facebook has not presented *this* particular issue—whether its duplication and redirection of communications to other websites constitutes "interception" under section 2511(1)(a)—to this Court. And even if it had, the Ninth Circuit declined to rule on it. Apart from reversing the district court's ruling on the party-exemption question, the Ninth Circuit "d[id] not opine whether the Plaintiffs adequately pleaded the other requisite elements of the" Wiretap Act, instead remanding

those questions to the district court. Pet. App. 33a-34a. "This Court, however, is one of final review, not of first view." *F.C.C. v. Fox Television Stations, Inc.*, 556 U.S. 502, 529 (2009). Facebook will have sufficient opportunity—in the district court and, potentially, again in the Ninth Circuit—to argue that its tracking practices do not constitute "interception" under the Wiretap Act.

More generally, that this appeal arises at such an early stage in the proceedings further counsels against review. Facebook argued below that the Wiretap Act claim should be dismissed for other reasons, including because its cookie trackers are not "devices" under the Act. But the Ninth Circuit did not reach these arguments either. Depending on how the district court rules on remand—or information that may come out through discovery—the question presented may become irrelevant. And that is leaving aside the fact that Facebook's petition concerns only *one* of the eight claims that the decision below reinstated. Pet. App. 39a-40a. So, no matter how this Court resolves the present appeal, the plaintiffs' action against Facebook will proceed.

IV. The decision below is correct.

Certiorari is also unwarranted because the decision below is correct.

A. The Ninth Circuit held that Facebook is not a "party to the communication" under the Wiretap Act. Pet. App. 33a. That holding, in Facebook's view (at 21), "exalt[s] perceived legislative purposes over text." That is wrong. The Ninth Circuit's interpretation reflects the best reading of the statute's text, even without reference to its history or purposes (which only reinforce this conclusion).

Section 2511(2)(d) provides that "[i]t shall not be unlawful . . . for a person . . . to intercept a wire, oral, or electronic communication where such person is a party to the communication." 18 U.S.C. § 2511(2)(d). But "the Wiretap Act does not define the term 'party' in its liability exemption." Pet. App. 31a. Pointing to various dictionary definitions, Facebook contends that "party" must be understood as a "participant." Pet. 21-22. But that just prompts the question: What must a person do to "participate" in a communication?

Facebook asserts (at 21) that, "at a minimum," "party" means "the sole designated recipient of the information conveyed." But Facebook's assertion is just that—an assertion. This interpretation flows neither from its dictionary definitions nor from any natural reading of the term. The company's only support is a treatise that provides no guidance on the interpretive question, and indeed acknowledges uncertainty as to how section 2511(2)(d) should apply to "third parties" like Facebook who "track conduct on websites in ways that are not apparent to users." *See* 2 LaFave, Criminal Procedure: Detection and Investigation of Crime, § 4.6(l) (4th ed. 2020).

More importantly, Facebook's own preferred definition of "party" as a "designated recipient" doesn't even help it here. The same goes for the term "participant"—Facebook's other proposed definition. *See* Pet. 21. No one would describe an eavesdropper, hiding in a closet, as either a "designated recipient" or a "participant" of a conversation taking place between two others in the adjoining room. Yet that is analogous to the way in which Facebook received the communications in this case. To be a *designated* recipient requires some intent on behalf of the other parties to convey a communication. And to be a participant

requires that others must at least be aware of such participation. That is why a party to a communication requires something more than just receipt; what matters is whether *other participants are aware* of an individual's presence in a conversation or receipt of a communication. *See Eady*, 648 F. App'x at 192 (explaining that a person cannot "actually participate in a conversation unless his presence *is known* to the *other* participants" (emphasis added)).

Here, there is no dispute that internet users did not intend to communicate with Facebook—they intended to visit some other website, which happened to contain hidden Facebook source code. Pet. App. 31a. Nor did the users know that this code would redirect the content of their communication and their personal information to Facebook's servers. In fact, they believed, based on the company's express policies, that Facebook did *not* track its subscribers after they logged out. Pet. App. 19a-22a. But despite these promises, Facebook unilaterally initiated a "conversation" with logged-out users' browsers that duplicated their communications with non-Facebook websites. The users never knew about—let alone intended or consented to—the transmission that Facebook acquired.

Ironically, on Facebook's interpretation, the Wiretap Act would seemingly not even prohibit *wiretaps*. Telephones work by translating conversations into electric signals and transmitting those signals through a wire. A wiretap intercepts that electric signal, copies it, and bifurcates it. The same message is then received by two "end recipient[s]." *See* Pet. 22. According to Facebook (at 23), because a wiretapper makes herself the "sole designated recipient of information from the sender," the wiretapper

is a party to the conversation and thus exempt from liability under the *Wiretap* Act.[2]

This cannot be the correct reading of the statute's text. Accepting Facebook's circular interpretation—allowing a recipient to "designate" itself as a party without the sender's knowledge or intent—would strike at the heart of the Act. Indeed, as the Ninth Circuit observed, it would permit the party exemption to "swallow the rule." Pet. App. 33a. The only way to make sense of the statute's text is to distinguish between "seen" and "unseen"—known and unknown—recipients. *See Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, 31 F. Supp. 3d 237, 255 (D.D.C. 2014). Because Facebook's acquisition of its users' communication here was indisputably unknown to the users, the Ninth Circuit correctly held that Facebook is not a "party" under the Wiretap Act.[3]

---

[2] "Until the mid-1990s, most wiretaps required the manual 'bugging' of a phone or phone line. To bug a phone line, law enforcement would either physically attach a device to the phone wire or place a bug inside the phone itself. The phone company would then set up a separate line into which law enforcement could dial and listen to the conversations taking place over the bugged line. The separate line was essentially the same as any other business or residential phone line." *Prather v. AT&T, Inc.*, 847 F.3d 1097, 1099 (9th Cir. 2017). So, under Facebook's interpretation, the fact that a "separate line" transmitted the communication from the device (phone) to interceptor would make the interceptor a "party" to the communication—and thus immune from the Wiretap Act's requirements.

[3] This interpretation would not make the party status inquiry turn "on a plaintiff's subjective understanding of a communication." Pet. 23. Whether a person has knowledge for section 2511(2)(d) purposes can be determined on an objective basis—*e.g.*, based on what a reasonable person would know. Here, no one disputes that users were unaware of the secret transmissions to Facebook's servers.

B. This interpretation of "party" is also confirmed by the statute's history. For over a century, federal wiretapping laws have prohibited interception of communications by persons about whom the sender has no knowledge or awareness.

All these predecessor statutes were clear that a person could be exempt from wiretapping prohibitions only when the sender *knew* of that person's participation in the communication. *See supra* at 4-5. In fact, some of them provided that even knowledge wasn't enough—a person could not legally acquire a communication unless the sender specifically *authorized* him to do so. *See, e.g.*, 40 Stat. 1017-18 (1918) (providing that no person "shall, *without authority and without the knowledge and consent of the other users thereof* . . . tap any telegraph or telephone line") (emphasis added); 44 Stat. 1172 (1927) (making it a crime for any "*person not being authorized by the sender* [to] intercept any message") (emphasis added); 48 Stat. 110304 (1934) (codified at 47 U.S.C. § 605) ("No *person not being authorized* by the sender shall intercept any radio communication.") (emphasis added).

In light of this history, Congress reasonably assumed, when it enacted the ECPA in 1986 to update the Wiretap Act to comport with new technology, that a "party to a communication" in section 2511(2)(d) would not include someone about whom the sender is entirely unaware—like Facebook. Pet. App. 33a.

Facebook ignores this history entirely. Instead, it asserts that a party to an electronic communication under the Wiretap Act is merely the "end recipient of" it—regardless of whether the sender knew about the communication or the recipient. Pet. 22. But Facebook cannot explain why Congress would have *narrowed* the Wiretap

Act's coverage when the whole point of the Act was to *expand* federal wiretapping prohibitions "to protect the privacy of [electronic] communication" from "unauthorized interception." S. Rep. 90-1097, 1968 U.S.C.C.A.N. at 2177, 2178; *see Gelbard v. United States*, 408 U.S. 41, 49 n.7 (1972) (noting that the Act was intended to "provide the protection for privacy lacking under the prior law").

Resisting this conclusion, Facebook argues its interpretation is correct because Congress incorporated existing case law that "held that obtaining information through unknown and unauthorized participation was permissible." Pet. 25. But, as explained above (at 14-16), this argument rests on a fundamental misreading of Congress's reference to the Seventh Circuit's 1964 decision in *Pasha*, 332 F.2d 193. *Pasha* held that a sender's unawareness of the precise *identity* of the recipient does not mean that the communication's recipient is a wiretapper—it said nothing about a case like this one, where the sender doesn't even know of the *existence* of the communication or the purported "recipient." *Id.* at 198. And *Pasha* expressly differentiated between the officer's impersonation there and "a situation in which by surreptitious means a third party overhears" a conversation between two persons. *Id.*

Facebook's tracking practices here resemble the latter far more than the former. Through its "surreptitious" code on non-Facebook websites, Facebook redirects separate transmissions to itself that (through duplication) allow the company to "overhear[]" the internet user's communications with the website. *Pasha*, 332 F.2d at 198. That nonconsensual interception, the Ninth Circuit correctly held, violates federal law.

C. The Wiretap Act's purposes confirm what its text and statutory history make clear: Only *known* participants are "parties to a communication" under the statute.

In enacting the Act, "the protection of privacy was an overriding congressional concern." *Gelbard*, 408 U.S. at 48; *see also* S. Rep. 90-1097. And "[t]his concern for privacy was inseparably bound up with the desire that personal conversations be frank and uninhibited, not cramped by fears of clandestine surveillance . . . or suspicion that one's speech is being monitored by a stranger." *Bartnicki v. Vopper*, 532 U.S. 514, 543 (2001) (Rehnquist, C.J., dissenting).

And with each succeeding statute addressing wiretapping, Congress evinced an intent to strengthen privacy in the wake of new technology—not weaken it. These concerns grew in urgency with the advent of electronic communications over the internet. Congress expanded wiretapping protections to electronic communications specifically because of fears that personal information controlled by "third party computer operator[s]" could "be open to possible wrongful use and public disclosure by . . . unauthorized private parties." *See supra* at 5.

The Ninth Circuit correctly held that Facebook's interpretation of section 2511(2)(d) would severely undermine the Act's central purposes. Pet. App. 33a. Facebook's only response is that, along with individual privacy, Congress also sought to "preserv[e] technologies that hold such promise for the future." Pet. 24. But that is no reason to adopt Facebook's sweeping interpretation. The statute already protects innovation and development of new technologies by permitting interceptions made with a party's "prior consent." 18 U.S.C. § 2511(2)(d); *see supra* 18-21.

And, unlike Facebook's proposal, it does so in a way that advances, rather than erodes, individuals' privacy.

CONCLUSION

This Court should deny Facebook's petition for a writ of certiorari.

Respectfully submitted,

MATTHEW W.H. WESSLER
Counsel of Record
GUPTA WESSLER PLLC
1900 L St. NW, Suite 312
Washington, DC 20036
(202) 888-1741
matt@guptawessler.com

NEIL K. SAWHNEY
GUPTA WESSLER PLLC
100 Pine St., Suite 1250
San Francisco, CA 94111
(415) 573-0336
neil@guptawessler.com

DAVID A. STRAITE
KAPLAN FOX &
KISHEIMER LLP
850 Third Ave.
New York, NY 10022
(212) 687-1980
dstraite@kaplanfox.com

STEPHEN G. GRYGIEL
GRYGIEL LAW, LLC
301 Warren Ave., # 405
Baltimore, MD 21230
(410) 617-8945
sgrygiel@silverman-thompson.com

JAY BARNES
SIMMONS HANLY CONROY
One Court St.
Alton, IL 62002
(618) 693-3104
jaybarnes@simmons-firm.com

February 11, 2021 *Counsel for Respondents*