No. 20-____

IN THE

Supreme Court of the United States

FACEBOOK, INC.,

Petitioner,

v.

PERRIN AIKENS DAVIS ET AL.,

Respondents.

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

PETITION FOR A WRIT OF CERTIORARI

Michael R. Dreeben
Ephraim McDowell
O'MELVENY & MYERS LLP
1625 Eye Street, N.W.
Washington, D.C. 20006
(202) 383-5300

Jeffrey L. Fisher
Counsel of Record
O'MELVENY & MYERS LLP
2765 Sand Hill Road
Menlo Park, CA 94025
(650) 473-2633
jlfisher@omm.com

Yaira Dubin
O'MELVENY & MYERS LLP
Times Square Tower
7 Times Square
New York, N.Y. 10036
(212) 326-2000

QUESTION PRESENTED

The Wiretap Act prohibits the "intentional[] intercept[ion]" of an "electronic communication," but precludes liability for a "party to [a] communication" or when a party consents to the interception. 18 U.S.C. § 2511(1), (2)(d). Internet webpages are frequently composed of content—images and text—sent from multiple providers according to instructions communicated by a user's web browser to obtain that content. The question presented is:

Whether an internet content provider violates the Wiretap Act where a computer user's web browser instructs the provider to display content on the webpage the user visits.

PARTIES TO THE PROCEEDING

Facebook, Inc. is Petitioner here and was Defendant-Appellee below.

Perrin Aikens Davis, Brian K. Lentz, Cynthia D. Quinn, and Matthew J. Vickery are Respondents here and were Plaintiffs-Appellants below.

CORPORATE DISCLOSURE STATEMENT

Facebook, Inc. is a publicly traded company and has no parent corporation. No publicly held company owns 10% or more of its stock.

STATEMENT OF RELATED PROCEEDINGS

In re Facebook, Inc. Internet Tracking Litigation, No. 17-17486 (9th Cir.) (opinion issued and judgment entered on April 9, 2020; petition for rehearing denied June 23, 2020; mandate issued August 18, 2020).

In re Facebook, Inc. Internet Tracking Litigation, No. 5:12-md-02314 (N.D. Cal.) (order granting Facebook's motion to dismiss with leave to amend issued October 23, 2015; order granting in part Facebook's motion to dismiss second amended complaint with prejudice issued June 30, 2017; order granting Facebook's motion to dismiss third amended complaint with prejudice issued November 17, 2017).

There are no additional proceedings in any court that are directly related to this case.

TABLE OF CONTENTS

Page

TABLE OF CONTENTS
(continued)

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES (continued)

STATUTES

TABLE OF AUTHORITIES (continued)

OTHER AUTHORITIES

TABLE OF AUTHORITIES
(continued)

PETITION FOR A WRIT OF CERTIORARI

Petitioner Facebook, Inc. respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Ninth Circuit.

OPINIONS BELOW

The decision of the court of appeals is reported at 956 F.3d 589 and reprinted in the Appendix to the Petition ("App.") at 1a-40a. The decisions of the district court are reported at 290 F. Supp. 3d 916; 263 F. Supp. 3d 836; and 140 F. Supp. 3d 922, and are reprinted at App. 41a-53a; 54a-73a; and 74a-101a.

JURISDICTION

The court of appeals issued its decision on April 9, 2020, App. 40a, and denied rehearing on June 23, 2020, *id.* at 102a. This Court's March 19, 2020 order extended the deadline for all petitions for writs of certiorari due on or after March 19 to 150 days from the date of the lower court judgment or order denying a timely petition for rehearing. The jurisdiction of this Court is invoked under 28 U.S.C. § 1254(1).

RELEVANT STATUTORY PROVISIONS

Relevant statutory provisions are reprinted in the appendix to this petition. App. 103a-116a.

INTRODUCTION

This case presents a question of critical importance on which the circuits are openly divided: do certain ubiquitous practices in the technology industry involving computer-to-computer communications violate the federal Wiretap Act? The answer to this question has sweeping practical consequences. It will determine whether content providers on the internet will face sizable damages actions and potential criminal liability for routine business activity.

The Wiretap Act prohibits the "intercept[ion]" of "electronic communication[s]." 18 U.S.C. § 2511(1). But it makes clear that a "party to [a] communication" does not act unlawfully by "intercept[ing]" the very communication in which it takes part. *Id.* § 2511(2)(d). "Party to a communication" in the Wiretap Act means exactly what one would expect: a designated sender or recipient of information in an interaction between multiple entities.

This case arises from a putative nationwide class action asserted against Facebook, a social-media and internet company. Plaintiffs are Facebook users who allege that Facebook "intercepted" their communications, in violation of the Wiretap Act. Plaintiffs seek $15 billion in class-wide damages.

Plaintiffs' allegations focus on a prevalent practice in the technology sector: computer-to-computer communications involving internet users' web browsers, through which servers provide content to webpages users visit. Here, plaintiffs allege that, while logged out of Facebook, they visited webpages that had elected to integrate Facebook features, such as "Like" or "Share" buttons. Plaintiffs further allege that their browsers communicated with Facebook to allow Facebook to provide those features, without plaintiffs' knowledge or authorization. Through that communication, plaintiffs maintain, Facebook received certain data about the websites and pages they visited.

In the decision below, the Ninth Circuit held that plaintiffs' Wiretap Act claim could proceed, ruling that Facebook was not a "party to [a] communication" under the Act. App. 33a. While the court acknowledged that plaintiffs' browsers sent the information that Facebook allegedly intercepted directly to Facebook, the court believed that Facebook was not a "party" because plaintiffs did not know about or authorize their browsers' communication with Facebook. *Id.* at 30a-33a. The Ninth Circuit did not purport to base that holding on the Wiretap Act's text, which uses the unmodified term "party" and says nothing about knowledge or authorization. Instead, the court relied on its view of the Act's "paramount objective" and "legislative history." *Id.* at 33a (internal quotation marks omitted). The court's analysis of those considerations was itself erroneous—but more fundamentally, the Ninth Circuit disregarded this Court's repeated instructions to adhere to statutory language.

In reaching its conclusion, the Ninth Circuit expressly acknowledged that "the Third Circuit has held to the contrary." *Id.* at 32a (citing *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 143 (3d Cir. 2015)). In *In re Google*, the Third Circuit considered the same type of computer-to-computer communications at issue here and ruled that the Wiretap Act's "party" provision precluded liability. 806 F.3d at 143-44. Thus, if Facebook had been sued for a purported Wiretap Act violation in the Third Circuit, it could not be held liable. The same can almost certainly be said of the Fifth, Sixth, and Second Circuits, which have all rejected the Ninth

Circuit's rule that "unknown" or "unauthorized" participants cannot be "parties" to a communication. Meanwhile, the Ninth Circuit "adopt[ed]" decisions of the First and Seventh Circuits holding that defendants engaging in computer-to-computer communications that the Ninth Circuit perceived as similar to those here can face liability under the Act. App. 33a (citing *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 22 (1st Cir. 2003); *United States v. Szymuszkiewicz*, 622 F.3d 701, 706 (7th Cir. 2010)).

This square circuit conflict over the meaning of a federal statute warrants review. And that review should occur now. Most leading internet companies are based in the Ninth Circuit, so future plaintiffs will bring their Wiretap Act claims there, preventing additional courts from addressing this issue. In fact, since the Ninth Circuit's decision below, plaintiffs have already brought Wiretap Act class actions involving similar allegations in California federal court against Google and Microsoft. If this Court were to deny review, such suits would undoubtedly multiply. The risk of massive civil damages—and even possible criminal prosecution—will hang over the internet sector and stifle future innovation.

Facebook is deeply committed to user privacy. It has protected and will continue to protect users' data. But the Wiretap Act does not prohibit Facebook's participation in the routine computer communications at issue in this case. And if the Ninth Circuit's erroneous decision is left uncorrected, its error threatens to upend common internet practices and chill the creativity that allows the internet to flourish. The petition for certiorari should be granted.

STATEMENT

A. The Wiretap Act

In 1968, decades before Facebook and other internet companies came into existence, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act, known as the Wiretap Act. Pub. L. 90-351, 82 Stat. 197. The Wiretap Act's core provision makes it unlawful for any person to "intentionally intercept[] … any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). But the Act also makes clear that it is not unlawful for a person—whether or not "acting under color of law"—"to intercept a … communication where such person is a party to the communication." *Id.* § 2511(2)(d); *see id.* § 2511(2)(c) (cognate provision for "person[s] acting under color of law"). The exemption of a "party" "reflect[s] existing [pre-1968] law," which provided that a "person actually participating in [a] communication" could not face liability for intercepting that communication. S. Rep. 90-1097, 1968 U.S.C.C.A.N. 2112, 2182 (1968).

The Act's substantive prohibitions carry both criminal and civil penalties. First, the Act subjects those who "intentionally intercept[]" communications to the possibility of five years' imprisonment. 18 U.S.C. § 2511(4)(a). Second, it allows those whose communications have been intercepted to sue the person or entity that committed the relevant violation. *Id.* § 2520(a). Plaintiffs may recover either "the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation," or "statutory damages of whichever is greater of $100 a day for each day of violation or $10,000." *Id.* § 2520(c)(2). And courts may award "punitive damages in appropriate cases," as well as "a reasonable attorney's fee." *Id.* § 2520(b)(2)-(3).

Congress's last major amendment to the Act came in 1986, when it "enlarged [the Act's] coverage … to prohibit the interception of 'electronic' as well as oral and wire communications." *Bartnicki v. Vopper*, 532 U.S. 514, 524 (2001). That amendment "update[d] and clarif[ied] Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. Rep. No. 99-541, at 1 (1986), *reprinted in* 1986 U.S.C.A.A.N. 3555, 3555. Those new technologies included "electronic mail operations, cellular and cordless telephones, [and] paging devices." H. Rep. 99-647, at 18 (1986).

Since 1986, the world has witnessed a remarkable evolution in communication technologies—most importantly, "the advent of the Internet and the World Wide Web." *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 874 (9th Cir. 2002). But Congress has not altered the Wiretap Act or curtailed its exemption from liability for parties to communications.

B. Factual Background

1. This case involves a common form of computer-to-computer communication, called a "GET request." 7ER1201.[1] GET requests take place whenever a person is browsing the internet using a web browser,

[1] "ER" refers to the Appellant's Excerpts of Record in the Ninth Circuit. Facebook draws on the allegations in plaintiffs'

such as Apple Safari or Microsoft Internet Explorer. *Id.* When the user seeks to visit a particular webpage, she types that webpage's address into the browser's navigation bar or clicks on a hyperlink. At that time, the browser sends a message to the server that hosts the requested webpage, asking the server to display the webpage on the person's computer. *Id.* That message from the browser to the webpage's server is called a "GET request"—effectively a request to get the relevant content. 7ER1201-02.

But the webpage's contents are not delivered by the server to the user in a single piece; rather, they consist of an assemblage of independent parts. 7ER1203. And many webpages include content that exists on different servers operated by third parties. *Id.* A common example of this third-party content is an advertisement. For instance, a NYTimes.com webpage may include content from not only the *New York Times*, but also from advertisers. These third-party advertisements are displayed in pre-arranged portions of the NYTimes.com webpage. *See* 7ER1203-04.

Third-party content providers, like advertisers, receive directions from users' browsers to display their content on the webpage the user is visiting. That direction occurs through a "separate but simultaneous GET command," also from the user's browser, but this time sent to the third-party server. 7ER1204.

second and third amended complaints and accompanying exhibits to describe the practices at issue for purposes of this petition, but it does not admit the veracity of all of these allegations.

Suppose a person browsing the internet seeks to visit NYTimes.com, and suppose that the NYTimes.com webpage she visits is designed to contain a third-party advertisement. To display the full webpage including the advertisement, the person's browser sends two separate GET requests. One is the GET request to the NYTimes.com server, asking the server to display the NYTimes.com webpage. The other, following a direction from the NYTimes.com webpage to seek third-party content, is a separate GET request to the third-party advertiser's server, asking it to display the relevant advertisement. *See, e.g.*, *In re Google*, 806 F.3d at 130 (describing this process for "internet advertising companies" that "serv[e] advertisements to the browsers of webpage visitors"). This entire process occurs in milliseconds. 7ER1204.

Because the third-party advertiser's server needs to know the webpage for which it is providing content, the GET request sent to the third party's server will generally contain the Uniform Resource Locator ("URL") of the webpage the internet user is visiting. *Id.* A URL is the familiar identifier that a person sees in her navigation bar when she visits a website—for instance, http://www.nytimes.com/business. 7ER1202-03. When sent to a third-party server, the URL is called a "referer header" because it refers the third-party server to the webpage the internet user is visiting. 7ER1204. If the third-party server did not receive the referer header, the relevant portion of the host webpage would appear blank. *See id.*

2. The other relevant technological concept in this case is "cookies." Cookies are small pieces of text that browsers and websites use to store information.

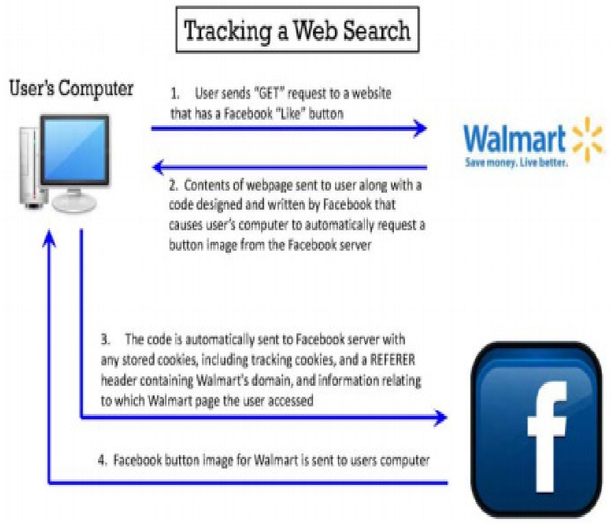
7ER1207. For instance, cookies enable websites to recognize users, which in turn allows the websites to keep users logged in and prevent unauthorized access to their accounts. 4ER614.

3. Facebook operates a social-media service with more than 2.4 billion users worldwide, including more than 200 million users in the United States. Facebook's users create personal profiles and share messages, photographs, videos, and content with the service's other users.

To enhance user experience, Facebook permits people or businesses to integrate "plug-ins," such as the Facebook "Like" or "Share" buttons, on their webpages. 4ER628; 7ER1207. Plug-ins consist of computer code that people or businesses can choose to embed on their webpages. For instance, an internet user visiting a NYTimes.com webpage may see, in addition to *New York Times* content and third-party advertisements, a Facebook "Like" button. Clicking that "Like" button enables the reader to seamlessly share the relevant *New York Times* content with her Facebook social network (rather than manually copying the link and sharing it directly on Facebook). Many other companies, like Twitter, Pinterest, and LinkedIn, have similar plug-ins that webpages may integrate.

When a person browsing the Internet visits a webpage with a Facebook plug-in, the person's browser engages in the two separate communications discussed above. 7ER1209. It sends one GET request to the server of the webpage being visited, asking it to display that webpage. *Id.* And after that server directs the user's browser to seek information from Facebook, the browser sends a "separate but simultaneous" GET request to Facebook, 7ER1204, asking it to display the plug-in on the webpage, 7ER1209. To instruct Facebook where to display the plug-in, the GET request sent to Facebook contains the referer header of the webpage being visited—*i.e.*, the webpage's URL. 7ER1210.

The following diagram (drawn from plaintiffs' complaint, 7ER1209) illustrates the GET request process:


Tracking a Web Search
User's Computer
1. User sends "GET" request to a website that has a Facebook "Like" button
Walmart
Save money. Live better.
2. Contents of webpage sent to user along with a code designed and written by Facebook that causes user's computer to automatically request a button image from the Facebook server
3. The code is automatically sent to Facebook server with any stored cookies, including tracking cookies, and a REFERER header containing Walmart's domain, and information relating to which Walmart page the user accessed
4. Facebook button image for Walmart is sent to users computer

This process occurs whether or not the internet user has a Facebook account, is logged in to Facebook, or has ever visited Facebook: it "is part of the normal operation of the Internet." 4ER635. If it did not occur, the portion of the webpage allocated to the plug-in would appear blank. 7ER1204.

As explained in its privacy policy, Facebook uses the information it receives from GET requests (such as the URLs a user visits) to show users "content from [their] friends that may interest [them]" and to "improve ads generally" on its service. 2ER140; *see* 2ER117-19.

C. Proceedings Below

1. Plaintiffs, four Facebook users, brought this case as a multi-district litigation on behalf of themselves and a putative nationwide class of people with active Facebook accounts between April 22, 2010 and September 26, 2011. 7ER1234. After the district court dismissed plaintiffs' first complaint with leave to amend, *see* App. 100a-101a, they filed a second amended complaint asserting eleven claims, including a violation of the Wiretap Act, 7ER1235-37.[2]

Plaintiffs' Wiretap Act claim alleges that while logged out of Facebook, plaintiffs visited websites containing Facebook plug-ins. 7ER1196; 7ER1223. When they visited those websites, plaintiffs allege, their browsers sent Facebook GET requests that included the websites' URLs. 7ER1237. According to plaintiffs, Facebook then employed "user-specific and user-identifying cookies" to "gather[]" these URLs. *Id.* Facebook's actions, plaintiffs contend, amount to unlawful "interception" of their data under the Wiretap Act. 7ER1235.

[2] Plaintiffs' other causes of action include a Stored Communications Act claim, 18 U.S.C. § 2701, as well as numerous state-law claims. *See* 7ER1237-1252.

Plaintiffs acknowledge that their browsers sent the URL data directly to Facebook, so that Facebook could display plug-ins on the webpages plaintiffs visited. 7ER1209. They also admit that their browsers' communications with Facebook were "separate from" their browsers' communications with the webpages they visited. 7ER1237. But plaintiffs maintain that Facebook was still not an "authorized party" to the communication through which it received URL data. 7ER1236. That is so, plaintiffs say, because plaintiffs did not "know[]" about their browsers' communication with Facebook and were logged out of Facebook when that communication occurred. *Id.*

Plaintiffs do not allege that Facebook represented to them that it would refrain from receiving URL data generally. Nor do plaintiffs allege that Facebook failed to accurately disclose its data-receipt practices as to *logged-in* users. 7ER1246. Rather, plaintiffs claim solely that Facebook's disclosures "implicitly promise[d]" that Facebook would not receive URL data about *logged-out* users. 7ER1089. And even as to that class of activity, plaintiffs assert only generalized privacy harms. 7ER1223-24. They do not assert that they engaged in different browsing behavior while logged out of Facebook, or that Facebook sold or disclosed any URL information it received.

Nevertheless, plaintiffs seek more than $15 billion in total damages. 5ER921.

2. The district court granted Facebook's motion to dismiss plaintiffs' second amended complaint, holding that plaintiffs failed to state a Wiretap Act claim. Facebook, the court concluded, was a "party to the [rele-

vant] communication," so it "did not 'intercept' Plaintiffs' communications within the meaning of the Wiretap Act." App. 63a (quoting 18 U.S.C. § 2511(2)(d)). "[W]hen someone visits a page where a Facebook 'like' button is embedded," the court explained, "two separate communications occur": "[f]irst, the user's browser sends a GET request to the server where the page is hosted"; "[s]econd," the "Facebook button triggers a second, independent GET request to Facebook's servers." *Id.* While "[t]he parties to the first transaction are the web user (e.g., one of the Plaintiffs) and the server where the page is located," the "[p]arties to the second transaction are that same web user and a Facebook server." *Id.* at 63a-64a. "As to the second transaction"—the only one in which URL data is sent to Facebook—"Facebook has not 'intercepted' the communication … because it is 'a party to the communication.'" *Id.* at 64a (quoting 18 U.S.C. § 2511(2)(d)).[3]

3. The Ninth Circuit reversed. After concluding that plaintiffs had standing to pursue their Wiretap Act claim, App. 11a-13a, the Ninth Circuit held that the claim could proceed because the "party" provision did not apply. The Ninth Circuit agreed with the district court that the "GET request and its associated [URL] referer header" sent from the user's browser to Facebook is the relevant communication through which Facebook receives a user's URL information—

[3] The district court likewise dismissed plaintiffs' other claims, though it granted leave to amend two of them. *Id.* at 72a-73a. After plaintiffs filed a third amended complaint asserting those two claims alone, the district court granted Facebook's motion to dismiss those claims without leave to amend. *Id.* at 53a.

i.e., the allegedly "intercepted" communication. *Id.* at 31a. And it agreed that the browser-to-Facebook communication is "separate" from the GET request sent from the browser to "the third-party website." *Id.* Nonetheless, the court held that Facebook was not a "party" to the supposedly "intercepted" communication and could face Wiretap Act liability. *Id.* at 33a.

The Ninth Circuit did not purport to base its conclusion on the Wiretap Act's text, which uses the unmodified term "party." Rather, the court based its conclusion on its view of the Act's purpose and legislative history. First, the court asserted that the Act's "paramount objective" is "protect[ing] effectively the privacy of communications." *Id.* (internal quotation marks omitted). Second, the court stated "that the Wiretap Act's legislative history evidences Congress's intent to prevent the acquisition of the contents of a message by an unauthorized third-party or 'an unseen auditor.'" *Id.* (quoting S. Rep. No. 90-1097, 1968 U.S.C.C.A.N. at 2154, 2182). In light of those two considerations, the court concluded that allowing the "party" provision to apply to "unauthorized duplication and forwarding of unknowing users' information" would allow too many "common methods of intrusion." *Id.*

In reaching this conclusion, the Ninth Circuit recognized that "the Third Circuit has held to the contrary." *Id.* at 32a. In *In re Google*, the court explained, the Third Circuit held that "internet advertising companies were parties to a communication" when they received "duplicated GET requests" from a web user's browser. *Id.* (citing *In re Google*, 806 F.3d at 143). But instead of following the Third Circuit, the Ninth Circuit "adopt[ed] the First and Seventh Circuits' understanding that simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception." *Id.* at 33a (citing *In re Pharmatrak*, 329 F.3d at 22; *Szymuszkiewicz*, 622 F.3d at 706).

The Ninth Circuit denied Facebook's petition for panel rehearing or rehearing en banc. *Id.* at 102a. This petition for certiorari follows.

REASONS FOR GRANTING THE PETITION

The Ninth Circuit acknowledged that its decision squarely conflicts with a Third Circuit decision, and that conflict reflects a wider disagreement in the circuits over the scope of the Wiretap Act's "party" provision. This Court should resolve the conflict—not only to restore uniformity on the meaning of an important federal statute, but also because the Ninth Circuit's decision is incorrect and casts doubt on the legality of common business practices integral to the internet's basic operation. Under the statutory text, Facebook was a "party" to the relevant communications because it was the sole designated recipient of GET requests from plaintiffs' web browsers, and those communications occurred by design, to display Facebook features embedded by the webpages plaintiffs visited. Facebook was not an uninvited interloper to a communication between two separate parties; it was a direct participant in communications with plaintiffs' browsers. In holding otherwise, the Ninth Circuit contravened basic interpretive principles by relying on legislative purpose and history rather than statutory text. And the impact of its error is stark: If allowed to stand, the decision could subject companies (including the many technology companies based in the Ninth Circuit) to the prospect of criminal and civil liability for engaging in commonplace, lawful business practices that enhance internet users' experiences.

A. The Courts Of Appeals Are Divided Over The Question Presented

1. Section 2511(2)(d) of the Wiretap Act provides that "[i]t shall not be unlawful … to intercept a wire, oral, or electronic communication where such person is a *party to the communication*." 18 U.S.C. § 2511(2)(d) (emphasis added). In the decision below, the Ninth Circuit held that an entity like Facebook that receives a request from an internet user's web browser to provide content to a particular webpage is not a "party to the communication" with the browser, where that request is "unknow[n]" to or "unauthorized" by the user. App. 33a.

In reaching its conclusion, the Ninth Circuit expressly rejected the Third Circuit's diametrically opposite interpretation of the Wiretap Act. *Id.* at 32a. The Third Circuit had addressed the same question about the meaning of a "party" in *In re Google*, 806 F.3d 125. There, the plaintiffs brought a class action against a group of internet advertisers, alleging that the advertisers violated the Wiretap Act by intercepting communications between the advertisers and plaintiffs' internet browsers. *Id.* at 140.

The Third Circuit held that the Act's "party" provision applied, precluding liability. As in this case, the defendants in *In re Google* allegedly "acquired the plaintiffs' internet [URL] history information by way of GET requests that the plaintiffs sent directly to the defendants." 806 F. 3d at 142. But unlike the Ninth Circuit, the Third Circuit held that "[b]ecause the defendants were the intended recipients of the transmissions at issue"—*i.e.*, "GET requests that the plaintiffs' browsers sent directly to the defendants' servers"—no liability could attach. *Id.* at 142-43. In contrast to the Ninth Circuit's atextual knowledge-and-authorization requirement, the Third Circuit focused on the "statutory language," which provides no indication that it excludes designated "recipients who procured their entrance to a conversation" without the sender's knowledge. *Id.* "[A] party to the conversation," the Third Circuit concluded, "is one who takes part in the conversation"—with or without the plaintiff's knowledge or authorization. *Id.* (quoting *Caro v. Weintraub*, 618 F.3d 94, 97 (2d Cir. 2010)).[4]

The difference between the interpretation of the Wiretap Act in the Third and Ninth Circuits is outcome determinative. Under Third Circuit law, a defendant that receives a GET request and accompanying URL information from a plaintiff's web browser is

[4] The Third Circuit reaffirmed its holding in *In re Nickelodeon Consumer Privacy Litigation*, 827 F.3d 262 (3d Cir. 2016). There, a class of plaintiffs alleged that Viacom and Google "unlawfully collected personal information about them on the Internet, including what webpages they visited and what videos they watched on Viacom's websites." *Id.* at 267. Relying on *In re Google*, the Third Circuit held that the plaintiffs had not stated a Wiretap Act claim because "Google was either a party to all communications with the plaintiffs' computers or was permitted to communicate with the plaintiffs' computers by Viacom, who was itself a party to all such communications." *Id.* at 274.

a "party" to the relevant communication and cannot face Wiretap Act liability. So in the Third Circuit, plaintiffs' Wiretap Act claim against Facebook would have been dismissed. But because plaintiffs sued in the Ninth Circuit, their claim can proceed, subjecting Facebook to the risk of massive statutory damages.

2. The square conflict between the Third and Ninth Circuits is part of a wider disagreement in the circuits over how the Wiretap Act applies to communications in which one entity's participation is not fully known or authorized by the other entity.

The Ninth Circuit expressly "adopt[ed]" what it perceived to be "the First and Seventh Circuits' understanding that simultaneous, unknown duplication and communication of GET requests do not exempt a defendant from liability under the party exception." App. 33a. In *In re Pharmatrak, Inc.*, 329 F.3d 9, the First Circuit held that where plaintiff internet "users communicated simultaneously with [a] pharmaceutical client's web server and with [defendant's] web server" through "the get method," so that both servers could "contribute[] content for the succeeding webpage," the defendant "intercepted" the URL information that the plaintiffs sent to it. *Id.* at 22. Like the Ninth Circuit, the First Circuit deemed it immaterial that "two separate communications" took place—one of which was sent directly to the defendant at the webpage's instruction—reasoning that liability can attach where those communications are "simultaneous" and the plaintiff did not know about the one sent to the defendant. *Id.*

And in *Szymuszkiewicz*, 622 F.3d 701, the Seventh Circuit held that a defendant "intercepted" communications through a program directing an email server to "contemporaneous[ly]" transmit to him all messages sent to another person, without that person's knowledge. *Id.* at 706. This conduct differs from the GET requests here and in *In re Pharmatrak*, which provide essential content to webpages a user visits; the *Szymuszkiewicz* defendant's program had no functional role in the user's internet experience at all. But the Ninth Circuit believed that the Seventh Circuit's approach supported its holding here. App. 31a-33a.

In contrast, the Fifth, Sixth, and Second Circuits have rejected the principle—endorsed by the decision below—that a defendant's "unauthorized" or "unknow[n]" participation in a communication renders the "party" provision inapplicable. *Id.* at 33a. While these circuits did so outside the context of computer-to-computer communications, the rationale of their decisions would have required ruling for Facebook here. Recognizing as much, the Third Circuit relied on two of these decisions in *In re Google*. 806 F.3d at 143-44 (citing *Caro*, 618 F.3d at 97; *United States v. Campagnuolo*, 592 F.2d 852, 863 (5th Cir. 1979)).

In *Campagnuolo*, 592 F.2d 852, a police officer answered phone calls while validly present in a criminal suspect's home to execute a search warrant, permitting the callers to assume that he was the suspect himself. *Id.* at 861-62. Even though the callers did not know they were communicating with a police officer, or authorize those communications, the Fifth

Circuit held that the "officer [was] a party" to the communications because he directly "answer[ed] [the] ringing telephone." *Id.* at 862-63.

The Sixth Circuit reached the same conclusion in *United States v. Passarella*, 788 F.2d 377 (6th Cir. 1986). There, too, a police officer answered phone calls while validly present in a suspect's home, without notifying the callers of his identity. *Id.* at 379. And there, too, the court held that the Wiretap Act's "party" provision applied, without employing the knowledge-and-authorization test that the Ninth Circuit fashioned based on its perception of legislative history and purpose. *Id.*

Similarly, in the Second Circuit's *Caro* decision, 618 F.3d 94, the defendant entered a room while a conversation was ongoing, "placed his iPhone on [a] table and, unbeknownst to [plaintiff], used the device to record the conversation." *Id.* at 96. The plaintiff argued that the defendant was not a "party" to the conversation because he had not been "invite[d] … to join [it]." *Id.* at 97. Rejecting "the proposition that one must be invited to a conversation in order to be a party to it," the court held that the defendant "was a party to the conversation for purposes of the Wiretap Act." *Id.*

3. The entrenched split on computer-to-computer communications alone warrants review. Three circuits—the First, Seventh, and Ninth—hold that a defendant can face liability for "interception" when partaking in a computer-to-computer communication that a plaintiff does not know of or authorize. The Third Circuit holds to the contrary. And because a large portion of technology companies are based in the

Ninth Circuit, plaintiffs will frequently have the ability and incentive to sue there to take advantage of the plaintiff-friendly law. The availability of a favorable Ninth Circuit forum will likely restrict the development of the law elsewhere.

The more general conflict over the Wiretap Act's "party" provision underscores the need for the Court's intervention. Four circuits hold that unknown or unauthorized participants can be "parties" under the Act, and three circuits hold the opposite. Only this Court can resolve that disagreement.

B. The Ninth Circuit's Interpretation Of The Wiretap Act Is Incorrect

Review is also warranted to correct the Ninth Circuit's erroneous decision. The decision below defies this Court's statutory-interpretation teachings by exalting perceived legislative purposes over text.

1. "[I]n any statutory construction case," a court must "start, of course, with the statutory text." *Sebelius v. Cloer*, 569 U.S. 369, 376 (2013) (quoting *BP Am. Prod. Co. v. Burton*, 549 U.S. 84, 91 (2006)). The Wiretap Act provides that an entity cannot be liable for intercepting a communication where that entity "is a party to the communication." 18 U.S.C. § 2511(2)(d). At a minimum, a "party to [a] communication" includes the sole designated recipient of the information conveyed. *See Party*, Merriam-Webster Online Dictionary (last visited Nov. 17, 2020) ("person or group participating in an action or affair"); *Party*, Black's Law Dictionary (11th ed. 2019) ("[s]omeone who takes part in a transaction"); *Party*, American Heritage Dictionary (2d ed. 1985) ("[a] participant").

And "[i]n the case of a computer network, [a] party to the communication" includes "the end recipient of the communication." 2 Wayne R. LaFave et al., Criminal Procedure: Detection and Investigation of Crime, § 4.6(l).

Facebook was a "party" to the relevant communication here. When plaintiffs navigated to webpages that had elected to integrate Facebook plug-ins, two distinct and contemporaneous communications occurred. 7ER1204; 7ER1209. First, plaintiffs' web browsers sent a GET request to the webpage plaintiffs sought to visit. 7ER1209. Second, after receiving a message from the webpage that a Facebook plug-in was necessary to complete the page on the user's screen, plaintiffs' browsers sent a "separate but simultaneous" GET request to Facebook. 7ER1204. That browser-to-Facebook communication contained URL information—necessary so that Facebook could load the plug-in on the proper page—and that is the communication that plaintiffs assert violated the Wiretap Act. 7ER1204; 7ER1235.

But Facebook was a "party" to that communication because it was the sole designated recipient of the relevant GET request and URL information sent by plaintiffs' browsers. And that browser-to-Facebook communication served an important purpose: to enable Facebook to provide features that a website had chosen to incorporate on a webpage that the user had requested to visit. Facebook was not an interloper to a separate communication between two entities communicating solely with each other.[5] Accordingly, Facebook's receipt of URL information cannot violate the Wiretap Act. That should be the end of the matter: where "the words of a statute are unambiguous," the "judicial inquiry is complete." *Barnhart v. Sigmon Coal Co.*, 534 U.S. 438, 461-62 (2002) (internal quotation marks omitted).

The Ninth Circuit reached the opposite conclusion because it did not ground its interpretation in the statutory text. It never isolated the relevant communication and asked whether Facebook was a "party" to that communication, under "a careful examination" (or any examination) of that word's "ordinary meaning." *Food Marketing Inst. v. Argus Leader Media*, 139 S. Ct. 2356, 2364 (2019). It instead adopted a policy-based rule that a defendant cannot be a "party" to a communication—even if it is the sole designated recipient of information from the sender—if the plaintiff does not know of or authorize that communication. App. 33a. But under that rule, "party" status would seemingly depend on a plaintiff's subjective understanding of a communication. Congress would not have intended that result: where the Wiretap Act seeks to distinguish between known and unknown

[5] The same result would follow even if plaintiffs had alleged that Facebook was participating in the communication between the users' browsers and the webpages they visited. Those webpages consented to Facebook's receipt of the URL information when they elected to incorporate a Facebook plug-in, precluding liability. *See In re Nickelodeon*, 827 F.3d at 274; 18 U.S.C. § 2511(2)(d) (no Wiretap Act liability "where one of the parties to the communication has given prior consent").

communications, it does so explicitly. *See* 18 U.S.C. § 2510(2) (defining "oral communication" to include non-electronic communications "uttered by a person exhibiting an *expectation that such communication is not subject to interception*" (emphasis added)).

Rather than engaging with the text, the Ninth Circuit rested its decision on the Act's "paramount objective" and "legislative history." App. 33a (internal quotation marks omitted). But, as this Court frequently emphasizes, "even the most formidable argument concerning [a] statute's purposes [can]not overcome" clear statutory "text." *Kloeckner v. Solis*, 568 U.S. 41, 55 n.4 (2012). The Ninth Circuit's approach harkens back to "a bygone era of statutory construction" when courts "inappropriately resort[ed] to legislative history before consulting the statute's text and structure." *Food Marketing Inst.*, 139 S. Ct. at 2364.

2. What is more, the Ninth Circuit's analysis of the Wiretap Act's purpose and history is flawed.

a. The Ninth Circuit proclaimed that the Wiretap Act's "paramount objective … is to protect effectively the privacy of communications." App. 33a (internal quotation marks omitted). But while protecting privacy is *one* of the Wiretap Act's purposes, it is not the only one. The Act's drafters sought to strike a "balance between the privacy expectations of citizens" and other interests, including preserving "technologies that hold such promise for the future." H. Rep. 99-647, at 18. That is why the Act does not flatly ban all interceptions of communications, but instead expressly eliminates liability for a "party" to a communication.

b. The Ninth Circuit also observed "that the Wiretap Act's legislative history evidences Congress's intent to prevent the acquisition of the contents of a message by an unauthorized third-party or 'an unseen auditor.'" App. 33a (quoting S. Rep. No. 90-1097, 1968 U.S.C.C.A.N. at 2154, 2182). This rationale improperly elevates one line of legislative history discussing the Act's broad purpose over the specific lineage of the "party" provision—the relevant provision here. In fact, the one line that the Ninth Circuit quoted is self-evidently irrelevant to the "party" provision: it focuses on "*third-party* … auditor[s]," not direct and designated recipients of a communication.

Had the Ninth Circuit focused on the "party" provision's history, it would have reached a different result. Congress's inclusion of the "party" provision in the 1968 Wiretap Act "reflec[ted] existing law." S. Rep. No. 90-1097, 1968 U.S.C.C.A.N. at 2182. Under existing federal law, "party" meant "the person actually participating in the communication." *Id.* As an illustration of existing law, the Senate Report cites *United States v. Pasha*, 332 F.2d 193 (7th Cir. 1964), which held that a police officer who impersonated the intended recipient of a phone call did not violate applicable federal wiretapping statutes. S. Rep. No. 90-1097, 1968 U.S.C.C.A.N. at 2182. Because *Pasha* held that obtaining information through unknown and unauthorized participation was permissible, and Congress sought to codify *Pasha* in the "party" provision, that provision must encompass unknown and unauthorized participants. *Accord Lorillard v. Pons*, 434 U.S. 575, 580 (1978) ("Congress is presumed to be aware of a[] [relevant] judicial interpretation" and "to adopt that interpretation"). In reaching the opposite conclusion, the Ninth Circuit overlooked the "party" provision's pedigree.[6]

3. Even if there were ambiguity about whether the "party" provision applies to Facebook in this case (there is not), that ambiguity must be construed in Facebook's favor under the rule of lenity. Although this case involves a civil class-action suit, § 2511(1)'s "interception" prohibition can carry criminal consequences. 18 U.S.C. § 2511(4)(a) ("whoever violates subsection (1) of this section shall be fined under this title or imprisoned not more than five years, or both"). And because the Court "must interpret the statute consistently, whether [the Court] encounter[s] its application in a criminal or noncriminal context, the rule of lenity applies." *Leocal v. Aschroft*, 543 U.S. 1, 11 n.8 (2004); *see United States v. Thompson/Center Arms Co.*, 504 U.S. 505, 517-18 (1992) (plurality opinion) (applying rule of lenity because "although it is a tax statute that we construe now in a civil setting, [it] has criminal applications"); *see also Clark v. Martinez*, 543 U.S. 371, 380-81 (2005). Under the rule of

[6] Courts that have rejected the Ninth Circuit's view have recognized that Congress sought to incorporate *Pasha*'s holding in the "party" provision. *See In re Google*, 806 F.3d at 144 ("We agree with the Sixth Circuit and the Fifth Circuit that, '[b]y citing *Pasha*, Congress strongly intimated that one who impersonates the intended receiver of a communication may still be a party to that communication for the purposes of the federal wiretap statute and that such conduct is not proscribed by the statute.'" (citing *Clemons v. Waller*, 82 F. App'x 436, 442 (6th Cir. 2003); *Campagnuolo*, 592 F.2d at 863)).

lenity, if an application of the traditional tools of statutory interpretation leaves the Court "with an ambiguous statute," *Shular v. United States*, 140 S. Ct. 779, 787 (2020) (internal quotation marks omitted), it must adopt the more lenient interpretation. To the extent that ambiguity remains about whether Facebook was a "party" to the communication in this case, the Court should decline to impose an atextual rule that *expands* liability. The Ninth Circuit's decision is erroneous for this reason as well.[7]

C. The Decision Below Raises Issues Of Exceptional Importance

1. The decision below carries enormous consequences for the internet and technology industry. Any time an internet user visits a webpage with third-party content—like an advertisement, social-media plug-in, shopping cart, embedded map, or PayPal integration—a GET request like the ones challenged in this case occurs. Recent studies suggest that approximately 88% of the most frequently visited webpages contain such third-party content.[8] And those content

[7] As Justice Kavanaugh has noted, the Court has varied in its rule-of-lenity cases between requiring "ambiguity" and "grievous ambiguity." *Shular*, 140 S. Ct. at 788 (Kavanaugh, J., concurring). But the rule's purposes support a simple ambiguity test: the rule protects citizens from punishment that is not "clearly prescribed" and encourages Congress to clarify the law while preventing courts from inventing it "in Congress's stead." *United States v. Santos*, 553 U.S. 507, 514 (2008) (plurality opinion of Scalia, J.).

[8] *See* Timothy Libert, *Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites*, Int'l

providers commonly use cookies to store referer header data and thereby improve the content they deliver to users. *See, e.g.*, *In re Nickelodeon*, 827 F.3d at 268 ("Advertising companies use … cookies to help them target advertisements more effectively at customers"); *Netscape Commc'ns Corp. v. ValueClick, Inc.*, 684 F. Supp. 2d 678, 682 (E.D. Va. 2009) ("cookies technology [is] ubiquitous, and plays a large role in Internet users' Web browsing").[9] The Ninth Circuit's decision means that internet companies can now face not only class-wide statutory damages, but also criminal liability, for these ordinary business practices.

Class-action plaintiffs and their attorneys are quickly seeking to capitalize on the Ninth Circuit's decision.[10] Already, two Wiretap Act class actions have

Journal of Communication, at 5, Oct. 2015, https://arxiv.org/abs/1511.00619.

[9] *See also* Aaron Cahn et al., *An Empirical Study of Web Cookies*, International World Wide Web Conference Committee, at 894, Apr. 2016, https://dl.acm.org/doi/abs/10.1145/2872427.2882991 (finding that 68% of cookies were used by third-party content providers, which "can largely be attributed to the adoption and popularity of 3rd party services such as targeted advertising, site analytics, and social media widgets").

[10] *See* Erik Manukyan, *Summary: Ninth Circuit Permits Federal Wiretap Act Claim Against Facebook*, LawFare (Apr. 24, 2020), https://www.lawfareblog.com/summary-ninth-circuit-permits-federal-wiretap-act-claim-against-facebook ("enterprising plaintiffs' attorneys may see [the Ninth Circuit's] ruling as a signal to start preparing data privacy lawsuits challenging other industry practices and seeking lucrative settlements (if not judgments) in the Ninth Circuit").

been asserted against leading internet companies in California federal district court. In *Rodriguez v. Google*, No. 3:20-cv-4688 (N.D. Cal.) (filed July 14, 2020), the putative class of plaintiffs asserts that Google's alleged receipt of consumer data through mobile applications and a private internet browser violates the Act, *id.* ECF 1; *see id.* ECF 60 (amended complaint also alleging Wiretap Act violation).[11] Google's alleged practices involve the same computer-to-computer GET request communications at issue here. *Id.* ECF 1, ¶¶ 23, 33; *id.* ECF 60, ¶ 49. And the plaintiffs' complaint—evidently relying on the Ninth Circuit's decision in this case—maintains that "Google was not an authorized party to the communication because Plaintiffs were unaware of Google's collection of [data]" and "did not knowingly send any of the communication to Google." *Id.* ECF 1, ¶ 119; *accord* ECF 60, ¶ 244 (same).

Similarly, in *Russo v. Microsoft*, No. 4:20-cv-04818 (N.D. Cal.) (filed July 17, 2020), the putative class of plaintiffs asserts that Microsoft's alleged receipt of consumer data through the Office 365 and Exchange Online programs violates the Act, *id.* ECF 1.[12] There, too, the plaintiffs' complaint contends that "Microsoft

[11] *See* Daisuke Wakabayashi, *Suit Claims Google's Tracking Violates Federal Wiretap Law*, N.Y. Times (June 2, 2020), https://www.nytimes.com/2020/06/02/technology/google-sued-wiretap-privacy.html (describing the lawsuit).

[12] *See* Hannah Albarazi, *Microsoft Accused of Giving Business User Data to Facebook*, Law 360 (July 20, 2020), https://www.law360.com/articles/1293487/microsoft-accused-of-giving-business-user-data-to-facebook (describing this lawsuit).

is not the intended recipient of the electronic communications and is not a party to those communications." *Id.* ¶ 143.

Unless this Court intervenes and corrects the Ninth Circuit's erroneous statutory interpretation, suits like these will only proliferate in that circuit—again, the home of the Nation's top internet and technology companies.

2. The Ninth Circuit noted that Facebook no longer engages in the practice that plaintiffs challenge in this case, *viz.*, recording and associating URLs with logged-out users through website plug-ins to the same extent that it does with logged-in users. App. 8a. But that fact does not detract from the impact of the decision below on Facebook and other internet companies. As explained, these companies still routinely engage in the same type of computer-to-computer communications at issue here whenever a webpage contains third-party content.[13] And they still use cookies to receive data from browsers and websites and thereby better customize user experiences.[14] The prospective importance of the decision

[13] *See What Information Does Facebook Get When I Visit a Site With the Like Button?*, Facebook, https://m.facebook.com/help/186325668085084 (explaining Facebook's current use of the "Like" button).

[14] *See Cookies & Other Storage Technologies*, Facebook, https://www.facebook.com/policy/cookies/ (explaining Facebook's current use of cookies technology).

below is confirmed by the allegations in the two recently filed class actions against Microsoft and Google.[15]

And even beyond affecting current practices, the Ninth Circuit's decision will stifle future technological advancement. The technology sector is fueled by innovation, as companies constantly aim to enhance and customize user experiences. Those efforts almost invariably involve both computer-to-computer communications and cookies: these practices are what allow companies to share and receive user data, which can then be employed to tailor content to users. Companies now face staggering potential liability for engaging in these practices.

3. In addition to its practical significance, the question presented has immense doctrinal significance. Lower courts have long lamented the difficulties of applying the Wiretap Act—passed before "the advent of the Internet and the World Wide Web"—to "modern forms of communication." *Konop*, 302 F.3d at 874; *see In re Pharmatrak*, 329 F.3d at 21; *United States v. Steiger*, 318 F.3d 1039, 1047 (11th Cir. 2003).

[15] Host websites or third-party content providers may obtain consent to communicate with users' browsers and employ cookies, precluding Wiretap Act liability. *See* 18 U.S.C. § 2511(2)(d). But consent will not always exist or be straightforward to ascertain, making the bright-line "party" question of first-order importance. *See, e.g.*, *Nguyen v. Barnes & Noble Inc.*, 763 F.3d 1171, 1177 (9th Cir. 2014) (absent "evidence that the website user had actual knowledge of the agreement, the validity of the … agreement turns on whether the website puts a reasonably prudent user on inquiry notice of the terms of the contract") .

And legal scholars have emphasized that the Act's application to the "surveillance of websurfing" is "a particularly tricky and important … problem."[16] This Court has not yet decided a case addressing the Wiretap Act's application to internet communications. Doing so here would provide much-needed guidance to lower courts.

D. This Case Is An Ideal Vehicle To Resolve The Question Presented

This petition raises a purely legal question without any complicating factual issues. The Ninth Circuit ruled, purely as a matter of statutory interpretation, that plaintiffs' Wiretap Act claim can proceed because an entity cannot be a "party" to a communication with another person who does not know of or authorize the entity's involvement. If that understanding of the Act is incorrect, plaintiffs' claim fails.[17]

[16] Orin Kerr, *Websurfing and the Wiretap Act*, The Washington Post (June 4, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/websurfing-and-the-wiretap-act/; *see also* Orin Kerr, *Websurfing and the Wiretap Act, Part 2: The Third Circuit's Ruling*, The Washington Post (Nov. 9, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/11/19/websurfing-and-the-wiretap-act-part-2-the-third-circuits-ruling/ (calling the Third Circuit's decision in *In re Google* "a very important opinion on Internet surveillance law").

[17] The Ninth Circuit also held that plaintiffs have Article III standing to raise their Wiretap Act claim. App. 11a-13a. The presence of a standing issue in the lower court decision does not militate against a grant of certiorari. Standing issues are likely to be litigated (or addressed sua sponte) in any case presenting the Wiretap Act question here because plaintiffs will generally assert intangible, non-economic harms. For that reason, the

That the Ninth Circuit remanded for further proceedings does not counsel against immediate review. Because of the Wiretap Act's draconian penalty scheme—which authorizes punitive damages and statutory damages of $100 per *day* of violation across class members, 18 U.S.C. § 2520(c)(2)—claims that survive past the motion-to-dismiss stage place enormous settlement pressure on defendants. In any event, this Court has often and recently granted certiorari in cases after a court of appeals has reversed a judgment in favor of defendants and remanded for further proceedings. *See, e.g.*, *Intel Corp. Inv. Policy Comm. v. Sulyma*, 140 S. Ct. 768, 775 (2020); *Apple Inc. v. Pepper*, 139 S. Ct. 1514, 1519-20 (2019). And this case—presenting a critical statutory issue at the center of the modern internet, with vast capacity to upend routine practices and dampen innovation, and reflecting a deep circuit conflict—provides a paradigmatic case for this Court's review.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Third Circuit also addressed standing in *In re Google*, finding that the plaintiffs there satisfied Article III's requirements. 806 F.3d at 134-35.

Respectfully submitted,

Michael R. Dreeben
Ephraim McDowell
O'MELVENY & MYERS LLP
1625 Eye Street, N.W.
Washington, D.C. 20006
(202) 383-5300

Jeffrey L. Fisher
Counsel of Record
O'MELVENY & MYERS LLP
2765 Sand Hill Road
Menlo Park, CA 94025
(650) 473-2633
jlfisher@omm.com

Yaira Dubin
O'MELVENY & MYERS LLP
Times Square Tower
7 Times Square
New York, N.Y. 10036
(212) 326-2000

November 20, 2020