No. 20-727

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

BRIEF FOR INTERNET ASSOCIATION, CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA, SOFTWARE AND INFORMATION INDUSTRY ASSOCIATION, AND COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION AS AMICI CURIAE IN SUPPORT OF PETITIONER

PATRICK J. CAROME
Counsel of Record
ARI HOLTZBLATT
AMY LISHINSKI
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Ave., NW
Washington, DC 20006
(202) 663-6000
patrick.carome@wilmerhale.com

ADDITIONAL COUNSEL LISTED ON INSIDE COVER

Jonathan Berroya
Internet Association
660 North Capitol St., NW
Suite 200
Washington, DC 20001
(202) 869-8680
jonathan@
internetassociation.org

Daryl Joseffer
Tara S. Morrissey
U.S. Chamber Litigation
Center
1615 H St., NW
Washington, DC 20062
(202) 463-5337
tmorrissey@uschamber.com

Christopher Mohr
Software and Information
Industry Association
1090 Vermont Ave., NW
Washington, DC 20005
(202) 289-7442
cmohr@siia.net

Matthew Schruers
Computer and
Communications
Industry Association
25 Massachusetts Ave., NW
Suite 300C
Washington, DC 20001
(202) 470-3620
mschruers@ccianet.org

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.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES AND RULES

OTHER AUTHORITIES[*]

[*] All websites last visited December 28, 2020.

TABLE OF AUTHORITIES—Continued

Page(s)

Inspect Network Activity In Microsoft Edge DevTools, Microsoft (Dec. 11, 2020), https://docs.microsoft.com/en-us/microsoft-edge/devtools-guide-chromium/network/ 8

Libert, Timothy, *Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites*, Int'l J. Commc'n (Oct. 2015), https://arxiv.org/abs/1511.00619 12

Mayer, Jonathan R. & John C. Mitchell, *Third-Party Web Tracking: Policy and Technology*, in *2012 IEEE Symposium on Security and Privacy* 415 (2012), https://ieeexplore.ieee.org/document/6234427 14

Moradi, Mohammad, et al., *CAPTCHA And Its Alternatives*, 8 Security and Communication Networks 12 (2015), https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1157 14

Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies (Nov. 8, 2016), https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-06.pdf 17

Open Microsoft Edge DevTools, Microsoft (Dec. 18, 2020), https://docs.microsoft.com/en-us/microsoft-edge/devtools-guide-chromium/open/?tabs=cmd-Windows 8

TABLE OF AUTHORITIES—Continued

Page(s)

Payment Gateway, Wikipedia, https://en.wikipedia.org/wiki/Payment_gateway 13

Schelter, Sebastian & Jerome Kunegis, *Tracking the Trackers: A Large-Scale Analysis of Embedded Web Trackers*, Tenth International AAAI Conference on Web and Social Media (Mar. 2016), https://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13024 12

Supreme Court of the United States, Electronic Filing System, https://file.supremecourt.gov/Account/Register 13

United States Senate, *Women of the Senate*, https://www.senate.gov/artandhistory/history/People/Women/Women-of-the-Senate.htm 16

University of Michigan, Vice President for Communications, *Dentistry During COVID-19: Engineering Anlaysis Offers Guidelines to Reduce Exposure* (Dec. 8, 2020), https://news.umich.edu/dentistry-during-covid-19-engineering-analysis-offers-guidelines-to-reduce-exposure/ 7, 8

Webster's Third New International Dictionary (1986) 22

TABLE OF AUTHORITIES—Continued

Page(s)

Yen, Ting-Fang, et al., *Host Fingerprinting and Tracking on the Web: Privacy and Security Implications*, in *Proceedings of the 19th Annual Network and Distributed System Security Symposium* (Feb. 8, 2012), https://www.ndss-symposium.org/ndss2012/ndss-2012-programme/host-fingerprinting-and-tracking-web-privacy-and-security-im plications/ 19

Zheng, Guangzhi & Svetlana Peltsverger, *Web Analytics Overview*, in *Encyclopedia of Information Science and Technology* 7674 *(*Mehdi Khosrow-Pour ed., 3d ed. 2015), https://www.researchgate.net/publication/272815693_Web_Analytics_Overview 17

BRIEF FOR INTERNET ASSOCIATION, CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA, SOFTWARE AND INFORMATION INDUSTRY ASSOCIATION, AND COMPUTER AND COMMUNICATIONS INDUSTRY ASSOCIATION AS AMICI CURIAE IN SUPPORT OF PETITIONER

Amici curiae respectfully submit this brief in support of Facebook, Inc.'s petition for a writ of certiorari.[1]

INTEREST OF AMICI CURIAE

The Internet Association ("IA") represents over 40 of the world's leading internet companies. IA's mission is to foster innovation, promote economic growth, and empower people through a free and open internet.

The Chamber of Commerce of the United States of America is the world's largest business federation. It represents the interests of more than three million businesses of every size, from every region of the country, and in every industry, including the internet and technology sectors.

The Software and Information Industry Association ("SIIA") is the principal trade association for the software and digital information industries. SIIA's membership includes more than 700 software companies, search engine providers, data and analytics firms, information service companies, and digital publishers that serve nearly every segment of society.

[1] No counsel for a party authored this brief in whole or in part, and no entity or person, other than amici curiae, their members, and their counsel, made a monetary contribution intended to fund the preparation or submission of this brief. Counsel of record for the parties received notice of amici's intent to file this brief at least 10 days prior to its due date, and all parties consented to the filing of this brief.

The Computer & Communications Industry Association ("CCIA") represents a broad cross section of communications and technology firms. For nearly fifty years, CCIA has promoted open markets, open systems, and open networks.

Amici are strongly interested in the proper interpretation of the Wiretap Act as it applies to internet communications. The technology challenged in this case enables countless daily internet communications. The Ninth Circuit's decision threatens to outlaw these everyday communications, impeding critical functions and security mechanisms that currently enable website publishers to present a rich array of content drawn from across the web on a single, integrated webpage. Amici submit this brief to demonstrate the wide range of common, innocuous conduct that is threatened by the Ninth Circuit's decision.

INTRODUCTION

This case involves one of the most fundamental and common technologies of the internet, one that undergirds much of how people experience the web today. When a person visits a webpage, the person's web browser displays a single unified page. But the content on the page is rarely drawn from a single server. Behind the scenes, the browser requests content from many different servers across the internet and then slots each component into place, presenting a seamless webpage.

This method of assembly has distinct advantages. It provides a richer, more dynamic experience to people surfing the web, with videos, maps, social media widgets, and other useful functions appearing alongside, or as an integral part of, content created by the website publisher itself. And it eases the burden on publishers of websites, who can weave their content together with content or services provided by others, rather than having to build every component of a website from scratch.

The decision below threatens all of this. In this case, plaintiffs alleged that they visited non-Facebook webpages that contained a "like" button provided by Facebook. As is typical, those webpages instructed plaintiffs' browsers to load the "like" button directly from a server operated or controlled by Facebook. In so doing, the browsers also transmitted to the Facebook server the address of the webpage (i.e., uniform resource locator, or URL). Facebook compiled the data it received in this way and used it to tailor its services. Even though plaintiffs' browsers sent the data directly to Facebook as an integral part of displaying the webpages plaintiffs were visiting, the Ninth Circuit held that Facebook could be subject to liability under the Wiretap Act.

In so holding, the Ninth Circuit pointed to features of the communications to Facebook that could scarcely be more common on the web. First, the Ninth Circuit emphasized that the communications were sent to Facebook's server, rather than the server that hosted the webpage the person was visiting. Pet.App. 31a. Second, the communications included the address of that webpage. *Id.* And third, the Ninth Circuit deemed the communications to be "unauthorized" in that the person was unaware that Facebook was receiving this information. Pet.App. 33a.

Communications with these same features are ubiquitous across the web; indeed, they underlie much of how the modern web operates. Modern webpages very rarely load from a single server operated or controlled by the webpage's publisher; instead, the visitor's browser is often instructed to request content or data from one or more *additional* servers. Those communications commonly contain information about the webpage being visited. And, by design, the entire process is seamless; the fact that these multiple sets of computer-to-computer communications emanate from the visitor's computer is typically not apparent to the visitor.

If communications with these features can amount to an illegal wiretap, then a vast quantity of everyday online communications could violate a criminal statute. The Ninth Circuit's decision thus imperils a whole universe of conduct, and its impact is not limited to the context of collecting user data for tailoring advertisements and recommendations. Any webpage that includes content loaded from one or more servers controlled by an entity other than the host of the webpage—which includes nearly every webpage—could trigger a Wiretap Act violation under the Ninth Circuit's analysis.

The petition for certiorari ably explains the errors in the Ninth Circuit's decision and the conflict with decisions of other circuits. This brief will explain in greater detail the technology underlying the challenged conduct and the practical implications of the Ninth Circuit's decision. The Ninth Circuit's erroneous interpretation of the Wiretap Act threatens to criminalize computer-to-computer communications that are common and fundamental to the operation of modern webpages. The Court should grant certiorari on this important issue, which has divided the courts of appeals.

STATEMENT

At its most basic level, the World Wide Web is a global filing cabinet, by which people connected to the internet may retrieve content from wherever it is stored. *See In re DoubleClick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 501 (S.D.N.Y. 2001). People typically access the web via browsers. A browser is a computer program on a person's computer, which communicates with other computers known as servers. *See generally* Gralla, *How The Internet Works* 145 (6th ed. 2002). Servers store the data that make up the web—in the form of "text, visual images, audio clips, and other information media"—and make it available over the internet. *In re Doubleclick*, 154 F. Supp. 2d at 501; *see also* Gralla, *supra*, at 25, 173.

When a person enters a webpage's address into his or her browser, the browser sends a request to the server at that address for the appropriate webpage. This request is typically a GET request—an instruction for the server to provide some content. *See* Fielding & Reschke, *RFC 7231: Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*, § 4.3.1 Internet Engineering Task Force (June 2014).[2] This brief will refer to a GET request sent from the browser to the server that hosts the webpage a person has requested as a "primary GET request."

All GET requests include information about the context of the request. *See* Fielding, *supra*, at §5.5. This typically includes a user-agent field, which provides the IP address of the computer sending the GET request. Fielding, *supra*, at § 5.5.3. It also typically

[2] https://tools.ietf.org/html/rfc7231#section-4.3.1

includes what is called a "referer header."[3] A referer header is the uniform resource locator (URL) of the webpage that "refer[red]" the browser to the content the GET request seeks. *Id.* § 5.5.2.[4] So, for example, when a person clicks a link that appears on the New York Times' website, her browser sends a primary GET request to the server that hosts the requested webpage, and that GET request includes a referer header with the URL of the New York Times webpage that contained the link.

The host server responds to the GET request by transmitting a file back to the person's browser. *In re DoubleClick*, 154 F. Supp. 2d at 501. This file is, in essence, a recipe for the webpage requested. *See* Gralla, *supra*, at 134-137. It describes what ingredients are needed, where those ingredients may be found, and how those ingredients should be combined in order to generate and display the webpage in question. *Id.*; *see also Perfect 10, Inc.* v. *Amazon, Inc.*, 508 F.3d 1146, 1155 (9th Cir. 2007).

After receiving the "recipe" for the webpage, the browser makes a series of requests to collect the other "ingredients" it needs to render the webpage. The content may be transmitted either from the server hosting the webpage, or from other servers. *See Perfect 10*, 508 F.3d at 1156. As discussed in greater detail below, the "recipe" file often instructs the browser to issue new

[3] The persistent misspelling of referrer is a quirk of history: In certain foundational HTTP documents, an r was inadvertently omitted, and the spelling stuck. *See* HTTP Referer, Wikipedia, https://en.wikipedia.org/wiki/HTTP_referer.

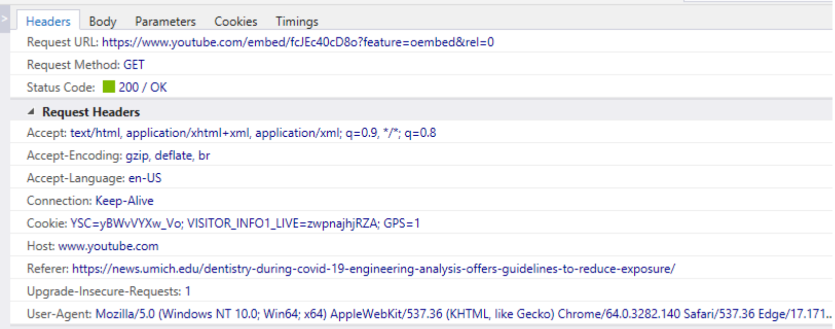
[4] A URL is a combination of characters, adhering to a standardized format, which refer to a webpage (or other content) by its location. *See* Gralla, *supra*, at 165.

GET requests—which this brief will refer to as "secondary GET requests"—to obtain content from servers other than the server hosting the webpage. These secondary GET requests are necessary to the rendering of a complete webpage whenever the page includes content or data that is not stored on the webpage's own server or servers. Like primary GET requests, secondary GET requests ordinarily include referer headers. And the referer header for a secondary GET request is typically the URL of the webpage being loaded.

For instance, suppose a person wants to access research about dentistry practices during the pandemic that the University of Michigan hosts on its website.[5] In order to load all of the content on this single webpage, the person's browser transmits over 80 GET requests to over ten different servers. One of those is a secondary GET request to a server controlled by YouTube that calls for a video discussing the research, which seamlessly appears as part of the webpage. That secondary GET request contains the following information:[6]

[5] https://news.umich.edu/dentistry-during-covid-19-engineering-analysis-offers-guidelines-to-reduce-exposure/

[6] This image is reproduced in a larger format at App. 2a. The appendix contains side-by-side images of the "request headers" of both the secondary GET requests that the user's browser transmits in example scenarios discussed in this brief and the primary GET requests (from the user's browser to the host website) that led to the later transmission of that secondary GET request.



```
Request URL: https://www.youtube.com/embed/fcJEc40cD8o?feature=oembed&rel=0
Request Method: GET
Status Code: 🟩 200 / OK
Request Headers
Accept: text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US
Connection: Keep-Alive
Cookie: YSC=yBWvVYXw_Vo; VISITOR_INFO1_LIVE=zwpnajhjRZA; GPS=1
Host: www.youtube.com
Referer: https://news.umich.edu/dentistry-during-covid-19-engineering-analysis-offers-guidelines-to-reduce-exposure/
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.171..
```

The first item in this secondary GET request is the address (URL) of the particular element of content sought (here, the video) ("https://www.youtube.com/embed/fcJEc40cD8o?feature=oembed&rel=0"). In addition to other information, this request also conveyed to the YouTube server the referer header, identifying "https://news.umich.edu/dentistry-during-covid-19-engineering-analysis-offers-guidelines-to-reduce-exposure/" as the webpage that instructed the person's browser to generate this secondary GET request.[7]

In the present action, plaintiffs allege that, while logged out of Facebook, they visited non-Facebook

[7] This sort of detailed information about each GET request that emanated from a person's browser in the course of rendering a webpage can be viewed using the inspector tools incorporated into any modern web browser. A person using the Microsoft Edge browser, for instance, may access this information during a visit to any webpage either by right-clicking and selecting "Inspect" or by simultaneously pressing Control, Shift, and I. *See* Open Microsoft Edge DevTools, https://docs.microsoft.com/en-us/microsoft-edge/devtools-guide-chromium/open/?tabs=cmd-Windows. Those actions open a panel with several tabs. The "Network" tab shows information regarding each request the browser made in rendering the webpage, including the type of request, the information sent, and where it was sent. *See* Inspect Network Activity In Microsoft Edge DevTools, https://docs.microsoft.com/en-us/microsoft-edge/devtools-guide-chromium/network/.

webpages that displayed a Facebook "like" button. Plaintiffs further allege that, as those webpages were being rendered on their computers, their browsers sent Facebook secondary GET requests that included, in the referer header, the URL of the webpage being visited.

The Ninth Circuit held that Facebook could be liable under the Wiretap Act because it "engag[ed] in the unauthorized duplication and forwarding of unknowing users' information." Pet.App. 33a. Facebook now seeks a writ of certiorari. For the reasons explained below, Facebook's petition should be granted.

ARGUMENT

I. THE NINTH CIRCUIT'S DECISION WOULD EXPOSE COMPANIES TO LIABILITY FOR A VAST NUMBER OF ORDINARY ONLINE COMMUNICATIONS

If left in place, the Ninth Circuit's decision would present a serious threat to the functioning of the internet. The decision threatens to make it both a federal felony and a basis for massive civil liability for companies to participate in everyday computer-to-computer communications that underlie much of the modern web. Secondary GET requests make millions of everyday internet communications more secure, more effective, and more streamlined. Yet the Ninth Circuit's application of the Wiretap Act threatens to make receipt of those requests a criminal act. Given the importance of this issue and the entrenched division among the courts of appeals, this Court should grant Facebook's petition for certiorari and reverse the Ninth Circuit's erroneous decision.

A. The Ninth Circuit's Decision Threatens Millions Of Everyday Internet Communications

The realm of communications implicated by the Ninth Circuit's decision is immense. The court's decision turns on facts that are extremely common on the web—something the Ninth Circuit appeared not to understand. If left in place, the decision would cast a shadow of potential massive civil and criminal liability over the web.

1. The Wiretap Act—last amended in 1986, *Bartnicki* v. *Vopper*, 532 U.S. 514, 524 (2001)—generally prohibits the "intentional[] intercept[ion] … [of] any … electronic communication," 18 U.S.C. § 2511(1)(a), "through the use of any … device," *id.* § 2510(4). "[T]he basic purpose of the statute … is to 'protec[t] the privacy of wire[, electronic,] and oral communications.'" *Bartnicki*, 532 U.S. at 526 (second and third alterations in original). The Act also includes a number of exceptions, including an exception for parties to the communication at issue: "It shall not be unlawful under this chapter for a person … to intercept a[n] … electronic communication where such person is a party to the communication." 18 U.S.C. § 2511(2)(d).

In this case, plaintiffs alleged that Facebook intercepted primary GET requests sent to webpages they had visited. 7ER1235-1237.[8] According to plaintiffs, these interceptions occurred when their browsers sent secondary GET requests to Facebook's servers with a referer header that included the address of the webpage being accessed. 7ER1209. Facebook countered that it was "a party" to the only "communication"

[8] "ER" refers to the Appellant's Excerpts of Record in the Ninth Circuit.

that it had in any sense accessed—namely, the secondary GET request, which called for the rendering of the Facebook "like" button on the plaintiff's screen—and so could not be liable under the statute. 18 U.S.C. § 2511(2)(d). Rejecting Facebook's argument, the Ninth Circuit held that the party exception was inapplicable here. Pet.App. 30a-33a.

The Ninth Circuit's ruling arose in the context of allegations that Facebook had used the information from the secondary GET requests to tailor advertisements and recommendations. But the Ninth Circuit's interpretation of the Wiretap Act does not depend on that context, and to face potential liability under the Ninth Circuit decision, a company need not use data received through secondary GET requests to tailor its services. Rather, the Ninth Circuit focused on three aspects of these computer-to-computer communications: *First*, the court noted that the secondary GET request was sent "to Facebook's server," rather than the server hosting the webpage being visited. Pet.App. 31a. *Second*, the court explained that the secondary "GET request also transmits a referer header." *Id.* And *third*, the court emphasized that the "duplication and forwarding" of the referer header was "unauthorized" because plaintiffs were "unknowing" of Facebook's receipt of this information. Pet.App. 33a.

Communications with these three features are entirely commonplace, and in fact used by nearly every website on the web. As a result, the Ninth Circuit's decision threatens to impose wide-ranging liability.

a. First, secondary GET requests are the norm on today's web. A recent study analyzed the home pages of the most popular 990,022 websites and found that 832,349—88%—instructed browsers to send secondary

GET requests. *See* Libert, *Exposing the Hidden Web: An Analysis of Third-Party HTTP Requests on One Million Websites*, Int'l J. of Commc'n, at 5 (Oct. 2015);[9] *see also* Schelter & Kunegis, *Tracking the Trackers: A Large-Scale Analysis of Embedded Web Trackers* 679, Tenth International AAAI Conference on Web and Social Media (Mar. 2016) ("The majority of websites contain third-party content, i.e., content from another domain that a visitor's browser loads and renders upon displaying the website.").[10] These webpages cause a visitor's browser to contact, on average, 9.47 distinct servers. Libert, *supra*, at 5.

The Ninth Circuit failed to appreciate the ubiquity of these secondary GET requests, opining that "[t]ypically, [a GET request] occurs only between the user's web browser and the [] website." Pet.App. 31a. The opposite is true: The web relies on secondary GET requests to display a whole universe of content. For instance, suppose a person, seeking information about COVID-19, were to navigate to the Center for Disease Control's (CDC) website and land on the webpage whose URL is in the margin below.[11] The person's browser would load not only content that resides on the CDC's own server, but also a video regarding the viral test for COVID, which loads via a secondary GET request to a different entity's server. Without the secondary GET request, the visitor would have to access the video on a separate webpage, rather than seeing

[9] https://arxiv.org/abs/1511.00619

[10] https://www.aaai.org/ocs/index.php/ICWSM/ICWSM16/paper/view/13024

[11] https://www.cdc.gov/coronavirus/2019-ncov/testing/diagnostic-testing.html

the video integrated with the other content on the webpage.

Secondary GET requests perform many important functions. Secondary GET requests, for example, free website publishers from having to create every part of their webpage and instead allow them to enlist specialists to provide content or to carry out certain tasks. For instance, webpages that need to accept payment can arrange for a payment platform to perform that function (which can be both complicated and expensive to build) without the visitor having to leave the page. *See* Payment Gateway, Wikipedia.[12] The service that provides the payment platform writes the necessary code, ensures compliance with all necessary regulations, and manages all aspects of the payment process. *See id.* This, in turn, allows the website publisher to focus on producing his own content instead of being forced to create his own payment processing modules.

Similarly, many websites make use of a "CAPTCHA"—a Completely Automated Public Turing test to tell Computers and Humans Apart—to ward off bots that could otherwise wreak havoc on their websites. *See CAPTCHA: Telling Humans and Computers Apart Automatically* (describing several kinds of web attacks waged by bots).[13] The internet is densely populated with CAPTCHA tests. For instance, this Court's e-filing registration page uses a CAPTCHA, which loads via a secondary GET request. *See* Supreme

[12] https://en.wikipedia.org/wiki/Payment_gateway (last visited December 28, 2020).

[13] www.captcha.net

Court of the United States, Electronic Filing System;[14] *see also* App. 3a-4a. Without such secondary GET requests, this Court and other website publishers would be forced to build a CAPTCHA from scratch—something most website publishers are not equipped to do. *See* Moradi et al., *CAPTCHA And Its Alternatives*, 8 Security and Communication Networks, 2143 (2014) (discussing "several unavoidable issues related to" websites creating custom CAPTCHA, including "defects in development and implementation," "costs," "bandwidth issues," and "copyright considerations").[15]

b. Second, GET requests (including secondary GET requests) also typically include a referer header. *See* Mayer & Mitchell, *Third-Party Web Tracking: Policy and Technology*, in *2012 IEEE Symposium on Security and Privacy* 415 (2012) ("When a first-party page embeds third-party content, the third-party website is ordinarily made aware of the URL of the first-party page through an HTTP referer or equivalent.").[16] In the University of Michigan webpage discussed above, the secondary GET request includes a referer header that contains the URL of the webpage being rendered. *See supra* at 7-8; App. 2a. Likewise, in the example from this Court's own webpage mentioned above, the secondary GET request includes a referer header that repeats the URL of this Court's e-filing registration page. App. 4a. By the same token, should a person search for a dermatologist in Washington D.C.

[14] https://file.supremecourt.gov/Account/Register (the CAPTCHA, which appears after one checks either of the two boxes, loads from remote.captcha.com).

[15] https://onlinelibrary.wiley.com/doi/full/10.1002/sec.1157

[16] https://ieeexplore.ieee.org/document/6234427

on healthgrades.com, her browser will send a secondary GET request that includes the referer header set forth in the margin below.[17] This referer header contains the full URL of the webpage being visited, which includes the location and type of healthcare provider that the visitor is seeking.

Referer headers contained in secondary GET requests serve many functions, but one prominent example is "simple analytics." Fielding, *supra*, at § 5.5.2. The recipient of a secondary GET request has an interest in knowing which website prompted a visitor to send the request, as well as the context from which the request originated. For instance, the operator of the server that received the secondary GET request may wish to control where her copyrighted content is being shared. *See Perfect 10*, 508 F.3d at 1159 (considering copyright implications of displaying images in search results via secondary GET requests). Additionally, because secondary GET requests draw data directly from the secondary server, they require bandwidth from that server—bandwidth that the server's owner may not wish to share in some cases. The owner can "use the Referer header field" to filter out GET requests she would prefer not to honor. Fielding, *supra*, at § 5.5.2.

c. Third, secondary GET requests are nearly always unnoticed by the person visiting the main webpage and therefore "unauthorized," as the Ninth Circuit used that term. The dynamic websites that make up today's web are highly complex, often instructing a person's browser to transmit dozens or

[17] https://www.healthgrades.com/usearch?what=Dermatology&where=Washington%2C%20DC%2020008&pt=38.935771%2C-77.059213&pageNum=1&sort.provider=bestmatch&state=DC&zip=20008

sometimes hundreds of secondary GET requests. For instance, when loading the CDC webpage discussed above (at 12), the visitor's browser sends out over 70 GET requests, 29 of which are secondary requests directed to servers at eleven distinct domains. Despite this complexity, the visitor's browser discreetly stitches together a single webpage, improving the browsing experience. *See Perfect 10*, 508 F.3d at 1156 ("[T]he user's window appears to be filled with a single integrated presentation … but it is actually an image from a third-party website framed by information from Google's website."). Most people viewing the CDC's webpage are uninterested in the extent of the computer-to-computer communications that went into loading it. And any process that would call each of these separate background events to the attention of the visitor would likely be cumbersome, time-consuming, and annoying to the visitor.[18]

Moreover, secondary GET requests do not always relate to visible content on the webpage. For instance, whenever a visitor accesses the Women of the Senate webpage on the United States Senate's website,[19] the webpage instructs the visitor's browser to issue a secondary GET request to the server of a web analytics service—a fact that is not obvious from the face of the website. *See* App. 5a-6a.

Web analytics services help website operators optimize their visitors' experiences, identify problems,

[18] As noted, however, a complete log of the primary and secondary GET requests that emanate from a person's computer during the rendering of any webpage can easily be accessed by that person if she wishes to see them. *See supra* at n.8.

[19] https://www.senate.gov/artandhistory/history/People/Women/Women-of-the-Senate.htm

improve website performance, and otherwise understand traffic to their website. *See* Zheng & Peltsverger, *Web Analytics Overview*, in *Encyclopedia of Information Science and Technology*, (Khosrow-Pour ed., 3d ed., 2015).[20] Secondary GET requests containing referer headers are important to the operation of these services, as they are one of the means by which the services understand which particular webpages are visited, the context in which those visits occur, and the manner in which those webpages are used. Web analytics services are so commonly used across the web that they are employed on the websites of the White House, the United States Department of Justice, the United States Senate, and at least nine of the United States Courts of Appeals. Indeed, the use of web analytic services is so firmly established—and the value so widely recognized—that websites operated by agencies in the executive branch of the United States government are "required" to implement them "on all public facing federal websites." GSA Technology Transformation Services, *Guide To The Digital Analytics Program*;[21] *see also* Office of Management and Budget, Memorandum for the Heads of Executive Departments and Agencies 4 (Nov. 8, 2016) ("All agencies must … deploy the [Digital Analytics Program (DAP)] tracking code on all public facing agency websites. The DAP provides agencies with free quantitative analytics to inform website management.").[22]

[20] https://www.researchgate.net/publication/272815693_Web_Analytics_Overview

[21] https://digital.gov/guides/dap/

[22] https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-06.pdf

2. Besides the three features set forth above, the Ninth Circuit's analysis of plaintiffs' Wiretap Act claim also states, in purportedly describing the "technical context" of the claim, that the secondary GET request that plaintiffs' browsers sent to Facebook "transmitted … personally identifiable URL information." Pet.App. 31a. By this, the Ninth Circuit evidently meant that the secondary GET request included Facebook cookies that enabled Facebook to associate the contents of the secondary GET request, including the URL in the referer header, with a particular Facebook user.[23]

The Ninth Circuit's decision does not expressly state that the secondary GET request's alleged inclusion of personally identifiable information was necessary to state a violation of the Wiretap Act against Facebook. Nor would it have made sense for the Ninth Circuit to have stated that. After all, the relevant question, for purposes of the Wiretap Act, is whether a communication was intercepted by a non-party to the communication. And the only "personally identifiable" information that the Ninth Circuit discussed were cookies, Pet.App. 7a-8a, 21a, which were transmitted only to Facebook and were not part of the primary GET request that Facebook allegedly intercepted. 7ER1206-1207, 1209. It is thus far from certain that the precedential impact of the decision, if not reversed, would be

[23] Cookies are small text files stored by web servers on a person's web browser, which are transmitted back to the server as a separate field in some GET requests. 7ER1206, 1209; Cahn et al., *An Empirical Study of Web Cookies*, International World Wide Web Conference Committee 891 (Apr. 2016), https://dl.acm.org/doi/abs/10.1145/2872427.2882991. Cookies enable a server to recognize a browser it has seen before, allowing for functions like persistent shopping carts. *Id.*

limited to secondary GET requests that contain "personally identifiable" information.[24]

In any event, even if the decision is understood to include that limit, it would not necessarily protect secondary GET requests from the risk of Wiretap Act liability. That is because every secondary GET request includes information that arguably qualifies as "personally identifiable"—namely, the IP address associated with the browser making the request. *See supra* at 5-6. Secondary GET requests uniformly include this information so that the server receiving the request knows where to send the requested content or other data. Those IP addresses, when combined with other information typically included in GET requests, can often be used to "fingerprint" the person associated with any particular secondary GET request. *See* Yen et al., *Host Fingerprinting and Tracking on the Web: Privacy and Security Implications*, in *Proceedings of the 19th Annual Network and Distributed System Security Symposium* 2, 4-5 (Feb. 8 2012);[25] *see also* Fielding, *supra*, at § 9.7.

* * *

[24] To the extent the Ninth Circuit viewed transmission of personally identifiable information not to be required to state a violation of the Wiretap Act but rather to be required to establish standing under Article III, that would at most limit any exposure to civil liability in a Wiretap Act lawsuit. But it would do nothing to limit companies' potential exposure to *criminal* liability under the Wiretap Act. *See United States* v. *Daniels*, 48 F. App'x 409, 418 (3d Cir. 2002) ("As sovereign, the United States has standing to prosecute violations of valid criminal statutes.").

[25] https://www.ndss-symposium.org/ndss2012/ndss-2012-programme/host-fingerprinting-and-tracking-web-privacy-and-security-implications/

In short, secondary GET requests improve users' browsing experiences in countless ways and in fact undergird the functions that characterize the modern web. These requests frequently include referer headers. The Ninth Circuit's decision threatens to subject this vast universe of communications to significant civil and criminal liability.

B. The Liability At Stake Is Substantial

The potential exposure unleashed by the Ninth Circuit's decision is substantial. A violation of the Wiretap Act would subject companies and potentially their executives to criminal liability. 18 U.S.C. § 2511(4)(a). And because the statute arms plaintiffs with a private right of action, *id.* § 2520, and empowers them to seek payment of attorney's fees, punitive damages, and penalties of $100 per day per person, *id.* § 2520(b)(2)-(3), (c)(2), the plaintiffs' bar would be highly motivated to try to challenge many of the countless, everyday computer-to-computer communications on which the internet relies. Moreover, because many (if not most) internet companies are based within the Ninth Circuit's jurisdiction, the decision (absent reversal) would govern their conduct, even though it is out-of-step with many other courts of appeals. *See infra* at 22-23.

* * *

The Ninth Circuit's decision thus threatens to impose significant liability for everyday internet communications. By outlawing all "unauthorized" secondary GET requests, the court cast doubt on the legality of an extraordinarily common practice. This Court's intervention is thus sorely needed.

II. FACEBOOK'S CONDUCT DID NOT VIOLATE THE WIRETAP ACT

Properly understood, the Wiretap Act does not prohibit secondary GET requests, because, as Facebook argued below and argues in its petition, the recipient of any such request is necessarily a party to that communication. The Ninth Circuit held the opposite, ruling that Facebook could be held liable under the Wiretap Act. That conclusion was wrong.

a. As explained above, *see supra* at 10, although the Wiretap Act generally prohibits the "intentional[] intercept[ion] … [of] any … electronic communication," it exempts from liability any "party to the communication." 18 U.S.C. § 2511(1)(a), (2)(d). Because secondary GET requests are sent directly from the person's browser to the secondary server in order to enable some function of the webpage, they fall within this party exception. In the case of the Facebook "like" button, the communication is simple: The person is the sender, and the designated recipient is Facebook. Because the designated "recipient of a communication is necessarily one of its parties," Facebook was a "part[y] to the transmissions at issue in this case." *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 143 (3d Cir. 2015).

Indeed, Facebook is necessarily a party to the secondary GET request. As the Third Circuit has explained, "[t]autologically, a communication will always consist of at least two parties: the speaker and/or sender, and at least one intended recipient." *In re Google*, 806 F.3d at 143. This tautology is reflected in the definitions of "communication" and "party." The statute defines "electronic communication" as "any *transfer* of signs, signals, writing, images, sounds, data, or intelligence of any nature." 18 U.S.C. § 2510(12). To transfer means to "convey … from … one person to another." *Black's Law Dictionary* 1803 (11th ed. 2019). In other words, a communication must have a recipient. The definition of party, too, assumes the presence of a second person: Black's defines "party" as "someone concerned in or privy to a matter; esp[ecially] someone involved in either of two sides in an affair." *Black's Law Dictionary* 1351 (11th ed. 2019); *cf. Webster's Third New International Dictionary* 1648 (1986) (defining "party" as "constituting alone or with others one of the two sides in a proceeding").

And the secondary GET request is the only communication that Facebook ever accessed. As explained above, the primary GET request is sent only to the server that hosts the webpage being loaded. Facebook had no access to that communication and was privy instead only to the secondary GET request.

For this reason, the Third Circuit has ruled that an internet company does not violate the Wiretap Act by receiving secondary GET requests sent directly to it for the purpose of serving advertisements to websites. *In re Google*, 806 F.3d at 142-143.

This straightforward logic has been recognized not only by the Third Circuit, but also by the Second, Fifth, and Sixth Circuits. Both the Fifth and Sixth Circuits have considered the situation where a police officer, validly present in a suspect's home, answered the suspect's phone without identifying himself. *United States* v. *Campagnuolo*, 592 F.2d 852, 855 (5th Cir. 1979); *United States* v. *Passarella*, 788 F.2d 377, 378 (6th Cir. 1986). Both courts held that, because the officers were parties to the communication, their conduct did not violate the Wiretap Act. *Campagnuolo*, 592 F.2d at 863;

Passarella, 788 F.2d at 379. Similarly, the Second Circuit rejected the argument that a defendant was not a "party" to a conversation he was not "invite[d] … to join." *Caro* v. *Weintraub*, 618 F.3d 94, 97 (2d Cir. 2010). The court found it "sufficient" that the defendant "was present at the table" where the conversation happened. *Id.* at 97-98.

b. The Ninth Circuit concluded otherwise, but its opinion neglected the plain meaning of the term "party." Rather than accepting the ordinary meaning of that term, the court crafted a new rule prohibiting "unauthorized duplication and forwarding of users' information." Pet.App. 33a. The Ninth Circuit's rule is misguided for the reasons explained in Facebook's petition. *See* Pet. 21-27. In addition, it misunderstands the relationship between primary and secondary GET requests. Pet.App. 33a.

Contrary to the Ninth Circuit's opinion, a secondary GET request is not "cop[ied] … from the [primary] GET request." Pet.App. 31a. Nor are the two requests "identical." Pet.App. 33a; *compare, e.g.*, App. 1a *with* App. 2a. As plaintiffs' complaint recognizes, while there is typically some overlap in the information contained in primary and secondary GET requests, each request also contains distinct information. 7ER1209 (depicting primary and secondary GET requests); *see also* App. 1a-6a.

In particular, as described, *supra* at 6-7, the referer headers for primary and secondary GET requests are not identical. A referer header communicates which webpage referred the browser to the content the GET request seeks. Fielding, *supra*, at § 5.5.2. For a primary GET request, this is often the webpage that the browser was displaying at the moment the request was transmitted. Thus for instance, if a person accesses the Women in the Senate webpage by clicking on a link appearing on the Senate's home page, the referer header in the primary GET request generated by that click will be the Senate's homepage. *See* App. 5a. By contrast, the referer header in a secondary GET request is typically the webpage being loaded. Thus, the referer header in secondary GET requests sent while the browser is loading the Women in the Senate webpage will be the *current* webpage (i.e., the Women in the Senate webpage), because that is the webpage that instructed the browser to send the secondary GET request. *See* App. 6a. The referer header is thus in no sense "copied" from the preceding GET request. *Contra* Pet.App. 31a.

For these reasons, and as explained in the Petition, the Ninth Circuit's analysis was flawed. Under a proper reading of the statute, Facebook was a "party to the communication" at issue and is thus exempt from Wiretap Act liability.

* * *

In light of the Ninth Circuit's incorrect interpretation of the Wiretap Act, its potential to outlaw practices common in the internet industry, and the entrenched split among the courts of appeals, this Court's intervention is badly needed. This Court should grant certiorari and reverse the Ninth Circuit's incorrect reading of the statute.

CONCLUSION

The petition for certiorari should be granted.

Respectfully submitted.

ELIZABETH BANKER
INTERNET ASSOCIATION
660 North Capitol St., NW
Suite 200
Washington, DC 20001
(202) 869-8632
elizabeth@
internetassociation.org

DARYL JOSEFFER
TARA S. MORRISSEY
U.S. CHAMBER LITIGATION
CENTER
1615 H St., NW
Washington, DC 20062
(202) 463-5668
tmorrissey@uschamber.com

CHRISTOPHER MOHR
SOFTWARE AND INFORMATION
INDUSTRY ASSOCIATION
1090 Vermont Ave., NW
Washington, DC 20005
(202) 289-7442
cmohr@siia.net

PATRICK J. CAROME
Counsel of Record
ARI HOLTZBLATT
AMY LISHINSKI
WILMER CUTLER PICKERING
HALE AND DORR LLP
1875 Pennsylvania Ave., NW
Washington, DC 20006
(202) 663-6000
patrick.carome@wilmerhale.com

MATTHEW SCHRUERS
COMPUTER AND
COMMUNICATIONS
INDUSTRY ASSOCIATION
25 Massachusetts Ave., NW
Suite 300C
Washington, DC 20001
(202) 470-3620
mschruers@ccianet.org

DECEMBER 2020

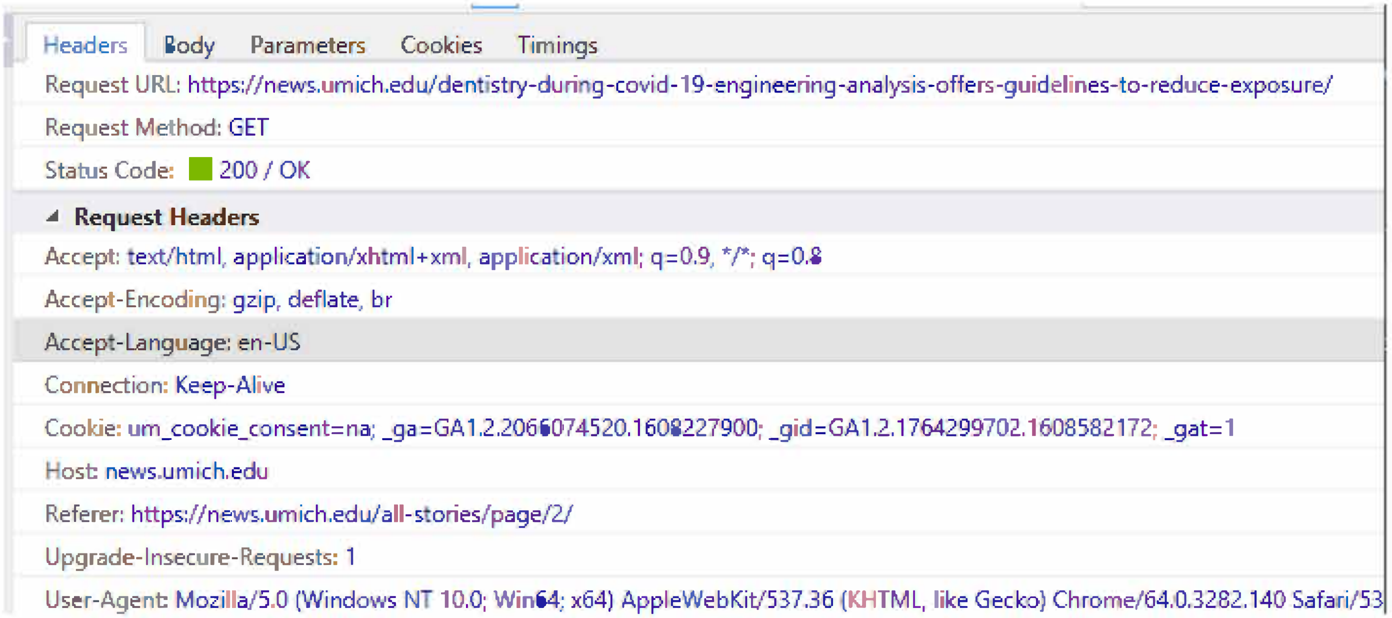
APPENDIX:

EXEMPLAR GET
REQUESTS ILLUSTRATING
SCENARIOS DISCUSSED IN BRIEF

1a

University of Michigan Website Scenario

Primary GET request for webpage concerning dentistry during COVID-19



Request URL: https://news.umich.edu/dentistry-during-covid-19-engineering-analysis-offers-guidelines-to-reduce-exposure/

Request Method: GET

Status Code: 🟩 200 / OK

Request Headers

Accept: text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US

Connection: Keep-Alive

Cookie: um_cookie_consent=na; _ga=GA1.2.2066074520.1608227900; _gid=GA1.2.1764299702.1608582172; _gat=1

Host: news.umich.edu

Referer: https://news.umich.edu/all-stories/page/2/

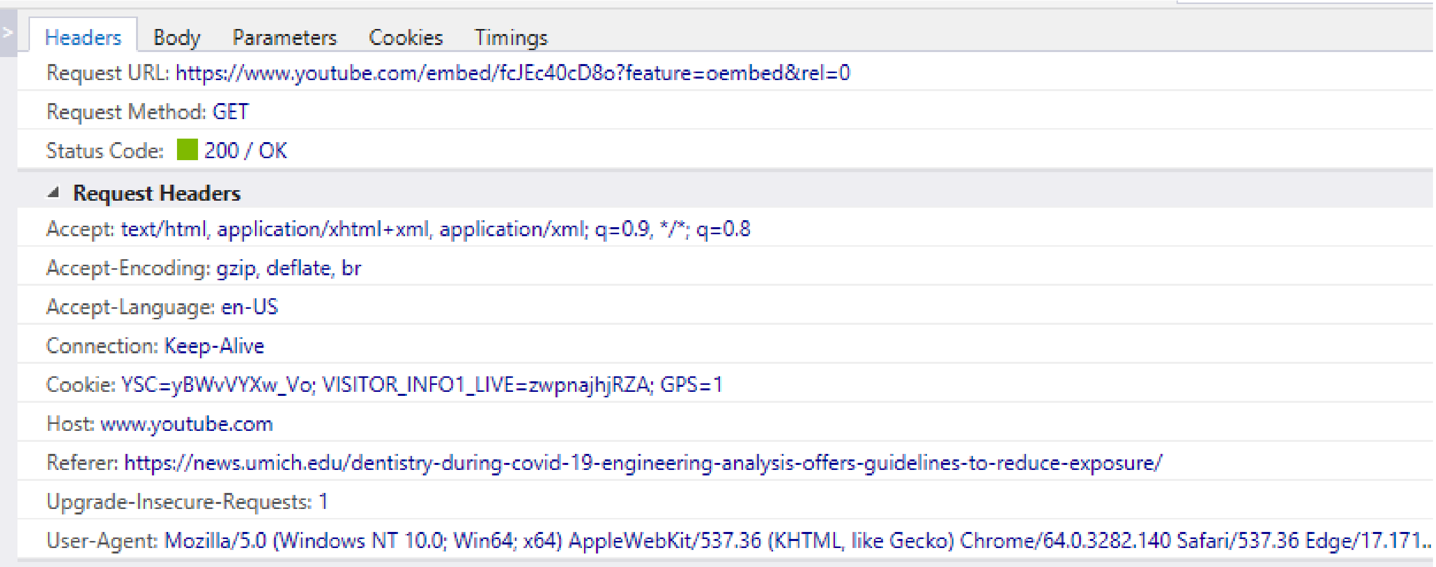
Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/53

2a

University of Michigan Website Scenario

Secondary GET request transmitted to load video from YouTube server



Request URL: https://www.youtube.com/embed/fcJEc40cD8o?feature=oembed&rel=0

Request Method: GET

Status Code: 🟩 200 / OK

Request Headers

Accept: text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US

Connection: Keep-Alive

Cookie: YSC=yBWvVYXw_Vo; VISITOR_INFO1_LIVE=zwpnajhjRZA; GPS=1

Host: www.youtube.com

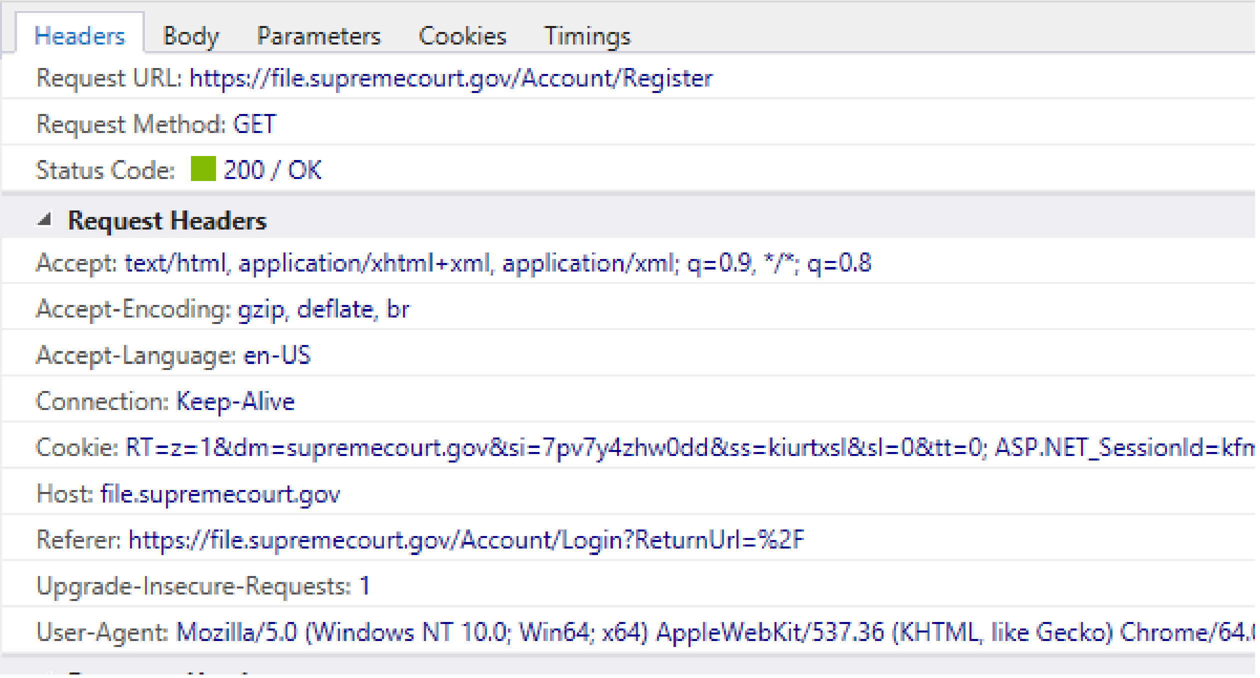
⇨ Referer: https://news.umich.edu/dentistry-during-covid-19-engineering-analysis-offers-guidelines-to-reduce-exposure/

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36 Edge/17.171..

United States Supreme Court Website Scenario

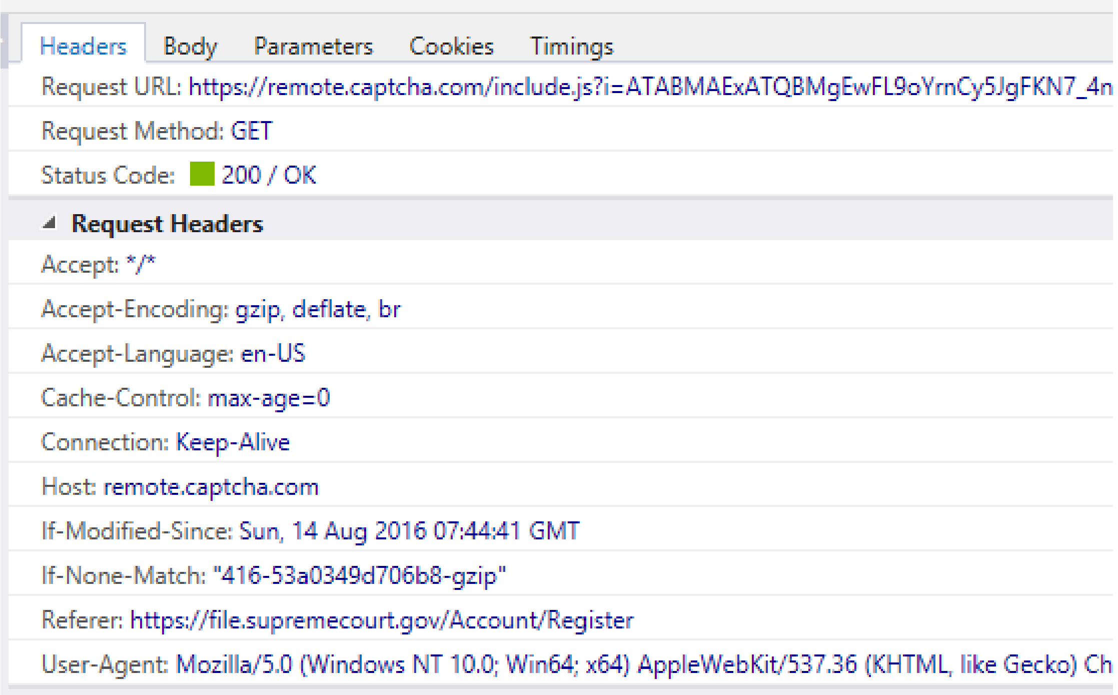
Primary GET request for e-filing registration webpage



```
Request URL: https://file.supremecourt.gov/Account/Register
Request Method: GET
Status Code: 🟩 200 / OK
◢ Request Headers
Accept: text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US
Connection: Keep-Alive
Cookie: RT=z=1&dm=supremecourt.gov&si=7pv7y4zhw0dd&ss=kiurtxsl&sl=0&tt=0; ASP.NET_SessionId=kfn
Host: file.supremecourt.gov
Referer: https://file.supremecourt.gov/Account/Login?ReturnUrl=%2F
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.
```

United States Supreme Court Website Scenario

<u>Secondary</u> GET request transmitted to load CAPTCHA from captcha.com server



Headers Body Parameters Cookies Timings

Request URL: https://remote.captcha.com/include.js?i=ATABMAExATQBMgEwFL9oYrnCy5JgFKN7_4n

Request Method: GET

Status Code: 🟩 200 / OK

◢ **Request Headers**

Accept: */*

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US

Cache-Control: max-age=0

Connection: Keep-Alive

Host: remote.captcha.com

If-Modified-Since: Sun, 14 Aug 2016 07:44:41 GMT

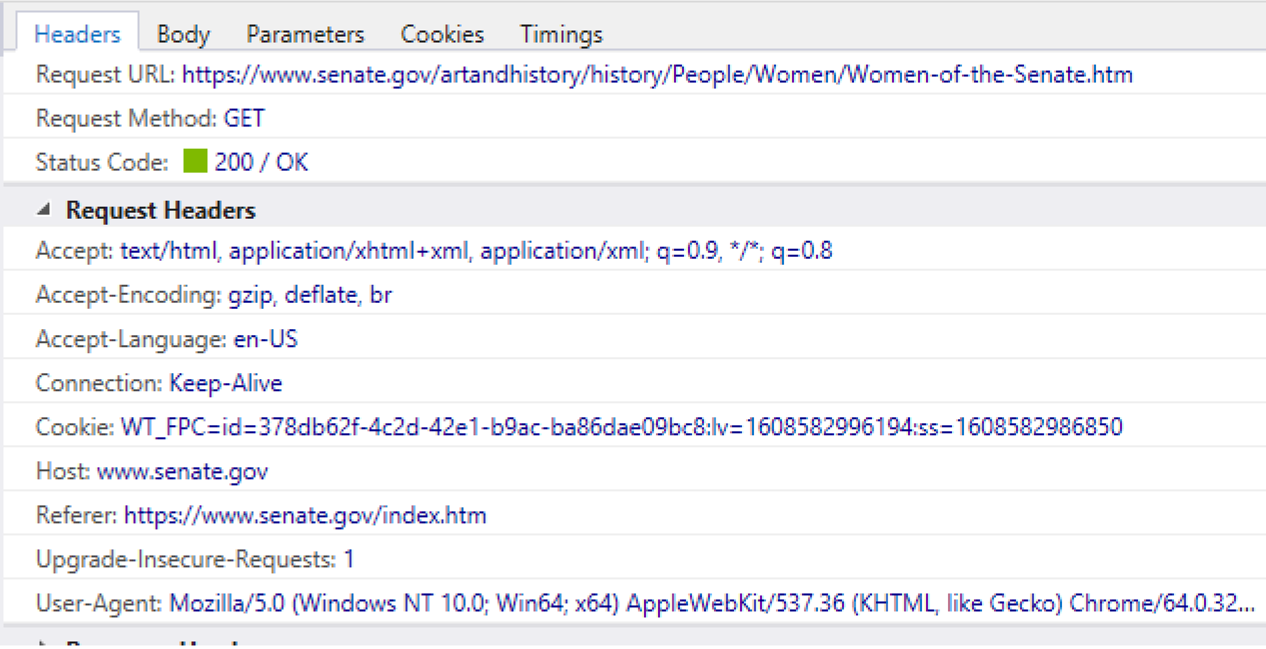
If-None-Match: "416-53a0349d706b8-gzip"

⇨ Referer: https://file.supremecourt.gov/Account/Register

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Ch

United States Senate Website Scenario

Primary GET request for Women of the Senate webpage



Request URL: https://www.senate.gov/artandhistory/history/People/Women/Women-of-the-Senate.htm

Request Method: GET

Status Code: 🟩 200 / OK

Request Headers

Accept: text/html, application/xhtml+xml, application/xml; q=0.9, */*; q=0.8

Accept-Encoding: gzip, deflate, br

Accept-Language: en-US

Connection: Keep-Alive

Cookie: WT_FPC=id=378db62f-4c2d-42e1-b9ac-ba86dae09bc8:lv=1608582996194:ss=1608582986850

Host: www.senate.gov

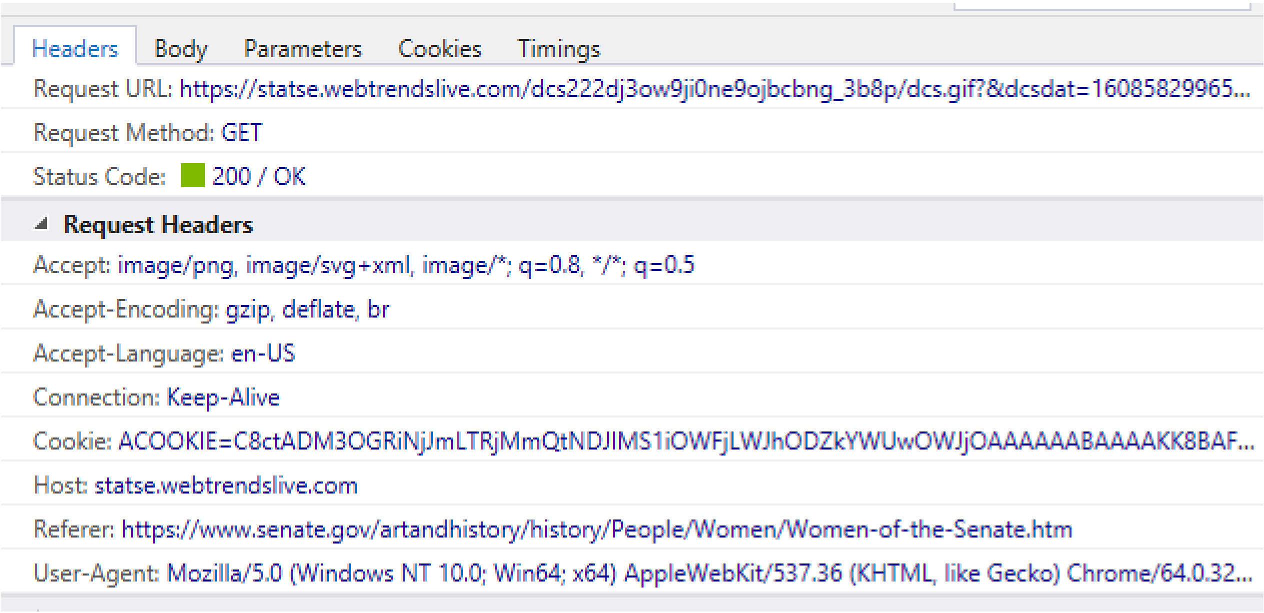
Referer: https://www.senate.gov/index.htm

Upgrade-Insecure-Requests: 1

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.32...

United States Senate Website Scenario

Secondary GET request transmitted to web analytics service provider



```
Request URL: https://statse.webtrendslive.com/dcs222dj3ow9ji0ne9ojbcbng_3b8p/dcs.gif?&dcsdat=16085829965...
Request Method: GET
Status Code: 🟩 200 / OK
◢ Request Headers
Accept: image/png, image/svg+xml, image/*; q=0.8, */*; q=0.5
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US
Connection: Keep-Alive
Cookie: ACOOKIE=C8ctADM3OGRiNjJmLTRjMmQtNDJlMS1iOWFjLWJhODZkYWUwOWJjOAAAAAABAAAAKK8BAF...
Host: statse.webtrendslive.com
⇨ Referer: https://www.senate.gov/artandhistory/history/People/Women/Women-of-the-Senate.htm
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.32...
```