No. 22-15293

In the United States Court of Appeals for the Ninth Circuit

ALEXIS HUNLEY *and* MATTHEW SCOTT BRAUER,
Individually and on Behalf of All Others Similarly Situated,
PLAINTIFFS-APPELLANTS

v.

INSTAGRAM, LLC,
DEFENDANT-APPELLEE

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA (21-CV-3778) (THE HONORABLE CHARLES R. BREYER)

BRIEF OF AMICUS CURIAE INTERNET SOCIETY IN SUPPORT OF APPELLEE

AMY MASON SAHARIA
D. SHAYON GHOSH
WILLIAMS & CONNOLLY LLP
680 Maine Avenue, S.W.
Washington, DC 20024
(202) 434-5000
asaharia@wc.com

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, *amicus* Internet Society states that it does not have a parent corporation, and no publicly held corporation owns 10% or more of its stock.

/s/ Amy Mason Saharia
AMY MASON SAHARIA
WILLIAMS & CONNOLLY LLP
680 MAINE AVENUE, S.W.
WASHINGTON, DC 20024
(202) 434-5000
asaharia@wc.com

OCTOBER 11, 2022

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases:

Statutes and Rule:

Other Authorities:

Page

Other Authorities—continued:

Page

Other Authorities—continued:

STATEMENT OF INTEREST[1]

Founded in 1992, the Internet Society is a U.S. non-profit organization headquartered in Reston, Virginia and Geneva, Switzerland for the worldwide coordination of, and collaboration on, Internet issues, standards, and applications. As a global non-governmental organization, the Internet Society believes that the Internet should be for everyone. It supports and promotes the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society, with an overarching goal that the Internet be open, globally connected, secure, and trustworthy. The Internet Society supports communities that seek to connect to the Internet. It advances the development and application of Internet infrastructure, technologies, and open standards. The Internet Society also advocates for policies that protect the Internet and allow it to flourish for all. The Internet Society's staff is comprised of technical experts in internetworking, cybersecurity, and network operations, among other fields, as well as policy experts in a broad range of Internet-related areas.

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), amicus certifies that no person or entity, other than amicus curiae, its members, or its counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. The parties have consented to the filing of this brief.

The Internet Society developed the "Internet Impact Assessment Toolkit" as an analytical framework to evaluate how policy proposals, legal decisions, market or geo-political developments, and technology might impact the Internet. The framework's key concepts derive from two foundational Internet Society white papers. *The Internet Way of Networking: Defining the Critical Properties of the Internet* describes the foundation the Internet needs in order to exist and work for everyone (including, for example, an "Open Architecture of Interoperable and Reusable Building Blocks").[2] *Enablers of an Open, Globally Connected, Secure and Trustworthy Internet* describes what the Internet needs in addition to its foundation to get closer to an aspirational state of the Internet widely recognized by countries and institutions worldwide.[3] This analytical methodology, as well as the Internet Society's extensive knowledge of how communications are developed and flow across the Internet, inform the arguments the Internet Society sets out below.

The Internet Society has long recognized that the success of the Internet depends on the ability for participants—including individuals—anywhere

---

[2] Internet Society, *The Internet Way of Networking: Defining the Critical Properties of the Internet* (Sept. 2020), https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Defining-the-critical-properties-of-the-Internet.pdf ("*Internet Way of Networking*").

[3] Internet Society, *Enablers of an Open, Globally Connected, Secure and Trustworthy Internet* (Nov. 8, 2021), https://www.internetsociety.org/wp-content/uploads/2021/11/Enablers-of-OGST-EN.pdf ("*Enablers*").

in the world to create and share content on the Internet. And content creators depend heavily, and sometimes even unknowingly, on embedding content. The imposition of copyright liability on content creators who embed content, as Plaintiffs here urge, would critically undermine the openness of the Internet, impede generation of innovative Internet content and technology, and frustrate the Internet Society's mission. The Internet Society submits this brief to help the Court understand the vast and serious implications of its ruling in this case for many different aspects of the Internet.

INTRODUCTION AND SUMMARY OF ARGUMENT

The Internet is "a global technical infrastructure, a resource to enrich people's lives, and a force for good in society." Internet Society, *Our Mission*, https://www.internetsociety.org/mission/. Built on a series of shared protocols, the Internet enables people across the world to communicate with each other, no matter where they reside or what device they use to access it. The Internet's architecture allows people across the world to independently generate innovative Internet technologies and content. As users develop and release new Internet technologies and content, which may be thought of as modules, others can use those modules without necessarily understanding how they work. In doing so, users can leverage the innovation of others to generate even more innovative technology and content and/or to enhance the functioning of the content they create on the Internet.

The act of embedding content or code—by which a creator of Internet content provides instructions for others' web browsers to access content or code from third-party servers—exemplifies the Internet's generative and modular capacity. Embedding enables the creation of content that is more accessible to a greater number of users and that incorporates modular content and technology created by others. Embedding is ubiquitous across many different aspects of the Internet. As in this case, websites on the World Wide Web may embed content from third-party servers. For example, this Court's own website embeds video content stored on YouTube servers. Others may embed content from third-party service providers whom the website creator pays to keep information updated. Emails and Internet-based text message applications frequently embed content from third-party servers. And website creators may embed code created by others to incorporate enhanced functionality into their websites—for instance, translation functionality or CAPTCHA functionality intended to secure websites.

This Court's server test protects Internet users' ability to deploy modular technology to generate content. The server test appropriately allocates copyright liability to the entity that actually "display[s]" a copy of copyright-protected content from its server to users' devices. 17 U.S.C. § 106(5). The entity that hosts content on its server is the entity that controls who may access the content and under what conditions users may access it. That entity

may delete, modify, or replace the content at any time, without any involvement or even knowledge of third parties who embed the content on their websites. The embedding entities do not themselves display or transmit the embedded content and have no control over it. Imposing copyright liability on creators who embed content would force dramatic changes to the functioning of the Internet and would frustrate the Internet's generative capacity.

ARGUMENT

I. The Ability To Embed Content on the Internet Is Critical to Its Function

The ability to "embed" content or code—to instruct others to use the Internet to access content or code developed by third parties and residing on third-party servers—is critical to the Internet's design and function.

A. The Internet Is a Modular Network Spanning the World

"The Internet is an international network of interconnected computers." *Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 849 (1997). It allows people to communicate with each other from anywhere. The Internet is built on a series of protocols, which are rules that govern the exchange of data. These protocols permit devices across the world to communicate across the Internet, regardless of who is using the devices, who made the devices, and where the devices are. In this way, Internet protocols facilitate interoperability among devices and connect people around the world. *See Enablers*, *supra*, at 7-9.

Many different applications are built on the Internet. One such application is the World Wide Web—a system through which devices can access content, including text, images, sound, video, sensors, and applications, provided by anyone else in the world. *See Reno*, 521 U.S. at 852. Users access content on the Web through "user agents" that act on their behalves. The most familiar user agent is a "web browser," such as Google Chrome, Mozilla Firefox, or Apple's Safari, which runs on the user's device and retrieves and displays content from the Web for the user. The content is provided or "hosted" by devices called "web servers," and users navigate to content using "web addresses" (formally known as Uniform Resource Locators, or URLs) that uniquely identify the location of the content. *See id.*

Although lay users often call the World Wide Web the "Internet," the Internet is much broader than just the World Wide Web. Many other everyday systems depend on the Internet, including email, social media applications, file transfer applications, messaging applications like iMessage and WhatsApp, and video-chat applications like FaceTime, Skype, and Zoom.

The Internet and the World Wide Web have become ubiquitous largely because they are decentralized and open. They are decentralized in the sense that "[n]o single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web." *Reno*, 521 U.S. at 853 (citation omitted). And

they are open in the sense that anyone can participate in the Internet in any capacity. *See Enablers*, *supra*, at 6-7. Anyone with access to an Internet-connected device can create content, receive content, and/or communicate with others from anywhere. The Internet Society's mission, among other things, is to protect these and other critical properties of the Internet, and thus to support the communications of people around the world.

B. The Internet's Success Hinges on Its Generativity and Modularity

The Internet has facilitated the rapid democratization of information and technology throughout the world. The Internet's success is often attributed to its "generative" nature, meaning that the technology itself can support further innovation by a large and varied audience, which can act independently and without coordination. *See* Jonathan Zittrain, *The Generative Internet*, 119 Harv. L. Rev. 1974, 1980 (2006); *see also, e.g.*, David G. Post, *The Theory of Generativity*, 78 Fordham L. Rev. 2755, 2757 (2010). "[G]enerativity increases with the ability of users to generate new, valuable uses that are easy to distribute and are in turn sources of further innovation." Zittrain, *supra*, at 1982. The Internet is "exceptionally generative": its adaptability, ease of mastery, and accessibility allow "programmers independent of the Internet's architects and service providers [to] offer, and consumers [to] accept, new software or services." *Id.* at 1987-88.

The Internet's generative capacity is in turn rooted in the architectural principles underlying the Internet discussed above. *See* Post, *supra*, at 2759-60. These principles allow the Internet's participants to develop and deploy openly available protocols according to their needs, creating a framework for people to connect with each other in an unlimited number of ways for an unlimited set of purposes. *See* Zittrain, *supra*, at 1987-96.

The principle of "modularity"—where everyone can build on what others have already done—fuels the generative nature of the Internet. *See, e.g.*, *Internet Way of Networking*, *supra*, at 5-6; Christopher S. Yoo, *Modularity Theory and Internet Regulation*, 2016 U. Ill. L. Rev. 1, 3-4. The Internet is best understood not as a single system but as a collection of technological modules that can evolve independently over time but that work together. *See Internet Way of Networking*, *supra*, at 5-6. Once someone releases a module into the world, others can treat it as a functional black box, without needing to understand its inner workings. For instance, a user can design an application on the assumption that the underlying network facilitates data transmission, without needing to consider or understand the inner workings of specific network protocols. *See id.*; Zittrain, *supra*, at 1988. The developers of the modules that implement the underlying network protocols, meanwhile, can make improvements over time to help applications using those modules operate faster or more securely, without the involvement or even the knowledge of the

applications' creators. *See Internet Way of Networking*, *supra*, at 5-6; Yoo, *supra*, at 18-24.

The network's capacity to distribute data further strengthens this modular approach. Internet participants—from ordinary users to content creators to tech companies—can use the underlying network to incorporate modular functionality or content from other sources anywhere on the Internet. *See Enablers*, *supra*, at 7-9. This capability enables website creators to access a near-infinite range of content and services, including so-called "back-end" services that provide benefits like hosting capacity or security functionality and "front-end" services that the end user can see immediately upon navigating to a website.

C. Embedding Is One Ubiquitous Example of the Internet's Modularity

One example of the modularity of the Internet is embedding content—which this Court has previously called "in-line linking"[4]—on the World Wide Web and other Internet technologies such as email. Internet participants routinely incorporate content or code from other sources on the Internet. Even unsophisticated Internet users may incorporate content on a near daily basis.

[4] *Kelly v. Arriba Soft Corp.*, 336 F.3d 811, 816 (9th Cir. 2003).

1. Embedding Content

One common example, and the one at issue in this case, is embedding content such as photographs on the World Wide Web. Each webpage, at a high level, is a collection of text and software code, often written in what is called the Hypertext Markup Language (HTML), that provides instructions to a web browser about how to display the webpage. *See Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146, 1155-56 (9th Cir. 2010).

Embedding content in a webpage essentially means including code in the page that tells the user's web browser to retrieve content such as an image from a particular source. *Id.* For example, a webpage can include code that tells the browser to retrieve an image from the same web server where the page is hosted. The HTML code for retrieving such an image might look like the following:

```
<img src="Smiley_Face.JPG">
```

On encountering this code, the user's web browser would access and display an image with the file name "Smiley_Face.JPG" from the same web server where the webpage is hosted.

Alternatively, the page can tell the browser to retrieve an image from someone else's web server by identifying the location of the image on that other server. The HTML code to instruct a web browser to access an image from a third-party web server might look like the following:

```
<img src="https://upload.wikimedia.org/wikipedia/commons/8/87/Smiley_Face.JPG">
```

On encountering this code, in contrast to the example above, the user's web browser would access and display the image with the file name "Smiley_Face.JPG" from the web address indicated above, which directs the browser to the Wikimedia Foundation's web server.

Embedding content is distinct from linking content. A link (short for hyperlink) on a webpage allows a user to navigate to another webpage or web resource by clicking the link. By contrast, embedding content allows a user to interact with content or code hosted by a third party within the webpage they are visiting, even though the content or code is hosted on the third party's server. *See Perfect 10*, 508 F.3d at 1156; *Kelly*, 336 F.3d at 816. Embedding benefits (1) Internet users who access the embedded content, (2) the entities that embed content or code from third-party servers, and (3) the third parties providing the content or code from their servers. Embedding allows users to see content from other websites without having to leave the webpage they are currently viewing. Embedding enables the webpage owner to provide important context together with the content, while avoiding the cost of storing, maintaining, and delivering the content on/from its server and while ensuring more reliable service by reducing the amount of content to be delivered. And embedding allows the third party to ensure that modifications to its content embedded by others—for example, security updates to software—are automatically accessed by users interacting with the embedded content.

Content creation software such as WordPress makes embedding content easy for users without coding expertise. For example, if a creator is writing a blog post or a news article through content creation software, the creator can simply click a button and paste the web address of a social media post. The software handles the rest. Specifically, it inserts into the content the code to load the embedded content that is located at and served from the social media site. When a user then views the webpage with the creator's content, the user's web browser will retrieve the embedded content from the identified server and display it within the creator's content. *See, e.g.*, https://wordpress.org/support/article/embeds/.

Importantly, that embedded content does nothing more than tell a web browser to access content from an identified location on another server. The webpage creator has no control over what is at that server location. Only the host of the third-party server controls the server's content. The third party can replace that content with new content at any time. If the third party changes what is stored at a given location on its server, someone viewing a webpage that embeds the content at that location will see the new content, without any action by the webpage creator.

It is common for creators to embed content, such as images and videos, from other sites too. For example, online product reviews can embed product

photos from Amazon. *See, e.g.*, https://www.nytimes.com/wirecutter/reviews/best-air-fryer/. Significantly, news sites can embed photos from sources like Getty Images or tweets from Twitter.[5] The latter has become very common in recent years, as newsworthy individuals often create or contribute to news by posting on sites like Twitter. News sites reporting on those posts then embed the tweets within the article reporting on the statement. This allows the reader to see the newsworthy communication in its native format without leaving the news site and while consuming the rest of the article, and also allows the reader to navigate to the Twitter site by clicking the image if the reader wants to see more of the context around the original tweet. According to a 2016 analysis in the United Kingdom, approximately 23 percent of online news articles embedded content from social media. Catalina Albeanu, *Report: Nearly a Quarter of News Articles Include Social Media Embeds*, Journalism.co.uk (Oct. 19, 2016).[6]

[5] *See, e.g.*, Yasmeen Abutaleb, *The Biden White House gets feisty on Twitter*, Wash. Post (Aug. 26, 2022), https://www.washingtonpost.com/politics/2022/08/26/white-house-twitter-megan-coyne/; Erik Ortiz & Lucy Bayly, *Elon Musk is 'considering' taking Tesla private*, CNBC (Aug. 7, 2018), https://www.nbcnews.com/tech/tech-news/elon-musk-tweets-he-s-considering-taking-tesla-private-n898366.

[6] https://www.journalism.co.uk/news/report-almost-one-in-four-news-articles-include-social-media-embeds/s2/a684313/.

Other examples abound. The Executive Branch embraces embedding, for example. The U.S. State Department's Bureau of Global Public Affairs maintains a website with public diplomacy content that it encourages Internet participants to embed on their websites. https://commons.america.gov/about. The website even provides instructions on how to embed its content. https://commons.america.gov/documentation/embed. For example, journalists writing articles about the war in Ukraine can use the website to locate and embed videos of President Biden's and Secretary Blinken's public statements about the war.

Companies may embed content from third-party service providers. For example, the Internet Society uses a third-party human resources company's services to advertise job openings and recruit candidates. The Internet Society embeds content from that third party in the "Open Positions" section of its "Careers" webpage. *See* https://www.internetsociety.org/careers/. By embedding content directly from its third-party service provider, the Internet Society can provide up-to-date information on its own website by causing any changes to its "Open Positions" on the third-party service provider's platform to appear on the Internet Society website without any action by Internet Society staff to edit the webpage.

Social bookmarking sites such as Pinterest also depend on embedding content. A Pinterest user's "board" is a collection of embedded content stored

on third-party servers. Creators also can embed interactive content such as maps (*e.g.*, Google Maps, Waze, or OpenStreetMap) on their webpages; for example, a company's website could embed a real-time traffic map to show potential customers where the company's branches or stores are located and how long it would take to get to each one. *See, e.g.*, https://www.sfgate.com/traffic/. Viewers can interact with the map at the same time as they interact with the creator's website, rather than having to visit a separate website for map/traffic information. Creators also can embed sound from sound hosting sites (*e.g.*, Spotify, SoundCloud, or Anchor.fm). An online music review, for instance, might embed a song from Spotify to allow readers with Spotify accounts to listen to a single from an album while they read about it. *See* https://newsroom.spotify.com/2018-09-04/how-to-embed-spotifys-play-button/. Online resources devoted to the Supreme Court, such as the Oyez website, can embed audio of recent Supreme Court arguments from C-SPAN. And a vast array of websites embed video content, including associated closed captioning, from third-party services (*e.g.*, YouTube, Vimeo).

In all of these cases, viewers access the content by visiting a website hosted on one server, but the embedded content is hosted and displayed to users from another server. While viewers could view the content on the third-party website directly, embedding allows the first website to provide contextual content alongside the embedded content.

This Court's own website illustrates how this works. The website contains pages where visitors can view recordings of the Court's oral arguments. Those recordings are embedded videos hosted on YouTube web servers. By embedding videos, this Court provides its website users important context such as the case name, case number, and panel for the oral argument alongside the video, and enables users to navigate easily to other parts of the Court's website. Viewers also could find the videos directly on YouTube, but embedding allows the Court's website to provide context about the video at the same time that it displays the video, while providing viewers with contemporaneous access to the website's other resources:

The World Wide Web is not the only Internet service that embeds content. Emails, for example, can embed images from other sources. If an email author wishes for the recipient to see an image, one option is to include the image itself in the email. Another option is to include embedded code in the email, effectively a "placeholder" pointing the recipient to the source of the image on a third-party server. When the recipient opens the email, the recipient's email client software—an application like Gmail or Outlook—will load the content of the email from the recipient's email server, retrieve the image from the image source's server, and then show the image within the email. This is why email applications sometimes ask email recipients for permission to show images; the images do not reside in the email itself but instead on servers that will transmit the images to the email recipient. Embedding makes emails significantly smaller and thus easier to transmit, since emails do not have to include the entire image that is embedded.

For example, email invitations from people or organizations often embed images containing more information about the event. When the recipient opens the email, the recipient's email client loads the image from a third party's web server. If the recipient forwards the email, the forwarded email retains the embedded link to the image on the third-party web server.

The same is true for text messages transmitted over the Internet, such as iMessage texts, WhatsApp messages, and Facebook messages. Text message users commonly send embedded content to each other. For example, one user may send another a link to an Amazon page to ask whether the item at that page would be a good gift for a mutual friend. The text message applications on the sending and receiving devices will typically display in the message an image and textual summary downloaded from an Amazon server (called a "link preview"). *See, e.g.*, https://developer.apple.com/library/archive/technotes/tn2444/_index.html.

2. Embedding Code

More broadly, web creators constantly embed code for various purposes, such as incorporating design elements, surveys, or maps; blocking unauthorized use; or advertising. To accomplish this, web creators can include in their own webpage software code that instructs the user's web browser to download additional code from third-party servers and interpret that code when displaying the webpage to the user. As with embedding content, this is typically as simple as writing a line of code in the webpage that points to the server containing the code to be embedded.

One common example is fonts, which like images can be subject to copyright restrictions.[7] Web creators can obtain access to a wide range of fonts from companies or communities. Many sources of web fonts are open source, which means (among other things) that they are free to use or incorporate. To display text on a website in a particular font, the creator of a website can insert a reference to load the code representing the font directly from the font provider. When a user later navigates to the website, the user's web browser loads the external code from the font provider's server. The user is in most cases never aware that the font displayed by the browser came from a source different than that of the website being viewed.

Another common example is translation—the ability for websites to offer dynamic translations of their content into other languages. When a website creator wants to incorporate translation functionality into a website, the creator simply can insert a reference to load translation code from a third-party translation provider like Google Translate. When a viewer navigates to the website, the user's browser loads the external code from the translation provider's server. This code typically instructs the browser to display something to the user, such as a button for the user to click, to allow the user to invoke translation.

[7] *See Adobe Sys. Inc. v. S. Software Inc.*, 1998 WL 104303, at *3-6 (N.D. Cal. Feb. 2, 1998).

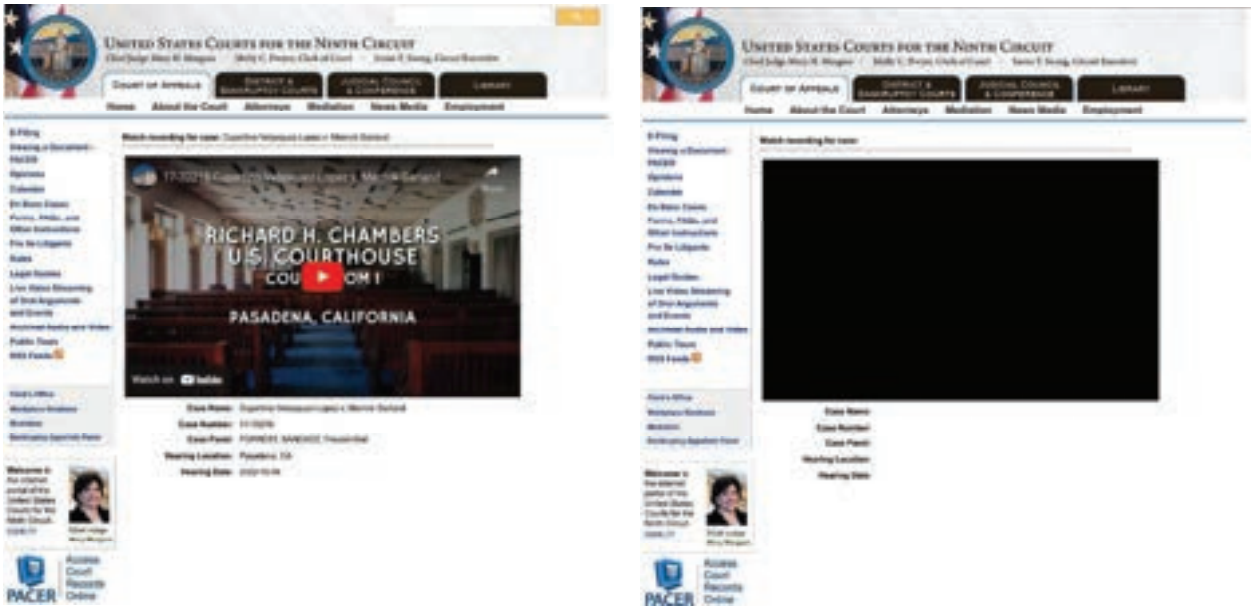
Yet another ubiquitous example is a CAPTCHA—the "tests" that websites use to determine whether a user is a human.[8] When a website creator wants to incorporate a CAPTCHA, the creator can obtain access to one from companies that provide them, some of which are open source. To incorporate the CAPTCHA into a website, the website creator inserts a reference to load code from the CAPTCHA provider. When a viewer navigates to the website, the user's browser loads the external code from the CAPTCHA provider's server—which also may load images, such as pictures of objects that may or may not be bicycles. CAPTCHAs are vitally important for cybersecurity on the Internet. Chandra Palan, *Importance of CAPTCHA in Web Security*, SecureBlitz (Nov. 30, 2019).[9]

Online calculators are yet another example. Webpage creators can embed code that generates a calculator to help the webpage visitors calculate various figures relevant to the services offered on the webpage—for example, monthly mortgage payments at various interest rates. *See, e.g.*, https://www.calcapp.net/lp/web-calculator/.

[8] For example, CAPTCHA tests protect against hackers using software to generate repeated password attempts or to generate automatic answers to on-line surveys in order to skew the survey responses.

[9] https://secureblitz.com/captcha-web-security/.

Most common websites include at least a handful and often dozens of pieces of embedded code like this. This Court's website, discussed above, is just one example. As shown in the images below, the website embeds not only videos of oral arguments from YouTube, but also case information and search functionality. On the left is a page from the website displayed as intended, and on the right is the same page when viewed in a web browser with embedding disabled:[10]



Almost 95% of websites use at least one third-party resource, and the median website uses 21 third-party servers in some form. HTTP Archive, *Web Almanac Part I, Chapter 7: Third Parties* (last updated Jan. 20, 2022).[11]

[10] The Internet Society created these images. The image on the right was created by turning off embedded third-party content before loading the webpage.

[11] https://almanac.httparchive.org/en/2021/third-parties#prevalence.

D. Embedding Is a Critical Feature of the Internet

Whether applied to code or content, the concept of embedding is a fundamental aspect of the generativity and modularity principles that underpin the Internet and its success. The Internet as we know it could not function without embedding.

Embedding allows creators to incorporate modules that others have developed, facilitating the rapid generation of new content. Absent the ability to embed code, for example, website creators would have to provide their own translations to make their websites accessible around the world, develop their own CAPTCHAs or other security tools, and rely on users to have the right fonts installed. Embedding modules created by others frees creators to focus on generating creative content, not on reinventing what has been done already. In other words, embedding encourages generation.

Embedding also encourages and facilitates consumption. Embedding allows users to navigate the Web more easily and quickly, without having to follow multiple links to consume content from other websites. For example, users can quickly compare products visually on a product review that embeds images from Amazon. Users can translate a webpage without having to methodically copy and paste the webpage's text into a separate translation application. Users can see how to drive to their destination without having to input the destination's address in a separate online map. And embedding content

allows users to see the content in context—for example, the information provided next to this Court's YouTube videos and the other resources on the website, *supra* p. 16—rather than having to piece together the relevant context for themselves by navigating among websites.

A more prosaic, but still critical, practical implication of embedding is that it helps preserve precious (and expensive) server space. Without embedding technology, content creators would need to store all images, videos, maps, and other content used on their website on their own servers—or otherwise refrain from using such content at all. That approach would lead to wasteful hosting duplication, as the same content would need to be stored on many different servers. By hosting the content on one server, moreover, the hosting company maintains control over all modifications, ensuring that different versions of the same content or code are not floating around the Internet at the same time.

Embedding also promotes strong—and critical—security practices such as the use of CAPTCHAs, which weed out automated "bots" that seek to hack into or block access to websites. Many CAPTCHA systems use images—which are hosted on third-party servers—to discern whether a human or a bot is seeking to access a website. Any court ruling that increases the risk of using CAPTCHA services would significantly increase near-term cybersecurity risk

on the Internet. It is unrealistic to expect that hundreds of thousands of websites would have the resources or technical sophistication to create and operate their own "one off" CAPTCHA services.

In all of these ways, embedding lowers the barriers of entry both for creators and consumers of content. Creators can create and maintain websites more easily, quickly, and securely, and consumers benefit by having a wider array of content available to them that they can navigate more effectively. Curbing creators' ability to *embed* content, including to embed modules created by others, would hinder their ability to *generate* content. The Internet would be poorer as a result.

II. The Server Test Protects the Generativity and Modularity of the Internet

The "server test" challenged in this case plays a critical role in preserving the generativity and modularity of the Internet. The test correctly allocates copyright responsibility for content where it should lie: the entity that is actually transmitting—in the terms of the Copyright Act, "display[ing]"—a copy of the at-issue content from its server to users' devices. *See* 17 U.S.C. § 106(5); *see also id.* § 101 (defining "to display" in relevant part as "to show a copy of it"). In this case, that entity is Instagram, and there is no dispute that Plaintiffs licensed Instagram to display their images to the public. Instagram Br. 3, 7-9.

The entity that displays content from its server ultimately controls access to and display of that content. That entity could choose to prohibit embedded access to that content entirely. For example, Vimeo allows paid users who host video on Vimeo's servers to disable embedding of their videos. *See* https://vimeo.zendesk.com/hc/en-us/articles/224969968-Embedding-videos-overview. The displaying entity also could require users to enter a password, pay a fee, or solve a CAPTCHA to access the content. For example, to listen to an embedded Spotify song, a webpage user must have a Spotify account. *Supra* p. 15. Or the entity could choose to limit access to the content to a particular number of users or to users located in a particular geographic region. For example, the BBC permits other websites to embed live or recorded videos from the BBC's web servers, but some of these videos are not available outside the United Kingdom. *See* https://www.bbc.com/news/help-21352667. The entity also could choose to add code that collects data about users' access to that content—when they accessed it, or for how long—or to derive revenue from the content by, for example, requiring users to watch an advertisement before accessing it.

Critically, the hosting entity also controls any modifications to the content that it stores. It could choose to delete, modify, or replace the content at any time or for any reason. If it deletes the content, meaning that no content resides at the particular server location, any webpages that point to that

server location will have a broken embed. Web browsers viewing the webpage will be unable to view the content from the hosting server. If the hosting entity modifies or replaces the content, web browsers viewing a webpage that points to that server location will automatically view the new content from the server.

It is logical that the entity that controls content and chooses the conditions under which it will transmit a copy of that content to the public should bear responsibility for ensuring that it has the right to display it. Otherwise, innocent creators could face copyright (or other) liability for acts entirely outside their control. Assume, for example, that an entity initially stores a photograph in the public domain at a given location. Third-party websites might then embed that photograph by directing web browsers to retrieve the image stored at that location. Suppose the entity then elects to replace that photograph with another one that is not in the public domain and for which it lacks the right to display the image. When a user visits the third-party website, her web browser will retrieve a copy of the new photograph because of the actions of the entity storing that photograph on its server—all without the knowledge of the third-party website creator.

Consider other examples. Under Plaintiffs' view of the Copyright Act, a journalist who embeds a video might be liable for a copyrighted image that appears somewhere in the video, on the theory that the journalist "displayed"

the video. Website operators that embed a third party's CAPTCHA technology might be liable if the CAPTCHA image, unbeknownst to the website operators, includes copyrighted photographs. An author of a music review who embeds a song from a service such as Spotify might be liable if Spotify failed to obtain the requisite license to play the song. The list goes on and on.

The potential for sweeping copyright liability across the Internet could force dramatic changes to the way the Internet functions. Even if defenses such as fair use might protect content creators in individual cases, *see Perfect 10*, 508 F.3d at 1168, the risk of liability and uncertainty of application of such defenses would chill embedding. The Internet would become less open and accessible. Content creators would eschew embedded content in favor of links, requiring more time-intensive navigation among websites. Content-hosting providers might become reluctant to permit embedding, maybe even blocking others from embedding content from the provider's site, even when the content creators that first uploaded the content ask to have it available to be embedded.

And operating user-friendly websites would be a significantly more cumbersome and expensive endeavor. Website creators would have to develop themselves or pay for functionality such as CAPTCHA technology intended to protect their websites. Even if they pay for such functionality (which many

website operators could not afford), that would not protect them from copyright suits if the embedded CAPTCHA technology infringes another's copyright; at best, they might have the right to contractual indemnification from the CAPTCHA provider. Creators would have to buy additional servers to host all the content they would now need to store on their own servers—producing an explosion of duplicative public domain content being stored across many servers. And news services would be far less effective in conveying to readers the context and significance of news stories that involve newsworthy tweets or other content, as in this case.

More broadly, the Internet would become less modular. Users would be unable to build off each other and link to each other's creative content. And the Internet would become less generative. Some content creators would stop creating content. Others would stop because they could not create the tools they need to protect or profit from their websites.

The end result of adopting Plaintiffs' rule would be an Internet that is less open to generation. The elimination or paring back of the server test, in short, would pull the Internet away from its role as "a resource to enrich people's lives, and a force for good in society." *Supra* p. 3.

CONCLUSION

The Court should affirm the decision below.

Respectfully submitted,

/s/ Amy Mason Saharia

AMY MASON SAHARIA
D. SHAYON GHOSH
WILLIAMS & CONNOLLY LLP
680 Maine Avenue, S.W.
Washington, DC 20024
(202) 434-5000
asaharia@wc.com

OCTOBER 11, 2022

CERTIFICATE OF COMPLIANCE
WITH TYPEFACE AND WORD-COUNT LIMITATIONS

I, Amy Mason Saharia, counsel for appellant and a member of the Bar of this Court, certify, pursuant to Federal Rule of Appellate Procedure 32(g)(1) and Ninth Circuit Rule 32, that the attached Brief of Amicus Curiae Internet Society, is proportionately spaced, has a typeface of 14 points or more, and contains 6,034 words.

/s/ Amy Mason Saharia

AMY MASON SAHARIA
WILLIAMS & CONNOLLY LLP
680 Maine Avenue, S.W.
Washington, DC 20024
(202) 434-5000
asaharia@wc.com

OCTOBER 11, 2022

CERTIFICATE OF SERVICE

I, Amy Mason Saharia, counsel for appellant and a member of the Bar of this Court, certify, that, on October 11, 2022, a copy of the attached Brief of Amicus Curiae Internet Society was filed with the Clerk through the Court's electronic filing system. I further certify that all parties required to be served have been served.

/s/ Amy Mason Saharia

AMY MASON SAHARIA
WILLIAMS & CONNOLLY LLP
680 Maine Avenue, S.W.
Washington, DC 20024
(202) 434-5000
asaharia@wc.com

OCTOBER 11, 2022