Exhibit 1

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

JUSTIN GOLDMAN *Plaintiff,* v. BRIETBART NEWS NETWORK, LLC; HEAVY, INC.; TIME, INC.; YAHOO, INC.; VOX MEDIA, INC.; BOSTON GLOBE MEDIA PARTNERS, LLC; NEW ENGLAND SPORTS NETWORK, INC., *Defendants.*	1:17-cv-3144-KBF

AMICUS BRIEF OF THE ELECTRONIC FRONTIER FOUNDATION AND PUBLIC KNOWLEDGE IN SUPPORT OF DEFENDANTS' MOTION FOR PARTIAL SUMMARY JUDGMENT

CORPORATE DISCLOSURE STATEMENT[1]

Pursuant to Federal Rule of Civil Procedure 7.1 and Local Rule 7.1.1, Amici Curiae Electronic Frontier Foundation and Public Knowledge (collectively, "Amici") state that neither of them has a parent corporation and that no publicly held corporation owns 10% or more of the stock of either of them.

[1] No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief.

TABLE OF CONTENTS

INTEREST OF AMICI CURIAE 1

INTRODUCTION 2

ARGUMENT 3

I. THE "SERVER TEST" IS A STRAIGHTFORWARD AND CORRECT APPLICATION OF THE COPYRIGHT ACT 3

A. How Online Images Work 3

1. HTML Files and Image Files 3

2. The Analog Equivalent of Online Images 5

3. The Links At Issue Here Follow the Same Process 6

B. The "Server Test" Properly Places Responsibility on the Entity That Transmits or Communicates the Copyrighted Work 6

II. THE SERVER TEST HAS BEEN ESSENTIAL TO THE GROWTH OF THE INTERNET AS A VEHICLE FOR SPEECH AND COMMERCE 8

III. THE SERVER TEST IS CONSISTENT WITH THE ARCHITECTURE OF THE DMCA'S SAFE HARBORS 10

IV. ABANDONING THE SERVER TEST WOULD HURT USERS WHO COULD UNKNOWINGLY INFRINGE 12

A. Undermining the Server Test Could Create Liability for Users Far Beyond the Sophisticated Defendant Targeted Here 12

B. Licensing and Fair Use Will Not Suffice to Protect Users and Platforms 13

V. RIGHTSHOLDERS HAVE OTHER OPTIONS THAT WOULD CAUSE FAR LESS COLLATERAL DAMAGE 14

CONCLUSION 16

TABLE OF AUTHORITIES

Cases

Am. Broadcasting Cos. v. Aereo, Inc.,
134 S. Ct. 2498 (2014) 7, 9

Brownmark Films, LLC v. Comedy Partners,
682 F.3d 687 (7th Cir. 2012) 14

BWP Media USA v. T&S Software Associates Inc.,
852 F.3d 436 (5th Cir. 2017) 9

Capitol Records, LLC v. Vimeo, LLC,
826 F.3d 78, 82 (2d Cir. 2016) 10

Cartoon Network LP, LLLP v. CSC Holdings, Inc.,
536 F.3d 121 (2d Cir. 2008) 9

CoStar Group, Inc. v. LoopNet, Inc.,
373 F.3d 544 (4th Cir. 2004) 9

Flava Works, Inc. v. Gunter,
689 F.3d 754 (7th Cir. 2012) 7

Grady v. Iacullo,
2016 WL 1559134 (D. Colo. Apr. 18, 2016) 7

Katz v. Google, Inc.,
802 F.3d 1178 (11th Cir. 2015) 14

Leveyfilm, Inc. v. Fox Sports Interactive Media, LLC,
2014 WL 3368893 (N.D. Ill. July 8, 2014) 7

Lipton v. Nature Co.,
71 F.3d 464 (2d Cir. 1995) 13

Live Face on Web, LLC v. Biblio Holdings LLC,
2016 WL 4766344 (S.D.N.Y. Sept. 13, 2016) 7

MAI Sys. Corp. v. Peak Computer, Inc.,
991 F.2d 511 (9th Cir. 1993) 15

MyPlayCity, Inc. v. Conduit Ltd.,
2012 WL 1107648 (S.D.N.Y. Mar. 30, 2012) 7

Nakada + Associates, Inc. v. City of El Monte,
2017 WL 2469977 (C.D. Cal. June 2, 2017) 7

Packingham v. North Carolina,
137 S. Ct. 1730 (2017) 8

Pearson Educ., Inc. v. Ishayev,
9 F. Supp. 3d 328 (S.D.N.Y. 2014) 7

Perfect 10 v. Google,
416 F. Supp. 2d 828 (C.D. Cal. 2006) 8

Perfect 10, Inc. v Amazon, Inc.
508 F.3d 1146 (9th Cir. 2007) 6, 7, 11

Perfect 10, Inc. v. Giganews, Inc.,
847 F.3d 657 (9th Cir. 2017) 9

Reno v. America Civil Liberties Union,
521 U.S. 844 (1997) 8

S.O.S., Inc. v. Payday, Inc.,
886 F.2d 1081 (9th Cir. 1989) 15

Savage v. Council on American-Islamic Relations, Inc.,
2008 WL 2951281 (N.D. Cal. July 25, 2008) 14

Totally Her Media, Inc. v. BWP Media USA, Inc.,
2015 WL 12659912 (C.D. Cal. Mar. 24, 2015) 7

Viacom Int'l. Inc. v. YouTube. Inc.,
676 F.3d 19 (2d Cir. 2012) 10, 14

Statutes

17 U.S.C. § 101 6

17 U.S.C. § 106 15

17 U.S.C. § 107 14

17 U.S.C. § 504 10

17 U.S.C. § 512 ..... 10, 11, 12, 15

Legislative Materials

H.R. Rep. No. 105-190 (1998) 15

H.R. Rep. No. 105-551 (1998) 12

S. Rep. No. 105-190 (1998) 12

Other Authorities

Andrew Berger, *Brownmark v. Comedy Partners: Court finds Fair Use Without Allowing Plaintiff Any Discovery*, IP In Brief (July 19, 2012), http://www.ipinbrief.com/brownmark-v-comedy-court-finds-fair-use-without-discovery/ 14

Jamie Williams, *Court of Appeals Rejects Attempt to Use Copyright to Censor Online Speech*, EFF Deeplinks (Sept. 17, 2015), https://www.eff.org/deeplinks/2015/09/court-appeals-rejects-attempt-use-copyright-censor-online-speech 14

Kurt Opsahl, *Fair Use Prevails Over Michael Savage's Copyright Claims*, EFF Deeplinks (July 28, 2008), https://www.eff.org/deeplinks/2008/07/fair-use-prevails-over-michael-savages-copyright-c 14

INTEREST OF AMICI CURIAE

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit public interest organization dedicated to protecting digital civil liberties and free expression. With more than 38,000 dues paying members, EFF promotes the sound development of copyright as a balanced legal regime that fosters creativity, innovation, and the spread of knowledge.

Public Knowledge ("PK") is a Washington, D.C. based not-for-profit public interest advocacy and research organization. PK promotes balance in intellectual property law and technology policy to ensure that the public has access to knowledge and the ability to freely communicate and innovate in the digital age.

INTRODUCTION

Everyday, Internet users of all kinds—bloggers, librarians, educators, political activists, students, job-seekers, and so on—share information and ideas online, using in-line links. Links do exactly what you might expect: they connect the reader to an original piece of material that a second person wants to comment on or simply call to attention. As part of the original design of the Internet hypertext medium, in line linking powerfully enhances users' ability to acquire and share information and ideas. It is an essential form of Internet communication.

If Plaintiff and Amicus Getty Images, Inc. have their way, however, the well-settled legal framework for linking would be upended, at least in this Circuit.[2] For almost a decade, users and intermediaries have relied on the 9th Circuit's "server test" to assess the potential legal risk of linking to content. The server test sensibly divides liability for infringement, assigning strict liability to the entity that is actually hosting the content and "serving" it to the rest of the Internet. That entity is best positioned to know whether the content is lawful, has the strongest incentive to take it down if it finds otherwise, and has the ability to do so. Third parties that direct people to that content can be held secondarily liable, if additional factors are present such as affirmative steps to encourage infringement. Absent those additional factors, third parties generally are not well-positioned to determine whether or not the content is lawful, can't control its original context, and aren't empowered to actually take it offline.

The server test is a logical interpretation of the Copyright Act that has become a legal cornerstone of Internet communication. Amici submit this brief on behalf of the many users and innovators that rely on the server test and would be harmed if this Court accepts Plaintiff's

[2] Amici have reviewed the amicus brief filed by Getty Images (US), Inc. in the related *Goldman v. Advance Publications, Inc.* proceedings, and understand that Getty will be filing a similar brief in this case. Case No. 1:16-cv-9031-ALC, Dkt. No. 30-1 (S.D.N.Y. compl. filed Nov. 21, 2016) ("Getty Br.").

invitation to create a circuit split. We urge the Court to reject that invitation.

ARGUMENT

I. THE "SERVER TEST" IS A STRAIGHTFORWARD AND CORRECT APPLICATION OF THE COPYRIGHT ACT

In the analog world, a person is free to tell others where they may view a third party's display of a copyrighted work, without being directly liable for infringement if that display turns out to be unlawful. The server test is the straightforward application of the same principle in the online context, which is one reason it has been widely embraced. It should govern here as well.

A. How Online Images Work

1. HTML Files and Image Files

Three different actors are involved when a user visits a webpage and views an image served by a third party: the user, administrator of the webpage's server, and the administrator of the image's server.

When a user visits a webpage, such as by typing a web address like "www.eff.org" into a browser (e.g. Safari, Firefox, or Chrome), their computer sends a request to that web address for a text file written in the "Hyper-Text Markup Language" (HTML). That HTML text file includes, among other things, words to be displayed and web addresses of additional content such as images.

The browser on the user's computer interprets that HTML file according to the preferences or defaults the user has set. The browser may behave as the website operator expects, or the user may have set other preferences. A user may have specified that text shall be displayed in a larger font, or block any content from known advertisers, or that audio should not be played unless they affirmatively click play. Many people with visual impairment configure their web browsers to not retrieve images at all, as do some people operating with very slow Internet connections. Many security- and privacy-related browser add-ons cause the browser to refuse to retrieve some images and other content, while several email services decline to retrieve images unless the user affirmatively indicates they wish to do so.

Because an HTML file is text, it cannot contain images. Instead, it *refers* to images according to their web address via a process called "in-line linking." For instance, the website at www.eff.org could refer to an image www.eff.org/logo.jpg, if there were such an image. This address translates to "the file called logo.jpg on the server named www.eff.org." The browser would then decide whether to attempt to retrieve the image.

In this example, the HTML file and the image are on the same server, the one at www.eff.org. But the www.eff.org HTML file could just as easily refer to another image on the Internet, such as www.whitehouse.gov/image1.jpg. In either case, if the browser attempts to retrieve that image, it will use the web address of the image to contact the hosting server and request the image associated with that address. Assuming such a file exists, and assuming the server is configured to respond to such a request, the server would transmit the image file to the user's computer, and their browser would decide whether and how to present it onscreen.

Whoever controls a server dictates whether and how it responds to requests for files. In the hypothetical case where www.eff.org includes a reference to www.whitehouse.gov/image1.jpg, whoever controls the whitehouse.gov server determines the contents of that "image1.jpg" file. If that web address initially pointed to a picture of the White House at the time that www.eff.org linked to it, but the operator of the whitehouse.gov server changes it so that "image1.jpg" is now a picture of the President, then the server will transmit a picture of the President when it receives that request from a user's browser.

Likewise, the person who runs a server has the power to decide which files are available to which requesters. For instance, many servers have private files. If your computer asks the server to provide such a file, it will politely decline (this is one cause of online error messages such as "Error 504: Forbidden"). Services like Cloudflare that help host web content have custom error messages to communicate when direct links to images are not permitted. Other servers refuse requests from certain parts of the world, or any request that does not come from a trusted computer.

Ultimately, the server that receives a request for a file controls what content to provide and whether to provide it at all to that requestor. Whatever content it provides travels directly across the Internet to the requestor; it does not pass through the control or awareness of the website provider. For instance, in the example above, the server at www.eff.org does not know whether or how the server at www.whitehouse.gov responded to the request for image1.jpg.

If the server does provide the content, the user's browser decides whether and how to present that content on the user's screen. By default, most browsers choose to depict images without accompanying information about what server provided them, unless a user clicks on the image for additional information. Thus, many users experience webpages as seamless collections of content from different sources. This is the ordinary and expected functionality of web browsers that people use to experience the Internet. It is not a nefarious or misleading practice, nor is it even within the ultimate control of a website designer. Rather, a user's web browser decides whether to highlight or obscure information about the source of each element of a web page, such as each image.

2. The Analog Equivalent of Online Images

To better understand how the above process works, imagine that a reporter, Wanda, has written a story about a safety issue in Toyota cars. She prints paper copies of the story, but she doesn't have her own image to illustrate it. She recalls that her friend Sally, the illustrator, does have such an image. So Wanda leaves a rectangle of space in her article, with the instructions "Cut out this rectangle, then ask Sally for picture #3, and peer at it through the opening."

Ronald, the reader, gets a copy of the article and decides to follow the instructions. So, he goes to Sally, asks her for picture #3, and she lifts up a picture of a Toyota. Ronald holds up Wanda's article and sees the picture through the cut-out. Meanwhile, Wanda is across town, unaware of whether Ronald visited Sally, whether Sally agreed to his request, or whether "picture #3" is still the illustration it was when she last visited Sally.

In the online context, Wanda is the website creator and Sally operates the server where images may be found. Wanda tells readers like Ronald where to go and what image to ask for, and Sally decides how to respond to the request.

3. The Links At Issue Here Follow the Same Process

The activity at issue here follows exactly the process outlined above. When a user navigates to a story hosted by a defendant, say one hosted by Yahoo!, the user's browser program interprets HTML instructions on Yahoo's webpage. These HTML instructions provide the user's browser with the address of the website for the third-party service's computer that stores the content (in this case, Twitter). By following the HTML instructions to access the third-party webpage, the user's browser connects to the website publisher's computer, downloads the full-size image, and makes the image appear at the bottom of the window on the user's screen.

The only question, then, is how the Court should assess liability for potentially infringing links. The answer is clear: the Court should apply the server test.

B. The "Server Test" Properly Places Responsibility on the Entity That Transmits or Communicates the Copyrighted Work

Decades after the enactment of the 1976 Copyright Act, the Internet presented seemingly novel questions of when and who could violate the display right the Act described. Keeping in mind the process described above, the Ninth Circuit correctly determined that these questions can be resolved by reference to the statutory language assigning liability to the party that "show[s] a copy of it," noting that a copy is a "material object[] . . . in which a work is fixed . . . and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device." *Perfect 10, Inc. v Amazon, Inc*. 508 F.3d 1146, 1160 (9th Cir. 2007); 17 U.S.C. § 101.

The court correctly concluded that in-line linking to an image hosted on a third party server is not a direct infringement of the display right:

> Because Google's computers do not store the photographic images, Google does not have a copy of the images for purposes of the Copyright Act . . . and thus cannot communicate a copy. Instead of

> communicating a copy of the image, Google provides HTML instructions [via in-line linking] that direct a user's browser to a website publisher's computer that stores the full-size photographic image. Providing these HTML instructions is not equivalent to showing a copy.

Id. at 1160-61. This doctrine – that the owner of a website that does not *store* an image on its own server, but rather provides an *in-line link* to it, is not displaying the image for purposes of direct copyright infringement – is known as the "server test." *Id.* at 1159. In the decade that followed that 2007 decision, numerous courts considering this issue, including courts in this District, have sensibly embraced it. *See e.g.*, *Flava Works, Inc. v. Gunter*, 689 F.3d 754, 756 (7th Cir. 2012); *Pearson Educ., Inc. v. Ishayev*, 9 F. Supp. 3d 328, 338 (S.D.N.Y. 2014); *Live Face on Web, LLC v. Biblio Holdings LLC*, 2016 WL 4766344, at *4 (S.D.N.Y. Sept. 13, 2016); *Grady v. Iacullo,* 2016 WL 1559134, at *5 (D. Colo. Apr. 18, 2016); *Totally Her Media, Inc. v. BWP Media USA, Inc.*, 2015 WL 12659912, at *10 (C.D. Cal. Mar. 24, 2015); *Leveyfilm, Inc. v. Fox Sports Interactive Media, LLC*, 2014 WL 3368893, at *5 (N.D. Ill. July 8, 2014); *MyPlayCity, Inc. v. Conduit Ltd.*, 2012 WL 1107648, at *12 (S.D.N.Y. Mar. 30, 2012), *adhered to on recons.,* 2012 WL 2929392 (S.D.N.Y. July 18, 2012); *Nakada + Associates, Inc. v. City of El Monte*, 2017 WL 2469977 *4 (C.D. Cal. June 2, 2017).

The server test is bolstered by guidance from Supreme Court's *Aereo* decision. The Court held that "an entity only transmits a performance when it communicates contemporaneously perceptible images and sounds of a work." *Am. Broadcasting Cos. v. Aereo, Inc.*, 134 S. Ct. 2498, 2510 (2014). By the same token, an entity only transmits an image when it communicates the perceptible image itself. Moreover, in its analysis of the public performance right, the Court repeatedly referred to scenarios in which an entity *possessed a copy* of an audiovisual work and physically transmitted the signal embodying that work. *Id.* That is precisely what a server does in response to a file request.

In sum, the server test is a sensible, statutorily rooted approach to liability that places the principal responsibility for any infringement on the entity that actually communicates the work rather than the myriad entities that simply point to it.

Plaintiff and Getty's proposed approach, by contrast, defies logic – as well as the text of the Copyright Act – by holding directly liable actors who do not possess and cannot transmit or communicate a copy of a work. It would hold website operators directly liable based on what users see after their browsers retrieve images from third-party servers, even though the operators are not ultimately in control of what users see or even what content those third-party servers provide. Copyright's strict liability scheme is expansive enough; the Court should resist Plaintiff's request to push it beyond practical and statutory bounds.

II. THE SERVER TEST HAS BEEN ESSENTIAL TO THE GROWTH OF THE INTERNET AS A VEHICLE FOR SPEECH AND COMMERCE

It seems that Plaintiff and Getty would like to see the Court adopt something like the incorporation test that was considered and rejected in the *Perfect 10* proceedings. *Perfect 10 v. Google*, 416 F. Supp. 2d 828, 839 (C.D. Cal. 2006). One reason for that rejection was that it "would cause a tremendous chilling effect on the core functionality of the web—its capacity to link, a vital feature of the internet that makes it accessible, creative, and valuable." *Perfect 10*, 416 F. Supp. 2d at 840. If anything, the district court understated the negative impact anything like the incorporation test would have had on the vitality of the Internet, and its utility as an engine of free expression and innovation.

This past term, the Supreme Court identified "cyberspace—the 'vast democratic forums of the Internet' in general—and social media in particular," as a crucial vehicle for free expression. *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017) (quoting *Reno v. America Civil Liberties Union*, 521 U.S. 844, 868 (1997))

The emergence of that vehicle has depended, in significant part, on the legal certainty the server test provides. The server test's limit on direct liability for linking encourages users and platforms to create interesting and informed content that contains links to other sites, leading to a better-informed and more diverse public sphere. E-commerce sites can employ embedded links to enable consumers to comparison shop. Online advertisers of all kinds, including political

campaigns, can embed links to images and related information. And libraries, educators and social agencies can use links to educate, inform and empower their users.

Equally importantly, the server test provides legal certainty to service providers that allow user-supplied content to reside on their sites.[3] Thanks to that certainty, a blogger can embed tweets commenting on particular news events to show the development of a story. An educator can embed images of famous works of art to illustrate a particular style. And an email sender can embed an image, and have that email forwarded to hundreds to thousands of people without their knowledge. These are all normal, everyday activities that Plaintiff and Getty would argue infringe on the display right absent fair use, license, or some other defense.

In addition, the server test spurs electronic commerce by allowing both users and professional creators to drive traffic to other sites. Under the server test, Facebook, for example, need not worry about direct infringement liability for a user post that embeds a link to YouTube or Twitter, and will therefore allow and even encourage it. Countless blogs and news articles embed links to videos posted on YouTube. Twitter, YouTube, and other social media platforms provide users with tools to make embedding as easy as possible. Platforms may benefit from the demand via embedded links for the content they host: directly or indirectly, this demand leads to more traffic and advertising revenue that, in turn, makes it possible for new platforms to emerge.

Under the incorporation test, by contrast, users would hesitate before embedding a link in their content for fear of incurring direct infringement liability. Because copyright is a strict liability offense, users could incur statutory damages of up to $150,000 for each embedded link

[3] To be clear, even in the absence of a server test, a platform would likely argue that it could not be directly liable because it did not engage in volitional conduct with respect to that content. *See BWP Media USA v. T&S Software Associates Inc*., 852 F.3d 436, 440 (5th Cir. 2017); *Perfect 10, Inc. v. Giganews, Inc.*, 847 F.3d 657, 666-67 (9th Cir. 2017); *Cartoon Network LP, LLLP v. CSC Holdings, Inc.*, 536 F.3d 121, 131 (2d Cir. 2008); and *CoStar Group, Inc. v. LoopNet, Inc.*, 373 F.3d 544, 551 (4th Cir. 2004). Nevertheless, some copyright owners wrongly persist in arguing that the volitional conduct doctrine did not survive the Supreme Court's decision in *American Broadcasting Company v. Aereo, Inc.*, 134 S. Ct. 2498 (2014). Moreover, identifying the volitional actor can be difficult – and therefore expensive—in some fact patterns.

to a work that may be infringing. 17 U.S.C. § 504(c)(2). In the face of such enormous potential liability, many would fear to link to anything, or embed links only to images and videos they were positive were noninfringing. Among other effects, this would encourage users to link only to images and videos posted by major media outlets or corporations, because they could reasonably assume that those did their due diligence and did not post infringing content.

What is worse, the platforms upon which many users rely to share information would hesitate to allow many forms of user-generated content. To avoid the risk of liability, platforms might have to conduct a legal review of all such content too root out any links that could lead to direct liability. Given the cost of such a review, most would choose to avoid the risk at all.

III. THE SERVER TEST IS CONSISTENT WITH THE ARCHITECTURE OF THE DMCA'S SAFE HARBORS

Not only is the server test consistent with the architecture of the Internet; it is consistent with the architecture of the Digital Millennium Copyright Act ("DMCA"). As the Second Circuit recently held, Congress enacted the DMCA in 1998 "to update domestic copyright for the digital age." *Capitol Records, LLC v. Vimeo, LLC*, 826 F.3d 78, 82 (2d Cir. 2016) (quoting *Viacom Int'l, Inc. v. YouTube, Inc*., 676 F.3d 19, 26 (2d Cir. 2012)) (internal citations and quotation marks omitted). The DMCA established four safe harbors, codified at 17 U.S.C. § 512, which protect qualifying Internet service providers from certain remedies for copyright infringement. The Court explained that the DMCA "insulates service providers from liability for infringements of which they are unaware . . . so as to make it commercially feasible for them to provide valuable Internet services to the public." *Id*.

Two of the four safe harbors are pertinent here. Section 512(c) limits the liability of service providers "for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider . . . " Thus, the Section 512(c) safe harbor shelters the service provider from liability

arising from its hosting of content uploaded by users.[4] Section 512(d) limits the liability of service providers "for infringement of copyright by virtue of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link . . . " Thus, the Section 512(d) safe harbor shelters the service provider from liability arising from its linking to sites containing infringing content.

Under the logic of the incorporation test, there would be no need for two separate safe harbors: hosting infringing content would be the same as linking to infringing content. That is not the logic Congress adopted. Instead, Congress recognized that hosting and linking were conceptually different, and that different rules should apply to each. In the case of hosting, the infringing activity is occurring on a network controlled or operated by the service provider. Accordingly, the service provider is eligible for the Section 512(c) safe harbor only with respect to content stored "at the direction of a *user,*" § 512(c) (emphasis supplied), rather than, say, content the service provider has chosen to post itself.

In the case of linking, however, the infringing activity is occurring on a third-party site beyond the control of the service provider. Section 512(d) is intended to shelter that distinct situation: it specifically applies to potential infringement arising from "the *provider* referring or linking users to an online location . . . " § 512(d) (emphasis supplied). Further, the safe harbor is not limited to directories or search engines that rely on bots or automated processes to establish

[4] To be clear, the existence of the DMCA's safe harbors does not diminish the importance of the server test for Internet platforms. Eligibility for the DMCA's safe harbors is conditioned on the service provider meeting a variety of procedural requirements, including identifying a DMCA agent on the provider's website, registering the agent with the Copyright Office, and adopting and implementing a policy for terminating the accounts of repeat infringers. Further, the service provider loses protection if it is aware of facts and circumstances from which infringing activity is apparent. If the service provider receives a claim of infringement from the copyright owner, it must remove or disable the infringing material expeditiously. In copyright litigation against service providers, copyright owners often argue that the service providers have lost their eligibility for the DMCA's protection. In *Perfect 10 v. Amazon.com*, for example, Perfect 10 argued unsuccessfully that Google did not qualify for the DMCA's safe harbors.

the links. Instead, the DMCA's report language explicitly addresses human involvement in creating links. When the DMCA was pending before Congress in 1998, the Internet portal Yahoo! expressed concern about its eligibility for this safe harbor because its employees actually visited websites to determine whether to include them in its directory. In response, the House and Senate Judiciary Committees adopted reports clarifying that a directory such as Yahoo! did not lose its safe harbor by virtue of its employees visiting and then linking to websites that turn out to contain infringing content. S. Rep. No. 105-190 (1998), at 49; *see also* H.R. Rep. No. 105-551, pt. 2 (1998), at 58. The reports explain that Section 512(d) "is intended to promote the development of information location tools generally, and Internet directories such as Yahoo!'s in particular, by establishing a safe harbor from copyright infringement liability . . . " *Id*.

In sum, the DMCA recognizes the profound difference between hosting and linking to infringing content. The server test reflects and complements that recognition.

IV. ABANDONING THE SERVER TEST WOULD HURT USERS WHO COULD UNKNOWINGLY INFRINGE

As the foregoing should suggest, the stakes of this litigation go far beyond the implications for the parties in this case. Any judicial decision undermining the server test could expose Internet users of all stripes to direct liability, often for conduct that is largely out of their control.

A. Undermining the Server Test Could Create Liability for Users Far Beyond the Sophisticated Defendant Targeted Here

Embedding links is not just the province of media companies such as the Defendants in this case. As noted, Internet users across the economic and resource spectrum regularly embed content that is hosted elsewhere, relying (knowingly or not) on the server test to engage in everyday acts without the risk of crippling copyright liability. A rule that threatens strict liability for any image displayed as a result of the transmission of a URL (whether expressed as a link, in-line link, or frame) would radically change linking practices, and thereby transform the Internet as we know it. The fast-moving, cross-linked array of resources that constitutes much of the Web

would be replaced by fewer, more-isolated publications willing to link to each other only after consulting with their errors & omissions insurers.

The chilling effect of such a rule would only be exacerbated by the absurdity of its results. For example, imagine that an unauthorized display of Goldman's image appears in the next episode of the popular HBO football reality series, "Hard Knocks," which is also made available from HBO's website. While HBO might face the possibility of direct infringement liability for broadcasting the image to the public on TV and transmitting it to the public from its website, Getty's conception of the public display right could also result in strict liability for fans who emailed friends or family with a link to the episode on HBO's website, if a court concluded that the email was a communication that "caused" the images to appear. [5]

B. Licensing and Fair Use Will Not Suffice to Protect Users and Platforms

To tidy up the mess created by its overbroad conception of public display, Amici expect Getty will again propose that the courts and parties can rely on the fair use doctrine or licensing to excuse the bulk of nominal infringements. This proposal falls far short of solving the problem, trading legal certainty for the prospect of expensive and uncertain litigation.

For example, absent the server test, those embedding content would potentially expose themselves to liability even though they believe their uses to be fully licensed. For example, those who embed YouTube content cannot raise the license in YouTube's terms of service as a defense to liability if the content was not lawfully uploaded. *See, e.g.*, *Lipton v. Nature Co*., 71 F.3d 464, 471 (2d Cir. 1995) ("[C]opying from a third source wrongfully copied from the plaintiff, without knowledge that the third source was infringing, does not absolve a defendant of liability for copyright infringement.") This is true even if there is every indication that the

[5] Again, we refer here to a theory Getty presents in a brief filed in the related *Goldman v. Advance Publications* litigation that we understand Getty will introduce in this case as well.

content *was* lawfully uploaded.[6] And those who embed cannot reasonably track down each user to confirm the licensing was proper.

Nor is it feasible to rely on fair use (17 U.S.C. § 107) to protect those who embed. Unfortunately, fair use can be expensive to determine and difficult to decide at the margins, and in light of those features, can be difficult for users to predict. Moreover, rightsholders often have extremely conservative views of what qualifies as fair use, which means that they may pursue legal action even in clear instances of fair use.[7] Given this reality, the prospect of litigation will discourage users and platforms alike from taking the risk in all but the narrowest of circumstances.

V. RIGHTSHOLDERS HAVE OTHER OPTIONS THAT WOULD CAUSE FAR LESS COLLATERAL DAMAGE

Denying Plaintiff the ability to hold media companies directly liable for links does not leave Plaintiff or other injured rights holders without a remedy. Copyright law has already developed other doctrines to appropriately place liability on those who *control* the display of a work, rather than those who merely provide a link to it.

---

[6] YouTube, of course, is likely protected by the DMCA. *See Viacom*, 676 F.3d at 35.

[7] *See, e.g.*, Kurt Opsahl, *Fair Use Prevails Over Michael Savage's Copyright Claims*, EFF Deeplinks (July 28, 2008), https://www.eff.org/deeplinks/2008/07/fair-use-prevails-over-michael-savages-copyright-c (discussing the grant of a defendant's motion for judgment on the pleadings that defendant's use of a four-minute audio clip in order to criticize the statements made in the clip was fair use, *Savage v. Council on American-Islamic Relations, Inc.*, 2008 WL 2951281 (N.D. Cal. July 25, 2008)); Andrew Berger, *Brownmark v. Comedy Partners: Court finds Fair Use Without Allowing Plaintiff Any Discovery*, IP In Brief (July 19, 2012), http://www.ipinbrief.com/brownmark-v-comedy-court-finds-fair-use-without-discovery/ (discussing a 7th Circuit opinion affirming dismissal on the pleadings based on a finding of fair use in the television show South Park's use of a parody of a song, *Brownmark Films, LLC v. Comedy Partners*, 682 F.3d 687 (7th Cir. 2012)).
Jamie Williams, *Court of Appeals Rejects Attempt to Use Copyright to Censor Online Speech*, EFF Deeplinks (Sept. 17, 2015), https://www.eff.org/deeplinks/2015/09/court-appeals-rejects-attempt-use-copyright-censor-online-speech (discussing an 11th Circuit opinion affirming grant of summary judgment of fair use where copyright owner attempted to use copyright in photo to stifle critical speech, *Katz v. Google, Inc.*, 802 F.3d 1178 (11th Cir. 2015)).

The first and most obvious tool in the arsenal of an aggrieved artist is a claim of direct copyright infringement against a proper party. Direct infringement is the most legally straightforward option, with only two requisite elements: "ownership of a copyright and a copying of protectable expression beyond the scope of a license." *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 517 (9th Cir. 1993) (quoting *S.O.S., Inc. v. Payday, Inc.*, 886 F.2d 1081, 1085 (9th Cir. 1989) (internal quotations removed)).

It is unclear why Plaintiff chose to forego a simple claim of direct infringement in this instance. In this case, Plaintiff alleges that one or more Twitter users uploaded Plaintiff's photo to Twitter without his permission. To the extent that any copyright infringement occurred, it occurred at this stage; in re-uploading the photo without permission, these users likely violated Plaintiff's rights of distribution and display.[8] 17 U.S.C. § 106. Plaintiff could have easily levied a claim of direct infringement against the actual uploader of the photo.

A second option for Plaintiff would be to avail himself of the uniquely powerful tools provided in the DMCA. The DMCA's safe harbors require, as on condition of immunity, that service providers hosting user-generated content, "upon notification of claimed infringement . . . expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity." 17 U.S.C. § 512(c). By design, this provision "preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment." H.R. Rep. No. 105-190, at 20 (1998).

Plaintiff would have achieved the exact result he seeks here if he had simply availed himself of Section 512's procedures. If he had sent Twitter a "takedown" notice, Twitter would

[8] For the sake of brevity (and to avoid duplicating any potential argument put forward by the parties), we assume *arguendo* that (1) Plaintiff's photograph was copyrightable, (2) the upload was outside the scope of any implied license, and (3) the unauthorized use of Plaintiff's photos on Twitter is non-protectable copyright infringement. Although all three issues are certainly arguable, we refrain from doing so, as that would go beyond the focus of this brief.

likely have removed the photo from the original tweets, thus removing it in turn from the embedded versions available on Defendants' news sites.

A third option—should Plaintiff find Twitter unwilling to remove the photos in question—would be to seek a finding of secondary liability. If, for example, he could show that the DMCA safe harbors did not apply and that Twitter knew of and materially contributed to the infringing activity, then he would likely have an additional cause of action to pursue under the secondary liability doctrine.

In short, Plaintiff chose to forego several clear legal avenues designed to address this very problem. Plaintiff declined to pursue action against the direct infringers; opted not to exercise self-help through the provisions of Digital Millennium Copyright Act; and thus could not even reach the backstop provided by the doctrine of contributory liability. Instead, he chose a more complicated path that can only succeed if the Court upends ten years of established precedent that has provided crucial legal certainty to intermediaries and users alike.

CONCLUSION

For the foregoing reasons, the Court should grant Partial Summary Judgment to the Defendants.

Dated: October 19, 2017

ELECTRONIC FRONTIER FOUNDATION

By: */s/Mitchell L. Stoltz*
Mitchell L. Stoltz

ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993
Email: mitch@eff.org

Attorneys for *Amici Curiae*
Electronic Frontier Foundation and
Public Knowledge