22-2760-cv

United States Court of Appeals

for the

Second Circuit

YOUT LLC,

Plaintiff-Appellant,

– v. –

RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.,
DOE RECORD COMPANIES, 1-10,

Defendants-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF CONNECTICUT

BRIEF FOR PLAINTIFF-APPELLANT

VALENTIN GURVITS
FRANK SCARDINO
BOSTON LAW GROUP, PC
825 Beacon Street, Suite 20
Newton Centre, Massachusetts 02459
(617) 928-1800

EVAN FRAY-WITZER
CIAMPA FRAY-WITZER, LLP
20 Park Plaza, Suite 505
Boston, Massachusetts 02116
(617) 426-0000

Attorneys for Plaintiff-Appellant

CORPORATE DISCLOSURE

Plaintiff-Appellant Yout LLC does not have any parent corporations; and no publicly-held corporation owns 10% or more of the party's stock.

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases:

Statutes and Other Authorities:

INTRODUCTION

The present case calls on this Court to examine for the first time novel questions arising under certain provisions of the Digital Millennium Copyright Act, 17 U.S.C. §1201, designed to provide protections to copyright holders who have employed effective technological measures to prevent the public from accessing or copying their copyrighted works without authorization or permission, from circumvention tools designed to thwart such effective technological measures. What makes this case unique, however, is: the fact that the copyright holders here did not themselves employ *any* technological measures (relying instead on technology utilized by a third party, YouTube, which may or may not be designed to prevent copying); the works at issue are made freely available to any person in the world with a connection to the Internet and a web browser; and there are no technological measures that effectively prevent the access or copying of the works at issue – with or without the use of Plaintiff's services.

More specifically, Plaintiff Yout, LLC provides a software platform that allows Internet users to download and save to their computers audio and videos that are freely available to the public, so that the user can "time shift"/"location shift" the viewing/listening of such content. (Much like the time-shifting approved by the Supreme Court in *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984)).

YouTube does not restrict access to the videos that appear on its website and anyone with a computer and a web browser can freely access the content provided by YouTube. Indeed, by virtue of YouTube's Terms of Service, by providing its videos to YouTube, the Defendants explicitly agree that visitors to YouTube may access (though not copy) the works at issue.

Neither YouTube nor the Defendants employ any form of Digital Rights Management ("DRM") or encryption, the inclusion of which would eliminate the ability of the Yout software to allow Yout's users to make copies of the works. Indeed, not only is there a lack of protection against such copying, the process can be accomplished by anyone with a web browser without the need for Yout's services (which simply automate the manual process anyone could use to download videos).

Despite this, Defendants improperly sent anti-circumvention notices to Google with the intent that Google would "delist" Yout's software platform, rendering it undiscoverable for the majority of Internet users seeking such services, which is precisely what occurred to Yout's detriment.

Yout brought the action below seeking: (1) a declaratory judgment that its software platform was not a circumvention tool, and (2) actual damages, costs, and attorney's fees resulting from Defendants' improper anti-circumvention notice, which improperly defamed and disparaged Yout and its software platform.

Despite the preponderance of disputed issue of fact – and the clear need for discovery and expert testimony - the Court below improperly allowed Defendants' Motion to Dismiss under Rule 12(b)(6), erroneously concluding that Yout's software platform was a circumvention tool under 17 U.S.C. § 1201.

JURISDICTIONAL STATEMENT

Plaintiff-Appellant Yout LLC ("Yout"), brought the underlying action seeking declaratory relief under 17 U.S.C §1201, and alleging violations of 17 U.S.C. §512(f), business disparagement, and defamation *per se* against Defendant-Appellees Recording Industry Association of America Inc. (the "RIAA") and Doe Record Companies 1-10 (collectively, the "Defendants"). The District Court had subject matter jurisdiction over Yout, LLC's ("Yout") claims under 28 U.S.C. §§ 1331 and 1367. Defendants' Motion to Dismiss was granted in a Memorandum of Decision and Order dated September 30, 2022 (J.A. 235-80), and Judgment was entered dismissing the suit the same day. (J.A. 285) Yout timely filed its notice of appeal on October 20, 2022. (J.A. 286) This Court has jurisdiction over this appeal under 28 U.S.C. § 1291.

STATEMENT OF ISSUES PRESENTED

The Digital Millenium Copyright Act created new categories of protections for copyright holders to protect their interests under U.S. Copyright law, while at the same time attempting to maintain the balance between such protections and Congress' desire to ensure that the variety and quality of services offered on the Internet would expand.

The new protections, which appear at 17 U.S.C., §1201, are either aimed at "access control" (§1201(a)), providing protection to a copyright holder against the circumvention of effective technical measures that the copyright owner has put in place to prevent unauthorized access to the works (as well as the trafficking in services or devices that facilitate such circumvention), or "copy control," (§1201(b)) providing protection to a copyright holder against the trafficking in services or devices that circumvent effective technical measures put in place by the copyright owner to prevent the improper infringement of certain rights afforded to copyright holders under the law, including the copying of the works.

The questions presented are:

1. Whether an unencrypted and unscrambled work that the copyright owner has made freely available to any person with a connection to the Internet and a web browser, and to which the copyright owner has agreed the public may

access, can nonetheless be said to be protected by an effective technical measure that can be circumvented.

2. Whether a copyright owner can rely on a technology utilized by a third party and claim such technology as an "effective technological measure" even though the copyright owner has provided its works to the third party specifically agreeing that the third party may provide the public with access to the works.

3. Whether there is "circumvention" of a technological measure that does not actually prevent either access or copying, with or without the service provided by the Plaintiff.

4. Whether a neutral service that is analogous to a VCR and which has significant non-infringing uses can be considered a service designed primarily to circumvent technological measures that protect against the infringement of a copyright owner's rights to control access and copying, particularly where the technological measures do not actually prevent either access or copying.

5. Whether a false allegation that a service violates the provisions of §1201 in a manner analogous to secondary copyright infringement violates 17 U.S.C., §512(f).

STATEMENT OF THE CASE

I. Nature of the Case and Procedural History

On October 25, 2020, Yout filed suit in the District Court for the District of Connecticut, seeking declaratory relief with respect to 17 U.S.C. §1201, as well as damages, costs, and attorney's fees for violations of 17 U.S.C. §512(f); business disparagement; and defamation *per se*. *See* Joint Appendix ("J.A.") 10-25. On December 14, 2020, Yout filed its First Amended Complaint. *See* J.A. 2 at ECF No. 9.

On January 14, 2021, the RIAA filed a Motion to dismiss the First Amended Complaint. On August 5, 2021, the Court (**Underhill, Stefan, J.**) held a hearing on the RIAA's motion. (J.A. 71-122). At the conclusion of the hearing, Judge Underhill stated that the factual argument of both parties "kind of wandered well, well beyond the complaint in your arguments" (J.A. 114 at ln. 12-13) and dismissed the Complaint without prejudice, requiring that Yout file a more detailed amended Complaint. (J.A. 117-20). Judge Underhill issued a minute order the same day dismissing the First Amended Complaint without prejudice. (J.A. 35.)

On September 22, 2021, Yout filed its Second Amended Complaint ("SAC"). (J.A. 36-70). On October 20, 2021, the RIAA moved to dismiss the Second Amended Complaint pursuant to Fed. R. Civ. P. 12(b)(6). J.A. 7 at ECF No. 49. On August 25, 2022, the Court (Underhill, Stefan, J.) held a hearing on

the RIAA's motion. (J.A. 172-234). On September 30, 2022, the Court (Underhill, J.) issued a Memorandum of Decision and Order granting the RIAA's Motion to Dismiss (J.A. 234-80) and a Judgment in the RIAA's favor. (J.A. 285). Judge Underhill's decision is reported as: *Yout, LLC v. Recording Indus. Ass'n of Am., Inc.*, No. 3:20-CV-1602 (SRU), 2022 WL 4599203, 2022 U.S. Dist. LEXIS 178462 (D. Conn. Sept. 30, 2022).

Yout filed a timely notice of appeal on October 20, 2022. *See* J.A. 286.

II. Statement of the Facts

Because the case was dismissed below on a Motion to Dismiss pursuant to Rule 12(b)(6), the facts as alleged in the SAC must be accepted as true. In addition, because it was referenced explicitly in the SAC, the District Court took judicial notice of a letter from the Electronic Frontier Foundation ("EFF") to GitHub DMCA Agent dated November 15, 2020. *See* J.A. 58 at ¶100 n.5; J.A. 281-84). The District Court also took judicial notice of YouTube's Terms of Service. *See* J.A. 239 at n.5. Accordingly, the relevant facts are as follows.

The Internet contains diverse types of content that can be accessed by persons using web browsers (such as Google Chrome). J.A. 39 at ¶25. This lawsuit involves Internet content that can be accessed using a web browser ("Web Content") using a unique hyperlink, uniform resource locator (commonly referred

to as a "URL"), or a "web address" that directs computing devices to such content on the Internet. *Id.* at ¶26.

Some Web Content exists behind a paywall such that a person can only access the content after paying for the specific content or a broader subscription (*e.g.* iTunes). *Id.* at ¶27. This lawsuit does *not* involve Web Content behind a paywall. Rather, this lawsuit involves content publicly accessible to anyone with a web browser and an Internet connection. *Id.* at ¶28.

At times, hosts or providers of Web Content will encrypt certain content to protect it from unauthorized access. *Id.* at ¶29. This lawsuit does *not* involve any encrypted Web Content. *Id.* at ¶30. Similarly, this lawsuit does not involve any Web Content that must be descrambled or decoded to view its content. *Id.* at ¶31. Similarly, this lawsuit does not involve any Web Content that has been hidden from view by use of a cipher or other means of concealing content or meaning. *Id.* at ¶32.

Description of the Yout Platform and Function

Yout created and operates a service by which a person can enter a URL linked to publicly accessible, unencrypted Web Content in certain limited formats (typically audio or video) and create a personal copy of that content on the person's computing device. J.A. 40 at ¶34. Yout does not store or keep a copy or any part of the Web Content. *Id.* at ¶35. Yout's website, located at the domain

yout.com (the "Website"), presents a homepage with a search box into which a visitor can insert a URL in order to download the Web Content in an MP3 (audio) or MP4 (audio and visual) format. *See* J.A. 40-41 at ¶¶36-40. A visitor can use Yout to save a personal recording on their personal computer for later viewing when not connected to the Internet. *See* J.A. 41-42 at ¶¶43-45. In essence, Yout allows a user to "time shift" content. J.A. 42 at ¶46. Yout never saves or retains its visitors' time-shifted content on its own servers. *Id.* at ¶47.

No Decryption, Descrambling, or Similar Circumvention Is Necessary to Download YouTube Content

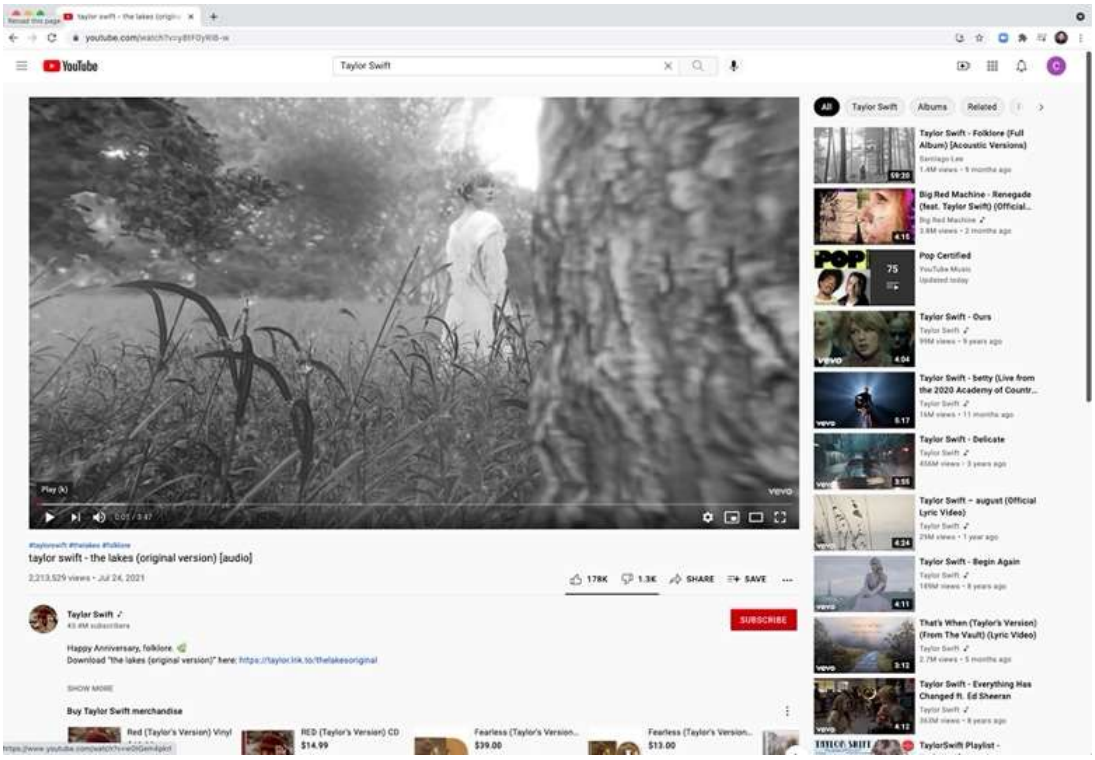
Any visitor to the Website can use Yout's services to save a local copy of publicly accessible, unencrypted Web Content. *See* J.A. 42-43 at ¶48, 55. Yout *cannot* and does not save any content protected by digital rights management ("DRM") protections or other technical protection measure utilized by copyright owners in their videos to make such content unavailable for download. J.A. 57 at ¶92. All of the Web Content on YouTube that is at issue in this case can be publicly accessed by anyone visiting YouTube.com without the use of any circumvention whatsoever. *See* J.A. 43 at ¶54.

Yout enables a visitor to the Website to interact with Web Content on YouTube in the same manner enabled by YouTube for use in popular web browsers. *Id.* at ¶56. Unlike the DRM mechanisms commonly used to encrypt and

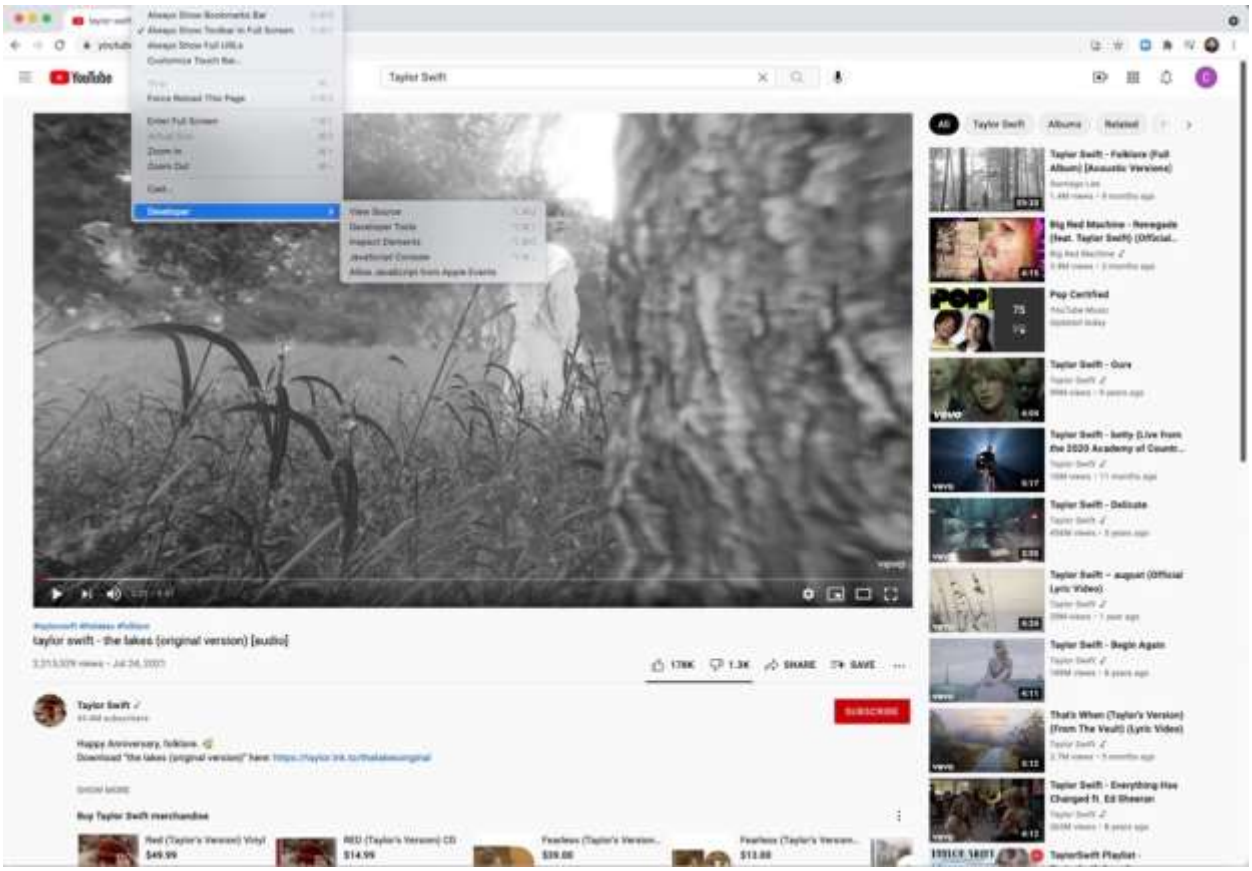
protect media such as, for example, DVD content, YouTube has no such mechanisms. *Id.* at ¶57.

If one accesses YouTube.com with the Google Chrome ("Chrome") browser, one can search for, view, and download any number of publicly accessible videos even without the use of the Yout Website by utilizing the "developer tools" that are easily accessed in the Chrome browser. J.A. 44 at ¶62, *see also*, J.A. 45-51, at ¶¶64-74. This can be done with the Chrome browser, **without** the use of the Yout Website, in the following manner:

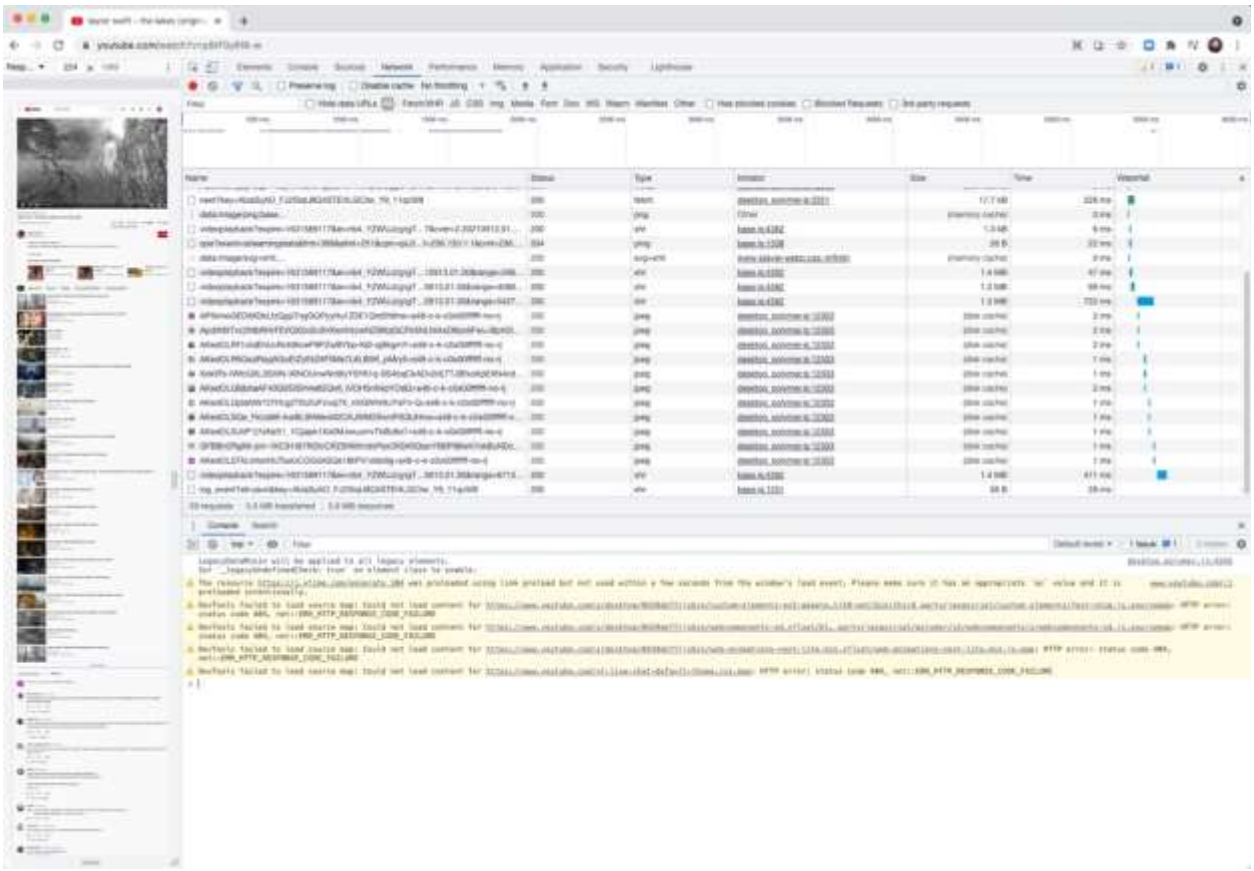
If one were to view the Taylor Swift music video, "The Lakes (Original Version)," on YouTube, the music video can be viewed at a specific URL on YouTube:



J.A. 45 at ¶64. After arriving at the above referenced URL, one can then select "View" from the Chrome menu bar on a MacOS system, and under the drop down for "Developer" select "Developer Tools" from the sub-menu, a screenshot of this follows:

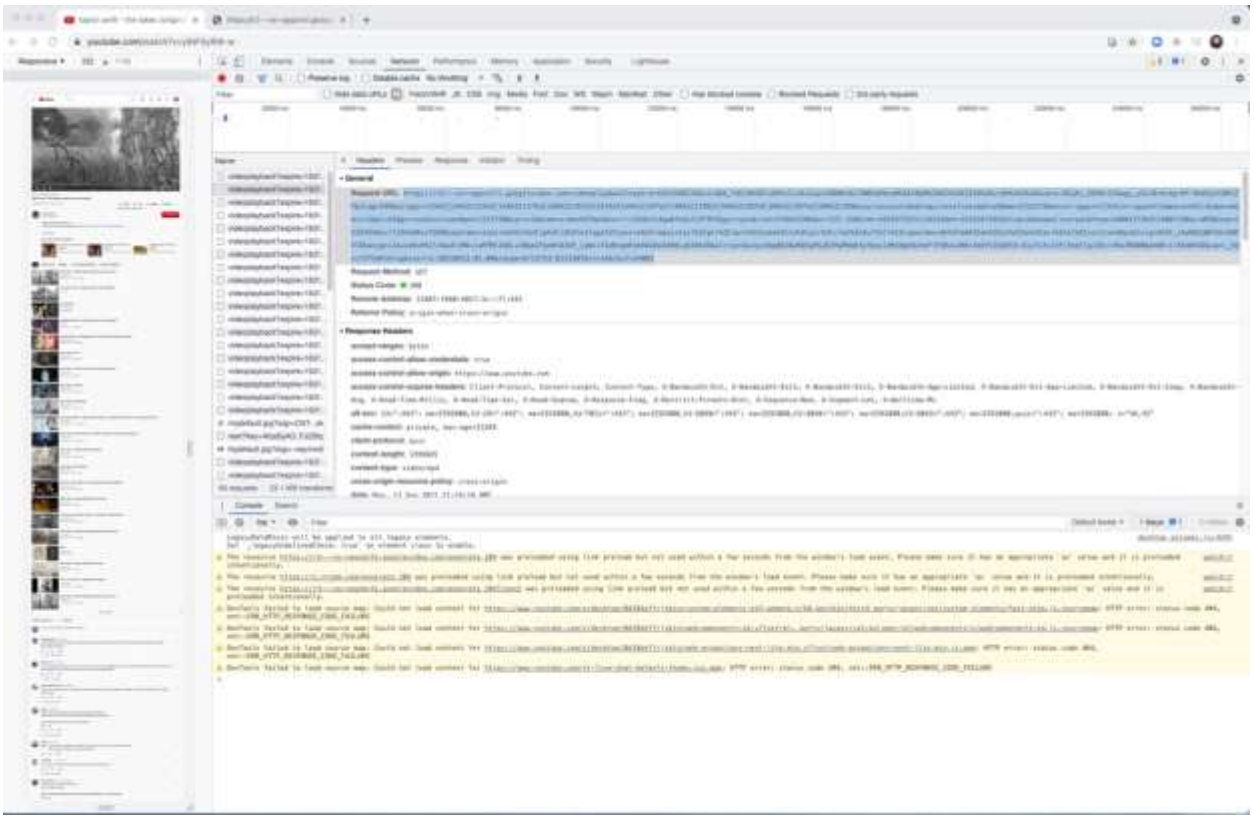


See id. at ¶65. After selecting "Developer Tools", several new frames open up within the browser window which is reflected below:



See J.A. 46 at ¶66.

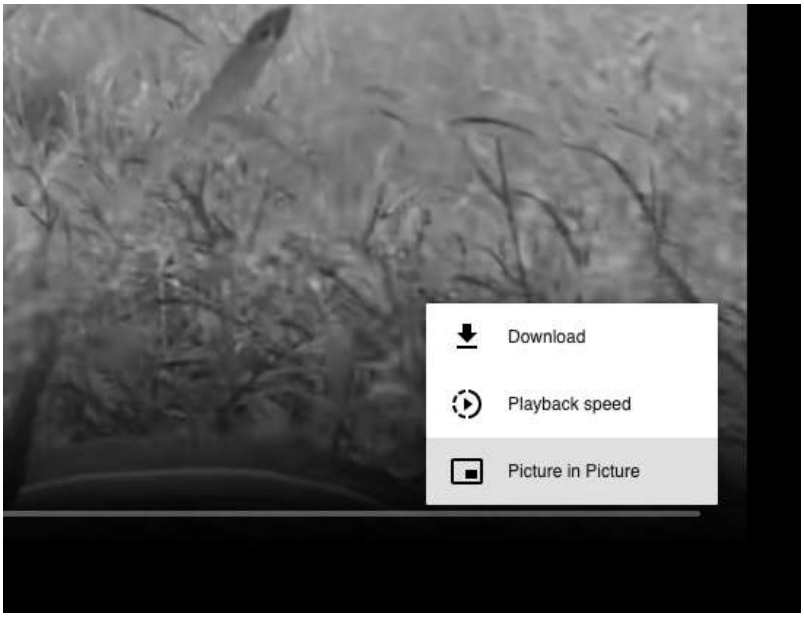
The files listed in the above window can be sorted by file size in the "Size" column by clicking the top of that column. *See id.* at ¶67. Once the files are sorted, one can highlight the first of the largest files and copy the text following the prefix "Request URL" as shown below:



See J.A. 47 at ¶48. One can then paste the text copied next to the "Request URL" prefix into a new Chrome window or tab; toward the end of the "Request URL" text exists a sequence of numbers following the text "range=" that can be modified to begin at 0 and end at a much larger number, a screenshot showing this is as follows:

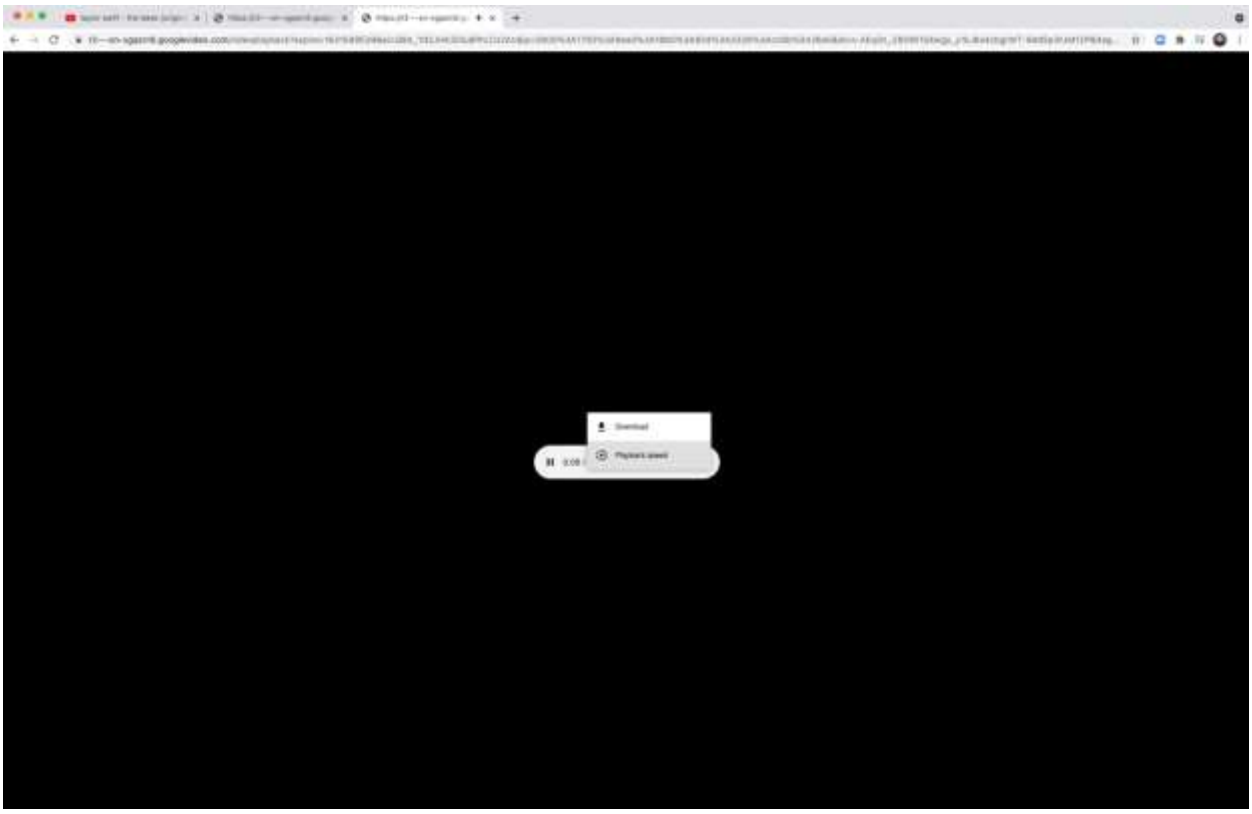
See J.A. 48 at ¶69. When one then clicks "return" or "enter" on their computer to access the "Request URL" text, a full-size video (without sound) appears within the Chrome window and begins to play. A screenshot of this video is as follows:

J.A. 49 at ¶70. On this video shown above, YouTube provides a menu to the right of the play bar identified by three vertical dots that includes a "Download" option. A screenshot reflecting this is as follows:

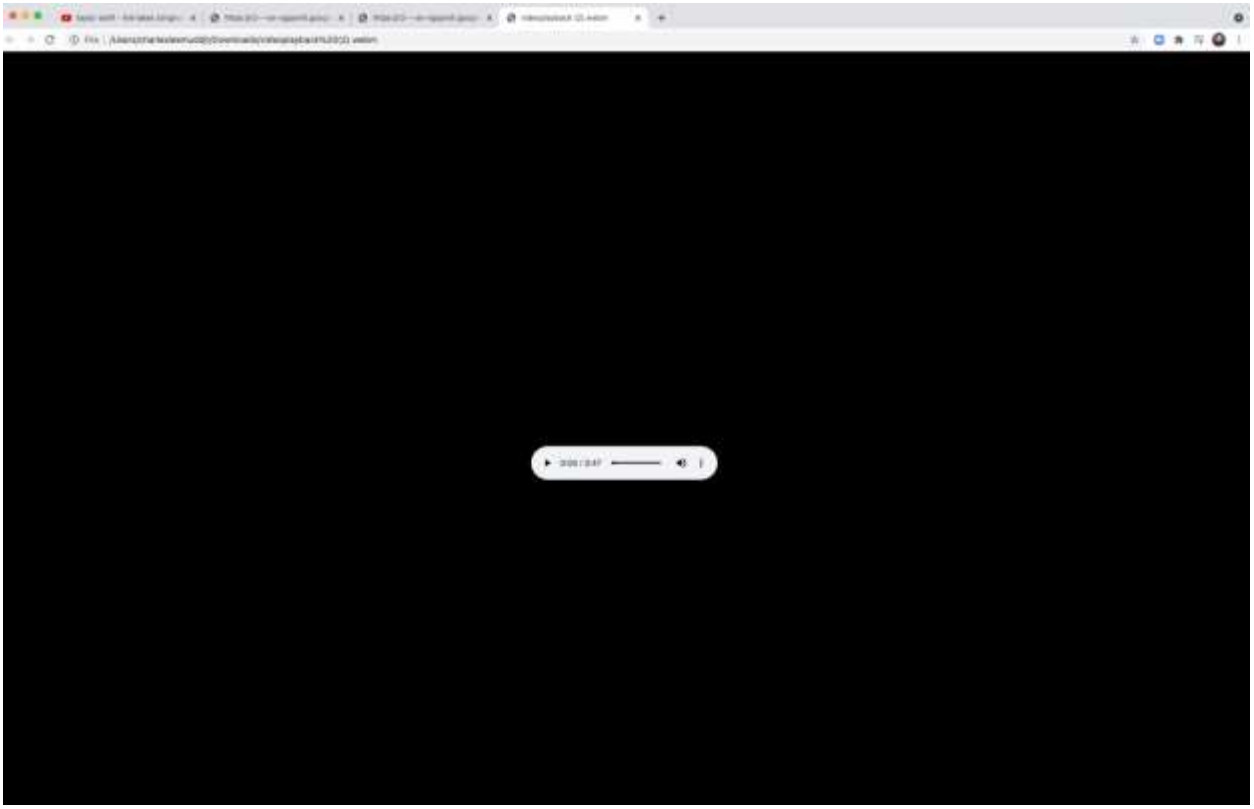


J.A. 50 at ¶71. By clicking "Download," YouTube – through the Chrome browser – then downloads a file entitled "videoplayback.mp4" that, when opened, plays the full music video (albeit without sound). *Id.* at ¶72.

The audio of YouTube music videos can also be downloaded in a similar fashion to the video of a music video. *See* J.A. 51 at ¶73. This can be done by returning to the Developer Tools provided by Chrome and searching the large files until the length of the Request URL changes to a shorter URL. *Id.* Following this, the process described above can be repeated which results in Chrome delivering the audio file that can, again, be downloaded, a screenshot reflecting this is as follows:



Id. When one selects "Download" as displayed in the above screenshot, the audio opens in a new browser tab and downloads the file to the local computer, the name of the file on the local computer reflects in the URL window, a screenshot of which is below:



J.A. 52 at ¶74.

Many websites provide detailed instructions on how to obtain the audio and video files in the fashion described above. *See id.* at ¶75. For instance, an article in Business Insider entitled "2 easy ways to download YouTube videos onto a computer to watch or share anytime" walks the reader through the exact process

described above. https://www.businessinsider.com/how-to-download-youtube-videos. *Id.* at ¶76.

Additionally, websites such as hongkiat.com gives detailed instructions for downloading content from YouTube using both Chrome and the Firefox browser at https://www.hongkiat.com/blog/download-youtube-media-without-tools/. JA-53 at ¶77.

The instructions provided there appear as follows:

How to Download Youtube Media

1. Open **Developer Tools** in the browser and go to **Network** tool, or if you're on Firefox press `Ctrl` + `Shift` + `Q`.

2. Click **Media** in the **Network** tool so that you'll see only the HTTP requests made to media files, like audio and video files.

3. Browse to a YouTube video you want to download. You'll start seeing the requests made by the YouTube page to the audio & video files in the **Network** tool.

4. Hover the cursor over the **Type** column of each request in the tool and look at the media type:

- If you want the audio, look for "audio/mp4".
- If you want the video, then look for "video/mp4".

Note: If you're using a browser that doesn't segeregate requests (like IE) or doesn't list the requests made to the audio & video files in YouTube under "Media" (like Chrome), just search the term "audio" or "video" in the search bar in the **Network** tool.

5. Once you found a request with the wanted media type (it'll be of the googlevideo.com domain), click on it, and copy the full URL from where it appears.

6. Paste the URL in the address bar, remove the `range` parameter in the query string and press `Enter`.

7. The video or audio will open, right-click on the page and select "Save As" to save the file.

8. If you want both the video and the audio, look for both with the steps above and **put them together** using any default media editor you have in your computer. It's actually pretty easy and quick to do so (even with programs like the outmoded Windows Movie Maker).

Id.

The final step listed in these instructions informs the reader how to combine the video file and the audio file together into one file: "If you want both the video and the audio, look for both with the steps above and put them together using any default media editor you have in your computer. It's actually pretty easy and quick to do so…. *Id.*

Likewise, a simple Google search produces countless videos showing how to accomplish this same task using Chrome and other common web browsers. J.A. 53-54 at ¶78. A more technical explanation of this process (which Yout automates) is contained in a letter from the Electronic Frontier Foundation (the "EFF's Letter) to GitHub DMCA Agent dated November 15, 2020. *See* J.A. 58 at ¶100 n.5, J.A. 281-84. The EFF's letter also contains an explanation as to how this process is accomplished without the use of any circumvention whatsoever. *Id.*

Yout's Actual Service v. the RIAA's Accusations

Yout's software platform enables a person to complete the process described above, but in fewer steps. J.A. 55 at ¶79. Many content creators use Yout's service to record their own original videos. *Id.* at ¶80. Further, many content creators encourage their audience and fans to use Yout to record and play back their original content. *Id.* at ¶81. In fact, the sound recordings the RIAA alludes to (it does not name any specific sound recordings) via its anti-circumvention notices

detailed below, represent a very small percentage of the available media on YouTube. *Id.* at ¶82.

On October 25, 2019, RIAA, on behalf of Doe Record Companies 1-10, sent an anti-circumvention notice under 17 U.S.C. § 512(c)(3) to Google with the intention of causing Google to delist Yout's software platform, rendering it undiscoverable for many Internet users. *Id.* at ¶83.

The October 25, 2019 notice reads as follows:

> To our knowledge, the URLs provide access to a service (and/or software) that circumvents YouTube's rolling cipher, a technical protection measure, that protects our members' works on YouTube from unauthorized copying/downloading.
>
> circumvention content: The services provided at the URLs indicated circumvent YouTube's technological protection measures.
>
> circumvention mechanism: To our knowledge, the URLs provide access to a service (and/or software) that circumvents YouTube's rolling cipher, a technical protection measure, that protects our members' works on YouTube from unauthorized copying/downloading.

Id. at ¶84; J.A. 26-27.

The RIAA, on behalf of Doe Record Companies 1-10, sent additional similar DMCA notices to Google. J.A. 55-56 at ¶85; J.A. 56 at ¶86; J.A. 28-29; J.A. 56 at ¶87.

The DMCA notices sent to Google by the RIAA on behalf of all Defendants (the "Notices") allege violations of 17 U.S.C. § 1201(a) which prohibits

circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work. J.A. 56 at ¶89.

Any DRM or other technical protection measure utilized by a copyright owner in their videos renders the video unavailable to download via Yout. J.A. 57 at ¶92. Contrary to Defendants' allegations, Yout's software platform is not designed to descramble, decrypt, avoid, bypass, remove, deactivate, or impair any technical protection measure or any technological measure that effectively controls access to a work protected by the Copyright Act. *Id.* at ¶93. In fact, any digital mechanism in place designed as anti-circumvention technology stops Yout users from recording and saving that protected work, thereby demonstrating Yout's compliance with any anti-circumvention protections that might exist. *Id.* at ¶94.

Yout's software platform contains no password, key, or other secret knowledge that is required to access YouTube videos. J.A. 58 at ¶99 Yout does not "circumvent" anything as that term is defined in 17 U.S.C. § 1201 because YouTube provides the means of accessing these video streams to anyone who requests them. *Id.* at ¶100.

Moreover, the Defendants have ***explicitly agreed that Youtube's visitors were permitted access to the copyrighted works*** by virtue of having agreed to YouTube's Terms of Service, of which the District Court took judicial notice:

> Rights you Grant
>
> You retain ownership rights in your Content. However, we do require you to grant certain rights to YouTube and other users of the Service, as described below.
>
> License to Other Users
>
> You also grant each other user of the Service a worldwide, non-exclusive, royalty-free license to access your Content through the Service, and to use that Content, including to reproduce, distribute, prepare derivative works, display, and perform it, only as enabled by a feature of the Service (such as video playback or embeds). For clarity, this license does not grant any rights or permissions for a user to make use of your Content independent of the Service.

J.A. 130.

Yout's software platform is not primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a copyrighted work, or that protects the right of a copyright owner. J.A. 60 at ¶117. Yout's software platform has commercially significant purposes and uses other than to circumvent a technological measure that effectively controls access to a copyrighted work or that protects the right of a copyright owner. *Id.* at ¶120. Yout's software platform has not been marketed for use in circumventing a technological measure that effectively controls access to a copyrighted work, or that protects the right of a copyright owner. *Id.* at ¶122.

The Defendants knew when they sent their DMCA Notices that Yout's software platform does not circumvent digital copyright mechanisms under the law

and does not infringe the Defendants' rights —via secondary copyright infringement or otherwise—but chose to send the Defendants' DMCA Notices anyway. *Id.* at ¶139.

Damage to Yout's Public Image and Reputation

The Defendants' DMCA Notices have falsely caused third parties to believe Yout engaged and continues to engage in illegal and unlawful conduct. *Id.* at ¶¶108-09. Defendants' DMCA Notices have caused Yout's customers to cancel subscriptions. *Id.* at ¶110. On information and belief, Defendants' DMCA Notices have caused PayPal to shut down Yout's account, causing Yout further significant monetary and reputational damage. *Id.* at ¶111.

SUMMARY OF THE ARGUMENT

I. Yout was required only to show that its complaint contains sufficient factual matter, accepted as true, to state a claim for relief that is plausible on its face, accepting all facts as alleged as true. This Court's review of the allowance of a motion to dismiss is *de novo.*

II. The DMCA created new protections for copyright holders which target both the circumvention of technological protection measures and the trafficking in devices or services that facilitate such circumvention.

III. The District Court incorrectly concluded that Yout violates the "access control" prohibitions of §1201(a).

A. The District Court improperly assumed the existence of a "technical measure," a disputed issue of fact.

B. Yout cannot violate §1201(a)(1), which prohibits direct circumvention of a technological measure designed to limit access to a work as Yout does not itself choose which videos to access nor does it directly access such videos (as opposed to providing a means to do so).

C. Yout did not circumvent any access control in violation of §1201(a) both because YouTube does not restrict access to the relevant videos and because the Defendants have explicitly

authorized access of their works.

D. The District Court Adopted a Definition of "Access" That Obliterates the distinction between access controls and copy controls, in contravention of the statute, the case law, the legislative history, and the commentary.

E. Yout does not violate either of the anti-trafficking provisions of the DMCA (§1201(a)(2) and §1201(b) and the District Court's claim, in a footnote, that Yout waived its arguments under §1201(b) is clearly erroneous.

F. Yout has plausibly alleged that its service was not primarily designed to circumvent protections afforded to a copyright owner.

G. Yout has plausibly alleged both that it has significant commercial purposes and uses other than the circumvention of protections afforded to a copyright owner and that it does not market itself as a tool for circumvention. And, in any event, each of these are questions of fact which could not have been properly resolved on a Rule 12(b)(6) motion.

IV. The allegations of the SAC plausibly allege a violation of §512(f) inasmuch as they allege that the RIAA notices knowingly misrepresented that Yout engaged in conduct tantamount to secondary copyright infringement.

V. Because Yout demonstrated that the RIAA's Notices contained false statements of fact that disparaged Yout, the District Court's dismissal of Yout's claims for business disparagement and defamation *per se* must be reversed.

ARGUMENT

I. Rule 12(b)(6) and the Standard of Review

This Court reviews "a district court's dismissal of a complaint pursuant to Rule 12(b)(6) *de novo*, accepting all factual allegations in the complaint and drawing all reasonable inferences in the plaintiff's favor." *Lea v. TAL Educ. Grp.*, 837 F. App'x 20, 22 (2nd Cir. 2020)(citations omitted).

Despite the Supreme Court's reworking of the 12(b)(6) standards in *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544 (2007) and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), to successfully oppose a motion to dismiss, a plaintiff is required only to show that the complaint contains "sufficient factual matter, accepted as true, to state a claim for relief that is plausible on its face." *Id*. at 678.

As this Court has held, "to keep the plausibility standard in perspective, we do well to keep in mind that just two weeks after deciding *Twombly*, the Supreme Court, reversing a Rule 12(b)(6) dismissal of a complaint, stated, 'Federal Rule of

Civil Procedure 8(a)(2) requires only a short and plain statement of the claim showing that the pleader is entitled to relief. Specific facts are not necessary; the statement need only give the defendant fair notice of what the claim is and the grounds upon which it rests.'" *Adia v. Grandeur Mgmt.*, 933 F.3d 89, 92 (2nd Cir. 2019), *quoting Erickson v. Pardus*, 551 U.S. 89, 93 (2007). "[T]o stave off threshold dismissal for want of an adequate statement of their claim, plaintiffs are required to do no more than state simply, concisely, and directly events that, they allege entitle them to damages." *Quinones v. City of Binghamton*, 997 F.3d 461, 468 (2nd Cir. 2021)(internal citations and quotation marks omitted).

"However unlikely it may appear to a court from a plaintiff's complaint that he will ultimately be able to prove an alleged fact such as mental state, the court may not go beyond FRCP 8(a)(2) to require the plaintiff to supplement his pleadings with additional facts that support his allegation of knowledge either directly or by inference. Whether the plaintiff can produce evidence to create a genuine issue with regard to his allegation is to be resolved through a motion for summary judgment." *Phelps v. Kapnolas*, 308 F.3d 180, 186-87 (2nd Cir. 2002).

II. The Relevant DMCA Provisions

The DMCA was enacted in 1998, *inter alia*, to implement the World Intellectual Property Organization Copyright Treaty, which required member nations to provide for legal remedies against the "circumvention of effective

technological measures that are used by authors in connection with the exercise of their rights… in respect of their works, which are not authorized by the authors concerned or permitted by law." *Universal City Studios v. Corley*, 273 F.3d 429, 440 (2d Cir. 2001).

In the 25 years since its enactment, this Court has only once had occasion to speak in detail as to the DMCA provisions at issue in the present case and, even then, the Court was only presented with some of the issues raised in this appeal.[1] *See, Corley, supra*.

In *Corley*, this Court outlined the three different provisions of the DMCA primarily at issue here:

> The Act contains three provisions targeted at the circumvention of technological protections. The first is subsection 1201(a)(1)(A), the anti-circumvention provision. This provision prohibits a person from "circumventing a technological measure that effectively controls access to a work protected under [Title 17, governing copyright]."
>
> …The second and third provisions are subsections 1201(a)(2) and 1201(b)(1), the "anti-trafficking provisions." Subsection 1201(a)(2), the provision at issue in this case, provides: No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

[1] *Corley*, in large part, focused on First Amendment arguments not at issue here.

> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title. Id. § 1201(a)(2).
>
> To "circumvent a technological measure" is defined, in pertinent part, as "to descramble a scrambled work . . . or otherwise to . . . bypass . . . a technological measure, without the authority of the copyright owner." Id. § 1201(a)(3)(A).
>
> Subsection 1201(b)(1) is similar to subsection 1201(a)(2), except that subsection 1201(a)(2) covers those who traffic in technology that can circumvent "a technological measure that effectively controls access to a work protected under" Title 17, whereas subsection 1201(b)(1) covers those who traffic in technology that can circumvent "protection afforded by a technological measure that effectively protects a right of a copyright owner under" Title 17. Id. § 1201(a)(2), (b)(1) (emphases added). In other words, although both subsections prohibit trafficking in a circumvention technology, the focus of subsection 1201(a)(2) is circumvention of technologies designed to prevent access to a work, and the focus of subsection 1201(b)(1) is circumvention of technologies designed to permit access to a work but prevent copying of the work or some other act that infringes a copyright. See S. Rep. No. 105-190, at 11-12 (1998). Subsection 1201(a)(1) differs from both of these anti-trafficking subsections in that it targets the use of a circumvention technology, not the trafficking in such a technology.

Corley at 440-41.

In addition to the distinctions between the DMCA's anti-circumvention provision (§1201(a)(1)) and its anti-trafficking provisions (§1201(a)(2) and §1201(b)), the two other relevant provisions are also sometimes referred to as the access control provisions (§1201(a)) and the copy control provisions (§1201(b)).

As might be expected, the access control provisions (both anti-circumvention and anti-trafficking) are directed at the protection of technological measures put in place by the copyright holder that prevent *access* to the copyrighted works. *See, e.g.*, 4 Nimmer §12A.03[A][1][a] at 12A-20 ("The key word here is 'access.' The statute bars one whom technology 'locks out' of a copyrighted work from 'breaking into it;'") and 4 Nimmer §12A.03[D][1] at 12A-30 (discussing the House Committee report and its comments on §§1201(a)(1) and §1201(a)(2)(the "access control provisions") that those sections "pertain 'where a person has not obtained authorized access to a copy or a phonorecord of a work for which the copyright owner has put in place a technological measure that effectively controls access to his or her work. In a more colloquial form: 'The act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work is the electronic equivalent of breaking into a locked room to obtain a copy of a book. The basic provision,[2] under this typology, is equivalent to breaking into a castle – the invasion of another's property is itself the offense.")

[2] Nimmer refers to the anti-circumvention provision of §1201(a)(1) as the "basic provision"; the anti-trafficking provision of §1201(a)(2) – which is also concerned with access control – as the "trafficking ban"; and the anti-trafficking provision of §1201(b) – which is concerned with copy control – as the "additional violations."

In contrast with the basic provision, the "trafficking ban" (*i.e.*, §1201(a)(2)) "targets not those who break into another's domain, but instead those who facilitate the process – say those who market siege engines or catapults, come up with ingenious infiltration strategies, and generally facilitate penetration of the stronghold." *Id.* at 12A-31. Finally, Nimmer discusses the additional provisions, the "copy-control" provisions, analogizing them to "disorderly conduct": "In contrast to invading the sanctity of another's castle through the basic violation, if a guest invited inside the manor contravenes the seigneur's edicts, then the trespass at hand differs qualitatively from breaking and entering. …the statute's additional violations come into play here. They ban 'circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner.'" *Id.*

III. Although the District Court Recognized the Distinction Between The "Access Control" Provisions of §1201(a) and The "Copy Control" Provisions of §1201(b), It Proceeded to Apply The Wrong Analysis In Addressing the §1201(a) Issue.

The District Court below clearly recognized the difference between the DMCA's access control and copy control provisions. J.A. 245("Whereas subsection 1201(a) focuses on technological measures that 'control access' to a copyrighted work, subsection 1201(b) focuses on technological measures that 'protect[]' or control 'a right of a copyright owner.' Because a copyright owner's rights include an exclusive right to reproduce a copyrighted work and to distribute

copies by sale or otherwise, 17 U.S.C. § 106, subsection 1201(b) is often deemed the 'copy-control" provision.'").

Having properly articulated this distinction, however, the District Court nonetheless proceeded to analyze the RIAA's arguments almost exclusively under §1201(a), holding that Yout violates the access control provisions of the statute, even though it is inconceivable for any number of reasons that Yout does so. As discussed below, the District Court's conclusion that Yout violates the access control prohibitions of the DMCA (or, really, that Yout failed to properly plead that it does *not* violate those provisions) is clearly wrong and, as such, the District Court's dismissal of Yout's SAC must be reversed.

A. Whether There Is Even A "Technological Measure" Is A Disputed Question of Fact Not Susceptible to Resolution On A Rule 12(b)(6) Motion.

Before turning to the arguments that are specific to any *one* of the three relevant DMCA provisions, there is one overriding issue that should have prevented the District Court from finding in the RIAA's favor, regardless of which provision the District Court was considering. Each of the three relevant provisions requires – as a threshold matter – the existence of a "technological measure" protecting *something*, whether that something is the ability to *access* a copyrighted work or the *protections* afforded to that work under U.S. Copyright law. The

RIAA and the District Court have both assumed the existence of such a "technological measure" (a factual question) without any valid basis to do so.

There is little question that there is some bit of "technology" – a small bit of Javascript code – at play here. When an individual visits the YouTube website to watch a video, YouTube's servers send the user's computer the Javascript code which calculates a signature value that the user's computer sends back to YouTube to initiate the playback of the requested video. That code is the "technology." There is no evidence, however, that YouTube intended this to be a "technological measure" designed to limit access or copying at all. And, if the technology was not designed or intended to limit or accessing copying, the Defendants cannot claim retroactively that such a technological measure exists by happenstance.

And, while it is true that it may not be an unreasonable *assumption* that YouTube intended this technology to be a "technological measure," such an assumption is precisely the type of disputed fact that must be tested via factual discovery. YouTube is not a party here and the Defendants can no better speak to YouTube's intentions than Yout can.

One could easily imagine the RIAA responding that (in its view) the *only* reasonable inference that the Court can draw is that the Javascript code is intended to protect the content creator's right to limit access or copying, but that is not necessarily the case. It is equally plausible that the Javascript code has nothing to

do with any interest the copyright holder might enjoy and everything to do with YouTube's own interests. For example, YouTube compensates content creators who share their content on YouTube based on the popularity of the videos the content creators post. It is certainly plausible that the Javascript code is designed to ensure that a content creator is not using an automated system to make it *appear* as if a human is accessing a video when in reality the request is coming from a bot farm designed to increase the compensation paid to the content creator. Under that circumstance, the Javascript code would have nothing to do with protection of any rights afforded to the copyright holder.

This is not to say, of course, that this is actually why YouTube utilizes the Javascript code. Yout has no way of knowing – at this stage of the proceedings – the intended purpose of this bit of technology or why YouTube deploys it. By the same token, neither do the Defendants, and that is precisely why the issue is not amenable to Rule 12(b)(6) motion.

In any event, because the SAC plausibly alleges that Yout does not circumvent (or provide technology to circumvent) a "technological measure" (*see, e.g.*, J.A. 57-58 at ¶¶92-101) and because the existence of such a "technological measure" is a factual question requiring resolution through discovery, the District Court's dismissal of Yout's complaint at this early stage must be reversed.

B. Yout Did Not Violate §1201(a)(1), As That Section Is Inapplicable To Yout.

As noted above, §1201(a)(1) states that "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." Unlike §1201(a)(2), §1201(a)(1) deals only with those persons alleged to have *directly* circumvented a technical measure, not those persons alleged to have *provided* a *service* that allows another to circumvent a technological measure. *See, e.g., Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294, 319 (S.D.N.Y. 2000)("As noted, Section 1201(a) of the DMCA contains two distinct prohibitions. Section 1201(a)(1), the so-called basic provision, 'aims against those who engage in unauthorized circumvention of technological measures . . . . [It] focuses directly on wrongful conduct, rather than on those who facilitate wrongful conduct'").

In the present case, the District Court perplexingly couched the vast majority of its opinion in terms of a purported analysis under §1201(a)(1), even though it clear from the SAC (and the Parties' arguments below) that the RIAA had alleged in its takedown notices to Google that Yout provided access to a *service* that the website's *users* could allegedly use to circumvent technological measures.[3] J.A. 26-32, J.A. 55-56 at ¶¶83-89. This is a clear error of law.

[3] There is no allegation that Yout selected which videos its users should access. To the contrary, as the SAC makes clear, visitors to the Yout website instruct the website's software which video the user wishes to access. J.A. 40-42at ¶¶34-39, 43-47.

Specifically, the RIAA, in its takedown notices to Google, did not allege that Yout itself *directly* circumvented YouTube's technological measures, but rather the RIAA alleged that the Yout website provides:

> access to a service (and/or software) that circumvents YouTube's rolling cipher, a technical protection measure, that protects our members' works on YouTube from unauthorized copying/downloading.
>
> circumvention content: The services provided at the URLs indicated circumvent YouTube's technological protection measures.
>
> circumvention mechanism: To our knowledge, the URLs provide access to a service (and/or software) that circumvents YouTube's rolling cipher, a technical protection measure, that protects our members' works on YouTube from unauthorized copying/downloading.

Id.

As such, even if the Yout website provided a service that allowed visitors to the website to circumvent a technological measure that effectively controlled access to copyrighted works (which it most assuredly does not), Section 1201(a)(1) would still be inapplicable because Yout provides access to a service and does not itself "access" the works, regardless of whether such access could be considered to be circumvention or not. *See, e.g., Universal City Studios v. Corley*, 273 F.3d 429, 440 (2d Cir. 2001)("Subsection 1201(a)(1) differs from both of these anti-trafficking subsections in that it targets the use of a circumvention technology, not the trafficking in such a technology"); *DISH Network L.L.C. v. World Cable Inc.*, 893 F. Supp. 2d 452, 464 (E.D.N.Y. 2012)("Section 1201(a)(1)(A), the anti-

circumvention provision, 'aims against those who engage in unauthorized circumvention of technological measures. . . . [It] focuses directly on wrongful conduct, rather than on those who facilitate wrongful conduct. . . . Thus, contrary to the Plaintiffs' argument in opposition to the motion to dismiss, the Defendants cannot be liable under § 1201(a)(1)(A) for the alleged circumvention by the World Cable subscribers"); *Autodesk, Inc. v. Flores*, 2011 U.S. Dist. LEXIS 11687, at *9 n.2 (N.D. Cal. Jan. 31, 2011)("The FAC is focused on allegations that Defendants sold or trafficked in circumvention technology and does not allege that they actually used the technology themselves. Thus, Autodesk does not appear to have pled a claim under § 1201(a)(1)(A)"); *Universal City Studios v. Reimerdes*, 111 F. Supp. 2d 294, 316 (S.D.N.Y. 2000)("As defendants are accused here only of posting and linking to other sites posting DeCSS, and not of using it themselves to bypass plaintiffs' access controls, it is principally the second of the anticircumvention provisions that is at issue in this case").

And, while this error of law is not – in and of itself – dispositive of the RIAA's motion to dismiss, the Court's improper focus on §1201(a)(1) nonetheless had important implications for its decision. Sections 1201(a)(2) and 1201(b), each of which address the offering of a *service* that facilitates circumvention of one type or another, have additional requirements not present in §1201(a)(1) – requirements which the District Court gave short shrift to – apparently under the mistaken belief

that it was addressing allegations under §1201(a). Ultimately, however, the District Court erred in finding, as a matter of law, that Yout violated any of the anti-circumvention provisions of the DMCA.

C. Yout Could Not Have Violated the Access Control Provisions of §1201(a) For the Simple Reason That YouTube Does Not Restrict Access To The Videos Available On Its Website.

Next, although there may be some disagreement with respect to the application of certain aspects of the anti-circumvention provisions of the DMCA, there is one area in which the courts (including this Court) and commentators are unanimous: Section 1201(a) concerns itself *exclusively* with the question of *access* to copyrighted materials and not what happens to those materials once they are accessed. *Universal City Studios v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001)("the DMCA targets the circumvention of digital walls guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the use of those materials after circumvention has occurred"); *MGE UPS Sys. v. GE Consumer & Indus. Inc.*, 622 F.3d 361, 366 (5th Cir. 2010)("Because § 1201(a)(1) is targeted at circumvention, it does not apply to the use of copyrighted works after the technological measure has been circumvented"); *United States v. Reichert*, 747 F.3d 445, 448 (6th Cir. 2014)("the DMCA 'targets the circumvention of digital walls guarding copyrighted material (and trafficking in circumvention tools),' even though it 'does not concern itself with the use of those materials after

circumvention has occurred'"); *Point 4 Data Corp. v. Tri-State Surgical Supply & Equip., Ltd.*, 2012 U.S. Dist. LEXIS 113997, at *5 (E.D.N.Y. Aug. 13, 2012)("The Second Circuit has squarely stated that 'the DMCA *does not concern itself* with the use of [protected] materials after circumvention has occurred,'")(citing *Corley*)(emphasis in original); *DISH Network L.L.C. v. World Cable Inc.*, 893 F. Supp. 2d 452, 465 (E.D.N.Y. 2012)("the Second Circuit has clearly held that 'the DMCA does not concern itself with the use of [protected] materials after circumvention has occurred'")(citing *Corley*); *Hattler v. Ashton*, 2017 U.S. Dist. LEXIS 236278 (C.D. Cal. Apr. 20, 2017)(where the "statutory structure, appellate precedent, and legislative history" all compel a conclusion that §1201(a)'s references to a "technological measure that control 'access' to a protected work, that section should be interpreted narrowly to exclude technologies that permit access to copyrighted work, but restrict copying. …Plaintiff cannot state a claim for relief under §1201(a)(1). Further, because it is uncontested that the Works are accessible to the public on many websites, any effort to amend the SAC would be futile.'").

The DMCA's legislative history also says as much: "Paragraph (a)(1) does not apply to the subsequent actions of a person once he or she has obtained authorized access to a copy of a work protected under Title 17, even if such actions

involve circumvention of additional forms of technological protection measures." H.R. Rep. No. 105-551, pt. 1, at 18; S. Rep. No. 105-190, at 28.

And, as Professor Nimmer has explained, "the basic provision of Section 1201 provides that 'no person shall circumvent a technological measure that effectively controls access to a work protected' by United States copyright. The key word here is 'access.' The statute bars one whom technology 'locks out' of a copyrighted work from 'breaking into' it." 4 Nimmer, §12.A.03[A][1][a] at 12A-19 to 12A-20. A Section 1201(a)(1) violation, which Professor Nimmer terms the "basic provision," is the "equivalent to breaking into a castle – the invasion of another's property is itself the offense." Nimmer, §12.A.03[D][1] at 12A-30 to 12A-31.

In the present case, there is no question but that the works at issue are freely available. Anyone with a computer and a web browser can go to youtube.com and *access* the works. Indeed, it is clear from YouTube's Terms of Service – which the District Court took judicial notice of – that, by providing their videos to Youtube – ***the Defendants explicitly agreed that Youtube's visitors were permitted access to the works***:

> Rights you Grant
>
> You retain ownership rights in your Content. However, we do require you to grant certain rights to YouTube and other users of the Service, as described below.

> License to Other Users
>
> You also grant each other user of the Service a worldwide, non-exclusive, royalty-free license to access your Content through the Service, and to use that Content, including to reproduce, distribute, prepare derivative works, display, and perform it, only as enabled by a feature of the Service (such as video playback or embeds). For clarity, this license does not grant any rights or permissions for a user to make use of your Content independent of the Service.

J.A. 130.

This explicit grant of access permission by the content provider is fatal to the RIAA's arguments under §1201(a). Section 1201(a)(3) defines the term "circumvent a technological measure" to mean "to descramble a scrambled work, to decrypt an encrypted work, or otherwise avoid, bypass, remove, deactivate, or impair a technological measure without the authority of the copyright owner." 17 U.S.C. §1201(a)(3)(A). The RIAA's arguments fail each part of this definition.

First, Yout has plausibly alleged in the SAC that its software does none of the things defined as "circumvention" in this section: there is nothing to descramble or decrypt and – far from avoiding, bypassing, removing, deactivating, or impairing any technology employed by YouTube – Yout simply engages with YouTube's technology (at least with respect to accessing the copyrighted works) in precisely the manner that YouTube intends the public to engage. YouTube's server generates a small bit of Javascript code that it intends the receiving computer to run in order to access the file being provided by YouTube. YouTube

provides this to ***anyone*** desiring such access. There is no "circumvention" at all; merely the use of YouTube's technology in precisely the way YouTube intends. And, as YouTube's Terms of Service make clear, all of this is done with the explicit consent of the content providers.

The SAC explicitly alleges that it does not circumvent YouTube's technology, citing to a letter from the Electronic Frontier Foundation (the "EFF"). J.A. 58 at n.5. Because the letter was key to Yout's assertions in the SAC, the District Court took judicial notice of the EFF's letter. As the EFF explained, "youtube-dl simply uses the 'signature' code provided by YouTube in the same manner as any browser, rather than bypassing or avoiding it…." J.A. 283.

Nevertheless, the RIAA contends that Yout's service circumvents a technological measure – despite the fact that Yout simply uses the process that YouTube makes available to anyone who wants it – because (the RIAA alleges), Yout's service is ultimately intended to use the accessed works in an unintended manner. This argument has repeatedly been rejected by the courts. *See, e.g., DISH Network L.L.C. v. World Cable Inc.*, 893 F. Supp. 2d 452, 465 (E.D.N.Y. 2012)("even assuming that the use of deception to obtain the EchoStar receivers meant that the Defendants' *use* of those receivers to decrypt the signals was without permission, it does not necessarily follow that the Defendants *access* to the decrypted signals was unauthorized. In the context of the DMCA, courts have

interpreted 'authorized' access to mean the use of the normal process or the intended mechanism for obtaining the copyrighted work"); *R. Christopher Goodwin & Assocs. v. Search, Inc.*, 2019 U.S. Dist. LEXIS 187073, at *7-8 (E.D. La. Oct. 29, 2019)("While the user id/password combination required for access was surely a 'technological measure' that controlled access to the works at issue, Pevny did not circumvent that measure. She validly accessed the system using her id/password combination while she was still an employee with Plaintiff. Even if the use that she made of that access is not something that Plaintiff would have authorized her to do, i.e., copy the materials at issue, it remains that Pevny's alleged abuse of her logon privileges does not rise to the level of descrambling, decrypting, or otherwise to avoiding, bypassing, removing, deactivating, or impairing anything"); *Joint Stock Co. Channel One Russ. Worldwide v. Infomir LLC*, 2017 U.S. Dist. LEXIS 22548, at *49-51 (S.D.N.Y. Feb. 15, 2017)("Similarly, there is no liability under § 1201(a)(1)(A) where the defendant misuses a password… to circumvent the technology that the copyright owner relied on for protection"); *Olmstead, Inc. v. CU Interface, LLC*, 657 F. Supp. 2d 878, 889 (N.D. Ohio 2009) (a defendant does not "circumvent or bypass any technological measure" when he uses "the approved methodology," such as a user name and password, to access copyrighted material). Because YouTube does not, in any way, restrict *access* to the works at issue, the District Court erred in finding, as a

matter of law, that Yout violated the anti-circumvention access control provisions of the DMCA contained in §§1201(a)(1) and 1201(a)(2). At a minimum, and as the EFF's letter amply demonstrates, the question of circumvention is a complicated and contested question of fact, one which must be resolved a jury, with the assistance of expert witnesses, after a full and fair opportunity for the Parties to conduct discovery.

D. The District Court Adopted a Definition of "Access" That Conflicts With the Statute Itself, the Caselaw, and the Commentary.

Having first discussed the different prohibitions included in §1201 – the "access control" provisions and the "copy control" provisions – the District Court then purported to fashion its own definition for the term "controls access" and, in doing so, managed to obliterate entirely the distinctions between "access controls" and "copy controls" by finding that the terms "controls access" was expansive enough to include a technological measure designed to prohibit the download (*i.e.*, copying) of a particular video file.[4] J.A. 250-51. Putting aside for the moment the

[4] It seems possible that the District Court made certain incorrect factual assumptions concerning Youtube's operation – somehow believing that two separate types of files exist for each video hosted by Youtube: one that can only be streamed and one that can be downloaded, and, based on that misunderstanding, then concluded that an access control mechanism existed in connection with the "downloadable version" of the music video but not the "streamable version." Such erroneous assumptions of fact – made without the benefit of either discovery or expert testimony - provides yet another reason why the District Court should not have attempted to decide complicated technical factual issues on a Rule 12(b)(6)

fact that YouTube does not even employ a technological measure that effectively controls copying, the District Court's error improperly conflated the two separate and distinct protections afforded by the DMCA.

Preliminarily, the distinction between "access control" (which was recognized as providing a new protection for copyrighted works not previously available to copyright holders) and "copy control" (which provides a new mechanism with which to protect those rights already afforded to copyright holders), was very much intentional in the enactment of the DMCA. The Senate Report on the DMCA makes plain the District Court's error:

> Although sections 1201(a)(2) and 1201(b) of the bill are worded similarly and employ similar tests, they are designed to protect two distinct rights and to target two distinct classes of devices. Subsection 1201(a)(2) is designed to protect access to a copyrighted work. Section 1201(b) is designed to protect the traditional copyright rights of the copyright owner. As a consequence, subsection 1201(a)(2) prohibits devices primarily designed to circumvent effective technological measures that limit access to a work. Subsection 1201(b), on the other hand, prohibits devices primarily designed to circumvent effective technological protection measures that limit the ability of the copyrighted work to be copied, or otherwise protect the copyright rights of the owner of the copyrighted work. The two sections are not interchangeable, and many devices will be subject to challenge only under one of the subsections. For example, if an effective technological protection measure does nothing to prevent access to the plain text of the work, but is

---

motion to dismiss. Even if this *was*, however, how the District Court went astray, its legal analysis would still be flawed: the RIAA's members hold copyrights to music and to videos and those are the protected "works," not a presumed (and non-existent) "downloadable version" of a music video as opposed to a "streamable version."

> designed to prevent that work from being copied, then a potential cause of action against the manufacturer of a device designed to circumvent the measure lies under subsection 1201(b), but not under subsection1201(a)(2).

Senate Report (DMCA), at p. 12.

Indeed, the importance of the distinction between the two types of prohibitions is evident in the statute itself. So, where §1201(a) prohibits circumvention of "a technological measure that effectively controls access" to a copyrighted work (and the provision of tools to enable such circumvention), §1201(b) prohibits circumventing the "protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof."

And, as is discussed in detail above, this Court has specifically held that the access control provisions of the DMCA are concerned not with the *use* of the copyrighted material (*i.e.* copying), but rather whether the copyrighted works were themselves protected by a technological measure that effectively controlled access to those works. *Corley* at 443 (and cases discussed, *supra*).

In a case presenting somewhat analogous facts, the Sixth Circuit rejected the definition and rationale utilized by the District Court here to define the term "controls access." *Lexmark International, Inc. v. Static Control Components, Inc*., 387 F.3d 522 (6th Cir. 2004). In *Lexmark*, Plaintiff Lexmark marketed computer printers. In an effort to ensure that its printers would only function properly with

toner cartridges that were manufactured or licensed by Lexmark, the Plaintiff utilized an "authentication sequence" that granted approved toner cartridges access to two computer programs (one of which was called the "Printer Engine Program") required for the printer's functionality. The Printer Engine Program also resided, in its entirety, in the memory of the Lexmark printers themselves (assuming that someone had the technological knowledge to access the printers' internal memory and copy the Printer Engine Program). The Defendant copied the Printer Engine Program from the internal memory of the printers and manufactured and sold a computer chip that rival toner cartridge manufacturers could use, bypassing the need for the authentication sequence that Lexmark had put in place intending to block access to the Printer Engine Program.

The District Court in *Lexmark* utilized the same Merriam-Webster Dictionary definitions as did the District Court here to conclude that "Lexmark's authentication sequence effectively 'controls access' to the Toner Loading Programs and the Printer Engine Program because it controls the consumer's ability to make use of these programs." *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 253 F. Supp. 2d 943, 967-68 (E.D. Ky. 2003). The Sixth Circuit explicitly reversed and remanded:

> We disagree. It is not Lexmark's authentication sequence that "controls access" to the Printer Engine Program. …It is the purchase of a Lexmark printer that allows "access" to the program. Anyone who buys a Lexmark printer may read the literal code of the Printer Engine Program directly from

> the printer memory, with or without the benefit of the authentication sequence, and the data from the program may be translated into readable source code after which copies may be freely distributed. …No security device, in other words, protects access to the Printer Engine Program Code and no security device accordingly must be circumvented to obtain access to that program code.
>
> The authentication sequence, it is true, may well block one form of "access" -- the "ability to . . . make use of" the Printer Engine Program by preventing the printer from functioning. But it does not block another relevant form of "access" -- the "ability to [] obtain" a copy of the work or to "make use of" the literal elements of the program (its code). Because the statute refers to "controlling access to a work protected under this title," it does not naturally apply when the "work protected under this title" is otherwise accessible. Just as one would not say that a lock on the back door of a house "controls access" to a house whose front door does not contain a lock and just as one would not say that a lock on any door of a house "controls access" to the house after its purchaser receives the key to the lock, it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works. Add to this the fact that the DMCA not only requires the technological measure to "control[] access" but also requires the measure to control that access "effectively," 17 U.S.C. § 1201(a)(2), and it seems clear that this provision does not naturally extend to a technological measure that restricts one form of access but leaves another route wide open. See also id. § 1201(a)(3) (technological measure must "require[] the application of information, or a process or a treatment . . . to gain access to the work") (emphasis added).
>
> … As shown above, the DMCA applies in these settings when the product manufacturer prevents all access to the copyrightable material and the alleged infringer responds by marketing a device that circumvents the technological measure designed to guard access to the copyrightable material.

Lexmark at 546-47, 548. *See also Dig. Drilling Data Sys., L.L.C. v. Petrolink Servs.*, 965 F.3d 365, 377 (5th Cir. 2020)("the issue is not whether the USB dongle and Interface Process were effective; it is whether they controlled access to the

database schema at all. On this point, the Sixth Circuit's reasoning in *Lexmark* is instructive. In that case, Lexmark argued that its 'authentication sequence' effectively controlled access to its Printer Engine Program—a copyrighted work installed on Lexmark printers—because the measure controlled consumers' ability to make use of the program. …The Sixth Circuit disagreed, holding that although the measure restricted users' ability to make use of the Printer Engine Program, it did not restrict access to the program itself, i.e., to its source code. …Precisely the same is true here: Although the USB dongle and Interface Process limited MWD companies' ability to make use of DataLogger, these measures did not control access to program's database itself, including its protected schema"); *Avaya, Inc. v. Telecom Labs, Inc*., 2011 U.S. Dist. LEXIS 164054, at *24-25 (D.N.J. Nov. 4, 2011)("a technological measure, in order to be effective, must prevent all forms of access to a work. …The Court agrees with Defendants' position and the reasoning of the Sixth Circuit. In the ordinary course of operation, Avaya's login combinations, activation/deactivation mechanisms, and its ASG Key authentication system do not prevent all forms of access to the protected work. …As the *Lexmark* and *MDY* courts aptly explained, '[j]ust as one would not say that a lock on the back door of a house 'controls access' to a house whose front door does not contain a lock . . . , it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works.'")

Nor is the District Court's interpretation saved by YouTube's Terms of Service. Even if such terms of service serve to restrict a user's permission to copy the otherwise publicly-accessible videos, such restrictions do not translate into a violation of the DMCA. *See, e.g., Joint Stock Co. Channel One Russ. Worldwide v. Infomir LLC*, 2017 U.S. Dist. LEXIS 22548, at *49-50 (S.D.N.Y. Feb. 15, 2017)("Violating contractual restrictions on access to or distribution of encrypted transmissions is 'not the type of 'circumvention' that Congress intended to combat in passing the DMCA'"); *DISH Network L.L.C. v. World Cable Inc.,* 893 F. Supp. 2d 452, 464 (E.D.N.Y. 2012)("Here, while the Defendants alleged fraud may have circumvented contractual barriers to receiving the signal, there are no facts in the first amended complaint from which the Court can infer that they circumvented the 'digital walls' that protected the copyrighted works. … there is no basis from which the Court can infer that simply moving the EchoStar receiver to an unauthorized location avoided or bypassed a 'digital wall', as opposed to a contractual restriction.")

E. Yout Has Plausibly Alleged That It Does Not Violate Either of the Anti-Trafficking Provisions of the DMCA.

Unlike the anti-circumvention provision (§1201(a)(1)), which requires a copyright holder to show *only* that a putative violator of the section circumvented a technological measure put in place by the copyright holder that effectively controls *access* to a work protected by a U.S. copyright, the two anti-trafficking provisions

(§1201(a)(2) and 1201(b)) add additional hurdles for the copyright holder which have significant overlap (despite the overlap, the sections do still differ somewhat in purpose, with §1201(a)(2) focusing on access, which has been discussed previously, and §1201(b) focusing on copy controls, discussed below). Yout has plausibly alleged that it did not run afoul of the anti-trafficking provisions and, in any event, the nature of the additional hurdles involved with respect to §1201(a)(2) and 1201(b) raise the types of factual issues not amenable to a Rule 12(b)(6) motion.

As noted above, the District Court properly parsed the relevant requirements of each of the two anti-trafficking sections:

> Congress enacted the anti-trafficking provision set forth in subsection 1201(a)(2), which proscribes "manufactur[ing], import[ing], offer[ing] to the public, provid[ing], or otherwise traffic[king] in any technology, product, service, device, component, or part thereof" that satisfies one of the following criteria:
>
> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;
> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.
>
> …Congress [also] adopted the "additional violations" provision, including subsection 1201(b), which proscribes "manufactur[ing], import[ing], offer[ing] to the public, provid[ing], or otherwise traffic[king] in any

> technology, product, service, device, component, or part thereof" that satisfies one of the following criteria:
>
> (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;
>
> (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or
>
> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

J.A. 244-45.

Certainly, Yout provides a "technology, product, or service" to the public. That being said, though, Yout has plausibly alleged that it does not meet any of the remaining criteria outlined in either §1201(a)(2) or 1201(b). And, although (for simplicity's sake) the discussion that follows will be framed primarily as addressing §1201(b) (because Yout has already discussed at length, above, many of the reasons why the RIAA's arguments under §1201(a)(2) fail), it should be noted that the arguments largely apply to both of the anti-trafficking provisions.

Before turning to the substantive anti-trafficking/copy control arguments, however, it seems important to address directly the District Court's erroneous contention – contained in a footnote in its opinion – that Yout "waived" the argument that it "does not violate 17 U.S.C. §1201(b)." Specifically, while

acknowledging that the "Second Amended Complaint repeatedly refers to section 1201 broadly," the District Court claimed that "neither the Second Amended Complaint not Yout's memorandum in opposition address whether Yout's technology violates the copy-control provision set forth in section 1201(b)." J.A. 274 at n.14. No such waiver occurred.

First, as the District Court acknowledges, the SAC "repeatedly refers to Section 1201 broadly." Obviously, §1201(b) is part of §1201, so the "broad" references in the SAC include §1201(b). Perhaps more to the point, the SAC discusses at length: (a) the process by which Yout allows users to download and copy video files to their computer (J.A. 40-42 at ¶¶34-46); (b) the fact that "No Decryption, Descrambling, or Similar Circumvention [Is] Necessary to Download YouTube Content" (J.A. 43-54 at ¶¶ 55-78); (c) that "Yout's software platform is not primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a copyrighted work, ***or that protects the right of a copyright owner*** (J.A. 60 at ¶117)(emphasis added); (d) that "any digital mechanism in place designed as anti-circumvention technology ***stops Yout users from recording and saving that protected work*** (J.A. 60 at ¶118)(emphasis added); (e) that "Yout's software platform has commercially significant purposes and uses other than to circumvent a technological measure that effectively controls access to a copyrighted work ***or that protects the right of a***

copyright owner (J.A. 60 at ¶120)(emphasis added); and (f) that "Yout's software platform has not been marketed for use in circumventing a technological measure that effectively controls access to a copyrighted work, ***or that protects the right of a copyright owner***")(J.A. 60 at ¶121)(emphasis added).

Each of these references (and there are more throughout the SAC), of course are relevant to the ***copy control*** provisions of §1201(b) and not the access control provisions of §1201(a). In the face of this, claims that the SAC fails to "address whether Yout's technology violates the copy-control provision set forth in section 1201(b)" are simply without merit.

Next, it bears noting that Yout's opposition was in direct response to the RIAA's motion to dismiss, a motion that never explicitly references §1201(b). This is crucial, of course, because – where the Complaint clearly alleges that Yout does not violate §1201(b) – it was the RIAA's burden, as the moving party, to prove that – as a matter of law –Yout *does* violate that subsection. Nevertheless, just as the RIAA's motion to dismiss discusses the *issues* surrounding downloading and copying (even if the RIAA never specifically references §1201(b)), so too does Yout's opposition. Again, those issues are relevant *only* to the copy control provisions of §1201(b).

And, finally, given that counsel for Yout below *repeatedly* argued during the hearing on the RIAA's Motion to Dismiss – both explicitly and by implication –

that Yout does not violate §1201(b),[5] the finding that Yout waved the argument cannot be upheld.[6]

F. Yout Has Plausibly Alleged That It Does Not Provide A Service That Is Primarily Designed or Produced For The Purpose of Circumventing Protection Afforded By A Technological Measure That Effectively Protects a Right of A Copyright Owner Under Title 17.

Turning, then, to the substantive anti-trafficking provisions (focusing, as noted, on §1201(b)), Yout has plausibly alleged facts to show that it does not provide a service or software that is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under Title 17.

First, as noted above, the existence of *any* technological measure is a disputed issue of fact precluding dismissal. Although the RIAA asserts that some bit of technology – that they did not themselves put in place – is designed to protect their rights as copyright holders, this is a factual issue that cannot be resolved without discovery.[7] Yout has clearly alleged in its complaint that no such

[5] *See* J.A. 195 at ln. 5-15; J.A. 196-97 at ln. 23-3; J.A. 204-05 at ln. 11-8; J.A. 205-06 at ln. 15-13; J.A. 207-08 at ln. 7-2; J.A. 208 at ln. 3-25; J.A. 209-11 at ln. 5-20; J.A. 220 at ln. 4-12; J.A. 220-21 at ln. 20-10; J.A. 231 at ln. 5-14.

[6] Notably, the Court never suggested during the hearing that he believed the point to be waived.

[7] Presumably the RIAA already has relevant evidence in its possession as there are undoubtedly communications between the RIAA and YouTube concerning the Javascript program at issue here and YouTube's purpose in utilizing that technology. One suspects that, if such evidence supported the RIAA's position, it

technological measure is in place. Also, as noted above, it is not at all clear (particularly given the legislative history) that the DMCA was intended to cover a circumstance where the supposed "technological measure" was put in place not by the copyright owner, but a third party for its own reasons. Permitting the case to proceed would, of course, permit the parties to better frame that argument at the summary judgment stage.

Even if the Court were to find it appropriate to assume the existence of a technological measure (thereby making a factual assumption at the 12(b)(6) stage in favor of the moving party), Yout has plausibly alleged that this technological measure does not effectively protect the right of a copyright owner.[8]

Section 1201(b)(2) provides that "a technological measure 'effectively protects a right of a copyright owner under this title' if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title." As the SAC alleges, YouTube's Javascript program does not do so.

---

would have answered the complaint, attaching such documents, and then moved for judgment on the pleadings. Instead, the RIAA moved to dismiss, cutting off the very discovery that might have shed light on YouTube's use of the Javascript program.

[8] The issue of protecting access has been addressed in part, above, though the arguments as to why the Javascript program does not effectively protect a right of a copyright owner apply equally to the access control provisions.

As the SAC details, any individual using a web browser (such as Google Chrome) can simply view a web page's source code using the built-in "developer's tools," identify the URL where the desired video is located, and use that URL to directly download the component parts of the video, using common software to put those parts back together again. *See, e.g.*, J.A., 44-54 at ¶¶62-78.

This is *not*, as the RIAA argued below, an argument that YouTube's software fails to effectively protect the Defendants' rights under copyright (if it is even intended to do so) because such "protection" can be easily thwarted, this is an argument that YouTube's software does not effectively protect the right at all. *See, e.g.*, *Lexmark,* 387 F. 3d at 549 (finding that the Printer Engine Program was not actually "protected" despite the existence of a technological measure designed to do so because the relevant computer code could also be freely extracted from the printer itself by anyone with the technological know-how to do so: "Doubtless, Lexmark is correct that a precondition for DMCA liability is not the creation of an impervious shield to the copyrighted work. …Otherwise the DMCA would apply only when it is not needed. But our reasoning does not turn on the *degree* to which a measure controls access to a work. It turns on the textual requirement that the challenged circumvention device must indeed circumvent *something*, which did not happen with the Printer Engine Program"); *Dig Dilling Data Systems*, 965 F.3d at 376-77 (where database protected by a computer dongle was otherwise publicly

available, there was no effective protection inasmuch as the protection was like "a house with a lock on the back door but none on the front. …At most, the portion of *Reimerdes* relied on by Digidrill stands for the rule that a technological measure need not be impenetrable to be 'effective' under the DMCA. …But here the issue is not whether the USB dongle and Interface Process were *effective, it is whether they controlled access* to the database schema at all.")

The RIAA has argued, however, that despite any person with a web browser having the ability to copy and download videos from YouTube using the web browser's easily-accessed developer's tools and despite the existence of an untold number of websites that instruct people how to do precisely that, YouTube still employs a technical measure that "effectively protects" their rights because (in their view) most people will find the process of using the web browser developer's tools to difficult or burdensome to undertake. Presumably, it is not easy to extract data from a memory chip in a printer and then reassemble that data into a program that might allow a person to use a competing toner cartridge with that printer, and yet that did not prevent the *Lexmark* court from finding a lack of effective protection there.

Ultimately, however, this becomes a question of fact for a jury to decide. Yout has plausibly alleged that the Javascript program utilized by YouTube (for unknown reasons) does not effectively protect the copyright interests of the

Defendants and, as such, the dismissal of Yout's complaint should be reversed and remanded to the District Court.

Even if the Court could conclude, however, that YouTube's Javascript was a technological measure that effectively protected the Defendants' rights under U.S. Copyright laws, Yout has plausibly alleged that it does not provide a service or product that circumvents that technological measure.

Before addressing the circumvention issue, though, it is important to detour briefly to discuss briefly the *nature* of the right at issue in this case, specifically, the right to copy a protected work. As Yout alleged in the SAC and as it argued below, the Court cannot consider that question of whether there is a "technological measure" "effectively protecting" a right held by the copyright owner without considering if the copyright owner really has the right it asserts. Here, it has long been established that an individual may legally make fair use of a copyrighted work by making a copy of that work so as to time-shift/location-shift the viewing of the work. *See, e.g., Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417, 446 (1984). Although the District Court recognized *Sony* as "well-settled anti-infingement law," it brushed aside any consideration of *Sony* in a footnote, holding that "Yout intends to push the boundaries of existing anti-circumvention law by drawing a parallel to well-settled anti-infringement law," a

parallel that it rejected solely because the present case "concerns alleged violations of the DMCA rather than copyright infringement…." J.A. 237 at n.3.

With respect to §1201(b), at a minimum, the District Court's analysis is flawed. A technological measure cannot be said to be effectively protecting a right held by a copyright owner if the "right" being protected is not a right at all. This, then, also presents a mixed question of fact and law not susceptible to dismissal at the 12(b)(6) stage and this Court should reverse the District Court's dismissal for that reason.

Next, even if the Court were to find that there was a technological measure that effectively protected a legitimate right of a copyright owner, Yout has plausibly alleged that it has not "circumvented" such a technological measure. Section 1201(b)(2)(A) defines the term "circumvent protection afforded by a technical measure" to mean "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure." As is discussed, above, Yout has plausibly alleged that it does not circumvent any technological measure that YouTube may have put in place because it does not avoid, bypass, remove, deactivate, or otherwise impair" any technological measure. Indeed, it is not even clear that YouTube's use of the Javascript code was intended to prevent copying of a protected work, or if it even does so. And, in any event, Yout does not

"circumvent" anything simply by utilizing the information that YouTube freely provides to each and every web browser.

Again, the question of circumvention is ultimately a complicated and contested question of fact, one which must be resolved by a jury, with the assistance of expert witnesses, after a full and fair opportunity for the Parties to conduct discovery. For this reason as well, the RIAA's motion to dismiss should have been denied and this Court should reverse the District Court's dismissal.

G. Yout Has Plausibly Alleged That Its Service (a) Has More Than Limited Commercially Significant Purposes and Uses Other Than To Circumvent Protection Afforded By A Technological Measure That Effectively Protects a Right of A Copyright Owner Under Title 17, and (b) Is Not Marketed By Yout For Use in Such Circumvention.

In examining the last two factors of §1201(b)(1), it is important to remember that, in enacting the DMCA, Congress was concerned that these sections might be misinterpreted to include devices or services that had significant non-infringing uses. Indeed, the legislative history is emphatic that Congress did not intend this section to include devices with multiple uses such as videocassette recorders. *See, e.g.*, House Judiciary Committee Report on the DMCA, §10 (Explaining that the limitations imposed by §1201(a)(2)(A-C) and their counterparts, §1201(b)(1)(A-C) are designed to ensure that the sections do not "include normal household devices such as Videocassette Recorders or personal computers, since such devices are not 'primarily designed' to circumvent technological protections… have obvious and

numerous commercially significant purposes and uses other than circumventing such protections, and are not intentionally marketed to circumvent such protections"); *Id.* at §§18-19 (restrictions are "drafted carefully to target 'black boxes' and to ensure that legitimate multipurpose devices can continue to be made and sold"); House Commerce Committee Report on the DMCA. §39 (As previously stated in the discussion of §1201(a)(2), the Committee believes it is very important to emphasize that… [§1201(b)(1)] is aimed at fundamentally outlawing so-called 'black boxes' that are expressly intended to facilitate circumvention of technical protection measures…. This provision is not aimed at products that are capable of commercially significant noninfringing uses, such as consumer electronics, telecommunications switches, personal computers, and servers – used by businesses and individuals for perfectly legitimate purposes"); Senate Judiciary Committee Report on the DMCA, §§29-30 (restrictions are "drafted carefully to target 'black boxes' and to ensure that legitimate multipurpose devices can continue to be made and sold"); House Manager's Report on the DMCA, §9 ("At the same time, the manufacturers of legitimate products such as Personal computers, VCR's and the like"); "Section 1201 of Title 17: a report of the register of copyrights" June 2017 ("In drafting the anti-trafficking provisions, Congress recognized the need to avoid prohibiting legitimate multipurpose devices designed for uses other than circumvention. The House Commerce Committee

Report ('Commerce Committee Report') specifically notes that section 1201(a)(2) 'is aimed fundamentally at outlawing so-called 'black boxes' that are expressly intended to facilitate circumvention of technological protection measures for purposes of gaining access to a work,' rather than 'products that are capable of commercially significant noninfringing uses, such as consumer electronics, telecommunications, and computer products.'")

With all of that in mind, Yout has alleged in the SAC that it has significant commercial uses other than to circumvent protections afforded by a technical measure that effectively protects the rights of a copyright owner. Indeed, one has to do little more than consider the fact that the majority of video files available on YouTube are not music videos and they are not necessarily protected by any copyright. Indeed, the software on which Yout operates has been widely recognized to have many legitimate uses, including for journalists, historians, and political activists around the world. *See, e.g,* "Music industry forces widely used journalist tool offline," *Freedom of the Press Foundation* (October 26, 2020), located at https://freedom.press/news/riaa-github-youtube-dl-journalist-tool/, last accessed February 2, 2023; "Music Industry Is Painting A Target On YouTube Ripping Sites, Despite Their Many Non-Infringing Uses," *Techdirt* (September 15, 2017), located at https://www.techdirt.com/2017/09/15/music-industry-is-painting-target-youtube-ripping-sites-despite-their-many-non-infringing-uses/, last accessed

February 2, 2023; "Despite RIAA's Claim That YouTube-dl Is Infringing, Journalists Use It All The Time," *Techdirt*, (November 12, 2020), located at https://www.techdirt.com/2020/11/12/despite-riaas-claim-that-youtube-dl-is-infringing-journalists-use-it-all-time/, last accessed February 2, 2023; "Youtube-dl is Back on Github: 'Our Priority Is Supporting Open Source'", *Vice* (November 16, 2020), located at https://www.vice.com/en/article/7k9b4q/youtube-dl-is-back-on-github, last accessed February 2, 2023.

Similarly, Yout plausibly alleged that it has not marketed itself as a service designed to circumvent protections afforded by a technical measure that effectively protects the rights of a copyright owner. To the contrary, Yout simply presents itself as a neutral tool, much like a VCR.

And, in any event, each of these factors present clear questions of fact that should not have been resolved on a Rule 12(b)(6) motion to dismiss.

IV. Yout Properly Plead A Claim Under Section 512(f).

To state a cause of action under 17 U.S.C. §512(f), a plaintiff must allege that the defendant knowingly misrepresented that a material or activity is infringing. *See, e.g., Crossfit, Inc. v. Alvies*, 2014 U.S. Dist. LEXIS 7930, at *6 (N.D. Cal. Jan. 22, 2014)("The DMCA targets the circumvention of digital walls guarding copyrighted material… Under the DMCA, specifically 17 U.S.C. 512(f),

any person who knowingly materially misrepresents that material infringes on a copyright shall be liable for damages incurred by the alleged infringer.")

And, while the District Court acknowledged that Yout alleged both of these things, it nonetheless held that Yout had failed to properly plead a claim under §512(f) because: (a) it believed §512(f) only to be applicable to claims of infringement and not circumvention, and (b) it required Yout to allege additional facts (without the benefit of discovery) as to the RIAA's state of mind in sending the notices to Google.

With respect to the first argument, the RIAA's notices to Google alleged that Yout provides "access to a service (and/or software) that circumvents YouTube's rolling cipher, a technical protection measure, that protects our members' works on YouTube from unauthorized copying/downloading." The key here, of course, is the assertion that Yout is enabling the infringement of the Defendants' copyrights, i.e., their right to control copying and downloading. In essence, then, the RIAA's notices to Google directly accused Yout of (at a minimum) secondary copyright infringement. Yout has alleged that this is a misrepresentation, sufficient to trigger the protections of §512(f).

And, with respect to the second, the Court's insistence that Yout was required to provide state of mind evidence prior to any discovery being taken is

misguided. Yout has alleged the requisite state of mind and, at the Rule 12(b)(6) stage, such an allegation is all that is required.

V. Yout Properly Alleged Claims for Business Disparagement and Defamation Per Se.

The entire basis of the District Court's dismissal of Yout's claims for business disparagement and defamation claims was its (erroneous) finding that the allegations contained in the RIAA's notices to Google were not "false" (inasmuch as the Court found that Yout violated the provisions of §1201). To the extent that this Court agrees that Yout has properly plead that it did not violate the provisions of §1201, it must also reverse the District Court's dismissal of these claims.

CONCLUSION

For the reasons stated hereinabove, this Court should REVERSE the District Court's judgment dismissing Yout's complaint and REMAND for further proceedings consistent with such reversal.

Respectfully submitted,

/s/ Evan Fray-Witzer

EVAN FRAY-WITZER
CIAMPA FRAY-WITZER, LLP
20 Park Plaza, Suite 505
Boston, Massachusetts 02116
(617) 426-0000
– and –
VALENTIN GURVITS
FRANK SCARDINO
Boston Law Group, PC
825 Beacon Street, Suite 20
Newton Centre, Massachusetts 02459
(617) 928-1800

Attorneys for Plaintiff-Appellant

CERTIFICATE OF COMPLIANCE

This document complies with the type-volume limit of Fed. R. App. P. 32(a)(7)(B), the word limit of Local Rule 32.1(a)(4) (A) because, excluding the parts of the document exempted by Fed. R. App. P. 32(f): this document contains 13,951 words.

This document complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because: this document has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point font Times New Roman.

Dated: New York, New York
February 2, 2023

ADDENDUM

ADDENDUM

Table of Contents

17 U.S.C. §1201

(a)VIOLATIONS REGARDING CIRCUMVENTION OF TECHNOLOGICAL MEASURES.—
(1)
(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

(B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

(C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine—
(i) the availability for use of copyrighted works;
(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;
(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

(v) such other factors as the Librarian considers appropriate.

(D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under

subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

(E) Neither the exception under subparagraph (B) from the applicability of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection—

(A) to "circumvent a technological measure" means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner; and

(B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

(b) ADDITIONAL VIOLATIONS.—

(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

(2) As used in this subsection—

(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological measure "effectively protects a right of a copyright owner under this title" if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.

(c) OTHER RIGHTS, ETC., NOT AFFECTED.—

(1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.

(2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.

(3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular

technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

(4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products.

(d) EXEMPTION FOR NONPROFIT LIBRARIES, ARCHIVES, AND EDUCATIONAL INSTITUTIONS.—

(1) A nonprofit library, archives, or educational institution which gains access to a commercially exploited copyrighted work solely in order to make a good faith determination of whether to acquire a copy of that work for the sole purpose of engaging in conduct permitted under this title shall not be in violation of subsection (a)(1)(A). A copy of a work to which access has been gained under this paragraph—

(A) may not be retained longer than necessary to make such good faith determination; and

(B) may not be used for any other purpose.

(2) The exemption made available under paragraph (1) shall only apply with respect to a work when an identical copy of that work is not reasonably available in another form.

(3) A nonprofit library, archives, or educational institution that willfully for the purpose of commercial advantage or financial gain violates paragraph (1)—

(A) shall, for the first offense, be subject to the civil remedies under section 1203; and

(B) shall, for repeated or subsequent offenses, in addition to the civil remedies under section 1203, forfeit the exemption provided under paragraph (1).

(4) This subsection may not be used as a defense to a claim under subsection (a)(2) or (b), nor may this subsection permit a nonprofit library, archives, or educational institution to manufacture, import, offer to the public, provide, or

otherwise traffic in any technology, product, service, component, or part thereof, which circumvents a technological measure.

(5) In order for a library or archives to qualify for the exemption under this subsection, the collections of that library or archives shall be—

(A) open to the public; or

(B) available not only to researchers affiliated with the library or archives or with the institution of which it is a part, but also to other persons doing research in a specialized field.

(e) LAW ENFORCEMENT, INTELLIGENCE, AND OTHER GOVERNMENT ACTIVITIES.—

This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term "information security" means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(f) REVERSE ENGINEERING.—

(1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

(2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other

programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.

(3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.

(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.

(g) ENCRYPTION RESEARCH.—

(1) Definitions.—For purposes of this subsection—

(A) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and

(B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

(2) Permissible acts of encryption research.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if—

(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption.—In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;3

(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

(4) Use of technological means for research activities.—Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to—

(A) develop and employ technological means to circumvent a technological measure for the sole purpose of that person performing the acts of good faith encryption research described in paragraph (2); and

(B) provide the technological means to another person with whom he or she is working collaboratively for the purpose of conducting the acts of good faith encryption research described in paragraph (2) or for the purpose of having that other person verify his or her acts of good faith encryption research described in paragraph (2).

(5) Report to congress.—Not later than 1 year after the date of the enactment of this chapter, the Register of Copyrights and the Assistant Secretary for Communications and Information of the Department of Commerce shall jointly report to the Congress on the effect this subsection has had on—

(A) encryption research and the development of encryption technology;

(B) the adequacy and effectiveness of technological measures designed to protect copyrighted works; and

(C) protection of copyright owners against the unauthorized access to their encrypted copyrighted works.
The report shall include legislative recommendations, if any.

(h) EXCEPTIONS REGARDING MINORS.—In applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which—

(1) does not itself violate the provisions of this title; and

(2) has the sole purpose to prevent the access of minors to material on the Internet.

(i) PROTECTION OF PERSONALLY IDENTIFYING INFORMATION.—

(1) Circumvention permitted.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if—

(A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;

(B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;

(C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and

(D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law.

(2) Inapplicability to certain technological measures.—
This subsection does not apply to a technological measure, or a work it protects, that does not collect or disseminate personally identifying information and that is disclosed to a user as not having or using such capability.

(j)SECURITY TESTING.—

(1) Definition.—
For purposes of this subsection, the term "security testing" means accessing a computer, computer system, or computer network, solely for the purpose of good faith testing, investigating, or correcting, a security flaw or vulnerability, with the authorization of the owner or operator of such computer, computer system, or computer network.

(2) Permissible acts of security testing.—
Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to engage in an act of security testing, if such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption.—In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—

(A) whether the information derived from the security testing was used solely to promote the security of the owner or operator of such computer, computer system or computer network, or shared directly with the developer of such computer, computer system, or computer network; and

(B) whether the information derived from the security testing was used or maintained in a manner that does not facilitate infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security.

(4) Use of technological means for security testing.—
Notwithstanding the provisions of subsection (a)(2), it is not a violation of that subsection for a person to develop, produce, distribute or employ technological means for the sole purpose of performing the acts of security testing described in subsection (2),[1] provided such technological means does not otherwise violate section [2] (a)(2).

(k) CERTAIN ANALOG DEVICES AND CERTAIN TECHNOLOGICAL MEASURES.—

(1) Certain analog devices.—

(A) Effective 18 months after the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in any—

(i) VHS format analog video cassette recorder unless such recorder conforms to the automatic gain control copy control technology;

(ii) 8mm format analog video cassette camcorder unless such camcorder conforms to the automatic gain control technology;.

(iii) Beta format analog video cassette recorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 1,000 Beta format analog video cassette recorders sold in the United States in any one calendar year after the date of the enactment of this chapter;

(iv) 8mm format analog video cassette recorder that is not an analog video cassette camcorder, unless such recorder conforms to the automatic gain control copy control technology, except that this requirement shall not apply until there are 20,000 such recorders sold in the United States in any one calendar year after the date of the enactment of this chapter; or

(v) analog video cassette recorder that records using an NTSC format video input and that is not otherwise covered under clauses (i) through (iv), unless such device conforms to the automatic gain control copy control technology.

(B) Effective on the date of the enactment of this chapter, no person shall manufacture, import, offer to the public, provide or otherwise traffic in—

(i) any VHS format analog video cassette recorder or any 8mm format analog video cassette recorder if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the automatic gain control copy control technology no longer conforms to such technology; or

(ii) any VHS format analog video cassette recorder, or any 8mm format analog video cassette recorder that is not an 8mm analog video cassette camcorder, if the design of the model of such recorder has been modified after such date of enactment so that a model of recorder that previously conformed to the four-line colorstripe copy control technology no longer conforms to such technology. Manufacturers that have not previously manufactured or sold a VHS format analog video cassette recorder, or an 8mm format analog cassette recorder, shall be required to conform to the four-line colorstripe copy control technology in the initial model of any such recorder manufactured after the date of the enactment of this chapter, and thereafter to continue conforming to the four-line colorstripe copy control technology. For purposes of this subparagraph, an analog video cassette recorder "conforms to" the four-line colorstripe copy control technology if it records a signal that, when played back by the playback function of that recorder in the normal viewing mode, exhibits, on a reference display device, a display containing distracting visible lines through portions of the viewable picture.

(2) Certain encoding restrictions.—No person shall apply the automatic gain control copy control technology or colorstripe copy control technology to prevent or limit consumer copying except such copying—

(A) of a single transmission, or specified group of transmissions, of live events or of audiovisual works for which a member of the public has exercised choice in selecting the transmissions, including the content of the transmissions or the time of receipt of such transmissions, or both, and as to which such member is charged a separate fee for each such transmission or specified group of transmissions;

(B) from a copy of a transmission of a live event or an audiovisual work if such transmission is provided by a channel or service where payment is made by a member of the public for such channel or service in the form of a subscription fee that entitles the member of the public to receive all of the programming contained in such channel or service;

(C) from a physical medium containing one or more prerecorded audiovisual works; or

(D) from a copy of a transmission described in subparagraph (A) or from a copy made from a physical medium described in subparagraph (C).
In the event that a transmission meets both the conditions set forth in subparagraph (A) and those set forth in subparagraph (B), the transmission shall be treated as a transmission described in subparagraph (A).

(3) Inapplicability.—This subsection shall not—

(A) require any analog video cassette camcorder to conform to the automatic gain control copy control technology with respect to any video signal received through a camera lens;

(B) apply to the manufacture, importation, offer for sale, provision of, or other trafficking in, any professional analog video cassette recorder; or

(C) apply to the offer for sale or provision of, or other trafficking in, any previously owned analog video cassette recorder, if such recorder was legally manufactured and sold when new and not subsequently modified in violation of paragraph (1)(B).

(4) Definitions.—For purposes of this subsection:

(A) An "analog video cassette recorder" means a device that records, or a device that includes a function that records, on electromagnetic tape in an analog format the electronic impulses produced by the video and audio portions of a television program, motion picture, or other form of audiovisual work.

(B) An "analog video cassette camcorder" means an analog video cassette recorder that contains a recording function that operates through a camera lens and through a video input that may be connected with a television or other video playback device.

(C) An analog video cassette recorder "conforms" to the automatic gain control copy control technology if it—

(i) detects one or more of the elements of such technology and does not record the motion picture or transmission protected by such technology; or

(ii) records a signal that, when played back, exhibits a meaningfully distorted or degraded display.

(D) The term "professional analog video cassette recorder" means an analog video cassette recorder that is designed, manufactured, marketed, and intended for use by a person who regularly employs such a device for a lawful business or industrial use, including making, performing, displaying, distributing, or transmitting copies of motion pictures on a commercial scale.

(E) The terms "VHS format", "8mm format", "Beta format", "automatic gain control copy control technology", "colorstripe copy control technology", "four-line version of the colorstripe copy control technology", and "NTSC" have the meanings that are commonly understood in the consumer electronics and motion picture industries as of the date of the enactment of this chapter.

(5) Violations.—
Any violation of paragraph (1) of this subsection shall be treated as a violation of subsection (b)(1) of this section. Any violation of paragraph (2) of this subsection shall be deemed an "act of circumvention" for the purposes of section 1203(c)(3)(A) of this chapter.

17 U.S.C. §512(f)

(f) MISREPRESENTATIONS.—Any person who knowingly materially misrepresents under this section—

(1)that material or activity is infringing, or

(2)that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.