22-2760

IN THE UNITED STATES COURT OF APPEALS
FOR THE SECOND CIRCUIT

YOUT, LLC,

PLAINTIFF-APPELLANT,

V.

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

DEFENDANTS–APPELLEES.

On Appeal from the United States District Court
for the District of Connecticut (New Haven)
Case No. 20-cv-1602 (SRU) (RAR)

BRIEF OF AMICUS CURIAE ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFF-APPELLANT AND REVERSAL

Mitchell L. Stoltz
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
mitch@eff.org
(415) 436-9333

Counsel for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, Amicus Curiae Electronic Frontier Foundation states that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

Dated: February 9, 2023

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

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Constitutional Provisions

Legislative History

Other Authorities

STATEMENT OF INTEREST[1]

The Electronic Frontier Foundation ("EFF") is a member-supported, nonprofit civil liberties organization that has worked for over 30 years to protect free speech, privacy, security, and innovation in the digital world. With over 33,000 members, EFF represents the interests of technology users in court cases and policy debates regarding the application of law to the internet and other technologies. EFF and the communities it serves have an interest in ensuring that copyright law safeguards freedom of expression, encourages innovation, and promotes creativity. EFF frequently participates in significant cases affecting copyright law, as amicus curiae, party counsel, or court-appointed attorneys ad litem.

[1] No counsel for a party authored this brief in whole or in part, and no person other than amicus or its counsel has made any monetary contributions intended to fund the preparation or submission of this brief. The parties have consented to the filing of this brief.

INTRODUCTION

The ban on circumvention of "technological measures" in Section 1201 of the Digital Millennium Copyright Act is strong medicine. Enacted to enhance the rights of copyright owners, these provisions also raise serious risks of interfering with First Amendment-protected speech and with lawful commerce in innovative technologies. The courts and Congress have acknowledged these risks.

One technology that is threatened by the overbroad application of Section 1201 is computer programs that automate the downloading of video and audio files from sites like YouTube. Plaintiff-Appellant Yout.com operates one such program. These programs fulfill the same function that videocassette recorders once did: they enable ordinary people to make and retain copies of videos that have already been released to the world at large by their creators. Like every reproduction technology—from the printing press to the smartphone—these programs, colloquially called "streamrippers," have important lawful uses as well as infringing ones. Video creators, educators, journalists, and human rights organizations all depend on the ability to make copies of user-uploaded videos. Copyright law ordinarily protects and promotes the lawful activities of these groups, through the fair use doctrine of 17 U.S.C. § 107 and other exceptions to copyright, but overbroad application of Section 1201 effectively strips that protection away, making these lawful activities legally fraught and practically difficult in the digital age.

Defendant-Appellees the Recording Industry Association of America and its member companies are engaged in a campaign to make streamripping tools a contraband technology, unavailable even to lawful users. Over the past several years, they have sought to block, censor, and demonetize providers of these tools because a subset of their users infringe copyright. The RIAA asserts that streamrippers necessarily circumvent access controls on video-sharing sites like YouTube in violation of Section 1201, a position adopted by the district court in this case.

That position is wrong. The district court adopted an extremely broad construction of a "technological measure that effectively controls access to a work" that is not supported by statutory text or precedent. The district court's holding effectively applies the strictures of Section 1201 to any copy of a work in digital form, not just the subset that rightsholders have chosen to protect with technological means. Because the exceptions to Section 1201 are narrower and more conditional than the exceptions to copyright itself, the district court's holding would increase legal *and* practical impediments to many lawful and important uses. That result would be contrary to the copyright's constitutional purpose: "to promote the progress of science." U.S. Const. Art. 1 § 8.

This Court should take a different approach. Text, legislative history, and precedent suggest clear limits on the definition of "technological measures."

YouTube's user-uploaded video service and its web-based player fall outside those limits.

ARGUMENT

I. Not Every Impediment to Access Is an "Effective" "Technological Measure."

Section 1201's three prohibitions apply to certain "technological measure[s]" used with copyrighted works. Subsections (a)(1) and (2) apply to measures "that effectively control[] access" to a work, while subsection (b) applies to measures that "effectively protect[] a right of a copyright owner . . . in a work." This statutory language places an important limit on the scope of "technological measures" subject to those prohibitions: it includes only technologies that were actually intended for use as controls on access or copying.

A. A "Technological Measure That Effectively Controls Access to a Work" Must Be One That Is Deployed for the Purpose of Controlling Access.

A computer program or other technology can impede access to a creative work, but only one that was installed *for that purpose* is a technological "measure." A technology may create an obstacle to copying without being designed or intended to uphold the rights of a copyright owner.

The word "measure" means "a step planned or taken as a *means to an end*."[2]

[2] "Measure," Merriam-Webster Dictionary (2022) (emphasis added).

Congress's word choice was deliberate. Section 1201 was enacted as an implementation of two World Intellectual Property Organization treaties that call for "legal remedies against the circumvention of effective technological measures that are *used by authors in connection with the exercise of their rights*" under copyright.[3] And this Court has held that "the focus of subsection 1201(a)(2) is circumvention of technologies *designed to prevent access* to a work." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 440-41 (2d Cir. 2001) (emphasis added).

As the House Commerce Committee noted when it passed the bill that would become Section 1201,

> [m]easures that can be deemed to "effectively control access to a work" would be those based on encryption, scrambling, authentication, or some other measure which requires the use of a "key" provided by a copyright owner to gain access to a work.[4]

The language of the statute reflects this legislative intent, treating "encrypted" or "scrambled" work as the canonical examples of works with technological measures. § 1201(a)(3). Encryption, when used effectively, prevents access to information without a key.[5]

---

[3] World Intellectual Property Organization, WIPO Copyright Treaty, art. 11, Dec. 20, 1996 ; World Intellectual Property Organization, WIPO Performances and Phonograms Treaty, art. 18, Dec. 20, 1996 ; *see* Conference Report No. 105-796, H.R. 2281, at 63 (105th Cong. Oct. 8, 1998) (emphasis added).

[4] Commerce Committee Report, No. 105-551, H.R. 2281, at 39 (105th Cong. July 22, 1998).

[5] Bruce Schneier, *Applied Cryptography* 3-4 (Wiley 1996).

In keeping with this interpretation, Section 1201 claims have usually been tied to technologies that were specifically designed and marketed as access controls or restrictions on copying. For example, the technology at issue in *Universal City Studios v. Corley* was an "encryption technology that motion picture studios place on DVDs." 273 F.3d 429, 435-36. A login that requires a password issued by the rightsholder is another valid measure. *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004), The common ingredient is the use of cryptographic keys, passwords, or other secret knowledge that the rightsholder (or its agent) makes some effort to withhold from the public. And courts have found that technologies like password protection, "authentication keys," and "secret handshake protocols" qualify as effective technological measures. *Id.*; *Adobe Sys. v. Feather*, 895 F. Supp. 2d 297, 302 (D. Conn. 2012); *Davidson & Assocs. v. Jung*, 422 F.3d 630, 642 (8th Cir. 2005). While not all of these involve encryption, they all involve some form of secret knowledge in the possession of the rightsholder or its agent without which access is exceedingly difficult.

The YouTube website code at issue in this case is different: it was not clearly designed to limit access to videos, or the ability to copy them. YouTube videos arrive at a viewer's device with no encryption or scrambling.[6] No login, password, key, or

[6] Like most web data, YouTube video streams may be encrypted using Transport Layer Security while in transit to the requesting user, to protect the user's privacy,

other secret knowledge is required to gain access. When a user requests a YouTube video using a web browser, YouTube's servers send a web page which contains a JavaScript program. The program appears to have several functions, including selecting the video quality that the user's internet connection can support and selecting the starting point for playback (the "range" function). The program also generates a "signature value" that is passed back to YouTube's servers to initiate the video stream. The program is not secret: any member of the public can read it by simply right-clicking on a web page, and any common web browser can run it. While Defendant-Appellee RIAA described this program as a "rolling cypher," the program does not limit any user's access to videos, or their ability to save a copy.

YouTube does not identify the player program as an access control. The district court cited to language in YouTube's Terms of Service asserting that users are not allowed to circumvent "features that . . . limit the use of the service or content," but those terms don't state or imply that any "feature" of the service, including the player program, is intended to prevent downloading. *Yout, LLC v. Recording Indus. Ass'n of Am., Inc.*, No. 3:20-CV-1602 (SRU), 2022 WL 4599203, at *10 (D. Conn. Sept. 30, 2022).

---

but this encryption is removed immediately by any web browser software upon receipt. It requires no verification of a user's identity or permission to access the data.

Tellingly, YouTube does use encryption and a password-controlled login to limit access to subscribers of its separate pay-TV service, YouTube TV. That similar access controls are not present on YouTube's core user-uploaded video platform is another indication that the company did not intend to impose an access control on user-uploaded videos.

The statutory text and legislative history support preserving the standard that courts have adhered to thus far: limiting the scope of technological "measures" under Section 1201 to tools that were designed to control access to or copying of works, and employed for those purposes, and when a technology does not require a key, password, or other secret knowledge in the possession of the rightsholder, that technology would not be effective at and likely was not intended to control access or copying.

B. The Absence of a Download Button in YouTube's Standard User Interface Does Not Transform the Interface into an Effective Technological Measure That Controls Copying.

The district court made the unwarranted assumption that the YouTube player code "was designed to gatekeep" access to videos, even though the code does not employ any of the types of technologies that could demonstrate an intent to control access. *See Yout LLC,* 2022 WL 4599203, at *17. That conclusion appears to be based on the observation that "YouTube does not readily offer a download button or other feature by which the user may access a downloadable audio or video file." *Id.*

at *7. The absence of a download button should not be relevant to whether a technological measure is present, let alone determinative.

People access the web using a great variety of technologies. Their hardware includes everything from smartphones and tablets to personal computers, appliances, wearable devices, smart speakers, and even vehicles. The software running on those devices can be a widely used web browser like Google Chrome, an alternative browser such as Brave or Opera, or a command-line utility that finds and retrieves web data. Users frequently modify these collections of personal technology by adding additional software such as browser extensions to serve a variety of purposes: limiting bandwidth usage on a slow internet connection, filtering content, enhancing privacy by blocking some forms of data harvesting, or rendering websites accessible to people with print disabilities.

These combinations of hardware and software ultimately provide a varying set of capabilities to the user, including a greater or lesser ability to make copies of the content they access. The standard browser on a mobile phone with limited data storage may not be capable of storing copies of video, audio, images, or text once the user is no longer viewing them. On the other hand, common utilities used by sophisticated internet users, such as "wget,"[7] save copies of web content by default for later viewing or analysis. In between these two extremes, typical browsers on a

[7] https://www.gnu.org/software/wget/.

personal computer store local copies of some parts of websites for days or longer, as a normal part of their operation. In many cases, the presence of a "download button" or automatic storage of local copies depends on the user's choice of web browsing technology and how it is configured. A viewer's control over the behavior of web pages is an ordinary and widely known aspect of the internet, not an extraordinary circumstance.

Some rightsholders use technology to limit the combinations of hardware and software that can be used to view and make further use of their works, putting technological limits on the viewer's discretion. For example, the subscription-based video services described above encrypt video data in ways that can only be decrypted by browsers or apps approved in advance by the service provider. Without a decryption key or password obtained from the service provider, either a user will not be able to access copies at all, or else any saved copies will remain encrypted and not usable. For example, the Spotify streaming music service allows users to download copies of songs, but it encrypts the downloads so that they can only be played by current subscribers through Spotify's own player app.[8] In these cases, the rightsholder has done more than simply direct users not to copy, or omit a download button—they have made copying difficult with any set of common, general-purpose

[8] Spotify Community, *Where Are My Downloaded Songs On My PC*, https://community.spotify.com/t5/Desktop-Windows/Where-are-my-downloaded-Spotify-songs-on-my-PC/td-p/4739320 (accessed Feb. 7, 2023).

web browsing hardware and software.

YouTube, again, doesn't fall into this category. Videos uploaded to YouTube are viewable and downloadable on a wide variety of hardware and software configurations. YouTube does not limit access to its video-sharing service to pre-approved browsers or hardware—its videos are viewable and downloadable through a wide variety of user tools. The JavaScript program that initiates a video stream can be run on any web browsing software that includes a JavaScript interpreter, another ubiquitous feature.

The district court concluded that the absence of a download button from the YouTube user interface when using a standard browser configuration establishes the presence of a technological measure that is effective "in the ordinary course" of its operation. *Yout LLC*, 2022 WL 4599203, at *13. (quoting 17 U.S.C. § 1201(a)(3)(B)). That defines "ordinary course" too narrowly, including only a single mode of accessing the web while excluding other common, general-use combinations of hardware and software that YouTube makes no effort to bar.

As the district court noted, "it is well-established that unauthorized access without circumvention does not constitute a violation of the DMCA." *Yout LLC,* 2022 WL 4599203, at *16; *see I.M.S*, 307 F. Supp. 2d at 532. But implying the presence of an effective technological measure from the absence of a download button in the "ordinary" user interface makes the application of Section 1201 turn

on the presence or absence of authorization, regardless of whether any circumvention occurs or is required—a result that is contrary to the extensive caselaw cited by the district court.

Allowing the presence of a technological measure to turn on the presence or absence of a download or copying function allows a rightsholder to impose liability for even non-infringing copying without employing a technology that actually impedes such copying. Consider a music copyright owner who releases music on phonograph records or CDs and provides buyers with a player that has a speaker, but no other audio output. Under the district court's holding, the rightsholder has applied an effective technological measure that prevents copying in the "ordinary course of its operation." Of course, this analysis ignores that a user can play the record or CD on another readily available player that has an audio output, and use that output to make copies, without circumventing any measure applied to the record itself. In this hypothetical, as in the instant case, the "ordinary course" of operation must include playing the unencrypted media with different, commonly available, general-purpose devices that may have a download or copy function.

II. The District Court's Unbounded Definition of a Technological Measure Would Impede Artistic, Educational, Documentary, and Other Important and Lawful Uses of Digital Media.

The district court's approach represents a significant expansion of the scope of Section 1201. If "technological measures" can be identified retroactively, in

litigation, without clear indicia that an access control was intended, then almost any work distributed in digital form could later be deemed subject to the circumvention ban of Section 1201(a)(1), and any tool that automates or otherwise enhances access to such content risks liability under the "trafficking" bans of Sections 1201(a)(2) and (b). That is a dangerous outcome that reaches far beyond the circumstances of this case, disrupting the balance of public and private interests that copyright embodies.

Copyright law has always allowed for a wide variety of uncompensated and permissionless uses of creative works through the exclusion of ideas, processes, systems, and methods from copyright's scope, the fair use doctrine, and specific statutory limitations for other uses. These exceptions and limitations enable education, journalism, critical commentary, scholarship, new creative work, and technological innovation. In doing so, they give effect to the Constitution's grant of authority to enact copyright laws "to promote the progress of science," and to conform the law to the First Amendment's guarantee of free speech. *Golan v. Holder*, 556 U.S. 302, 318 (2012).

Even properly construed, Section 1201 alters this balance by impeding access to works for those who would make lawful uses. Because some courts have held that Section 1201 liability does not require a "nexus" to some underlying act of copyright infringement, circumventing an access control to make lawful use of a copyrighted work, and providing tools to facilitate such lawful use, risk Section 1201 liability

unless one of the narrower defenses of that section apply.

Limiting the scope of works and technologies that Section 1201 covers helps mitigate the problem, albeit unsuccessfully. For example, if a lawful user can obtain a copy, including a digital copy, that is free from access controls, they can use it to the fullest extent allowed by copyright law, without fear of Section 1201 liability. That preserves opportunities for lawful uses of all kinds—including important uses of video-sharing sites like YouTube. Amateur video creators rely on the ability to download video to use excerpts in reviews or commentaries, or as part of new creative endeavors. Journalists and human rights monitoring organizations need to be able to save copies of eyewitness videos documenting notable events, conflicts, and malfeasance. Even copyright holders and their licensees rely on tools like Yout.com to download copies of their own or licensed works.

By contrast, expanding the scope of Section 1201 to potentially cover any digital copy of a work that a rightsholder can later claim was subject to some inadvertent or ambiguous technical impediment would dramatically narrow those opportunities. What is worse, by applying the "trafficking" bans of 1201(a)(2) and (b) to a much broader range of commonly used technologies, such an expansion makes these lawful and important uses more difficult and labor-intensive at best, or impossible at worst, by denying access to tools like Yout.com that facilitate and automate access to online video.

CONCLUSION

This Court should reject the unwarranted expansion of Section 1201 liability, and reverse the dismissal of Yout.com's claims.

Dated: February 9, 2023

Respectfully submitted,

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

Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
mitch@eff.org
(415) 436-9333

Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amicus Curiae Electronic Frontier Foundation in Support of Plaintiff-Appellant and Reversal. complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B), Fed. R. App. P. 29(a)(5), Second Circuit L. R. 29.1(c) and Second Circuit L. R 32.1(a)(4) because this brief contains 3,225 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief 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 brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, the word processing system used to prepare the brief, in 14-point font in Times New Roman font.

Dated: February 9, 2023

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

Counsel for Amicus Curiae

CERTIFICATE OF SERVICE

I certify that on this 9th day of February, 2023, I electronically filed the foregoing Brief of Amicus Curiae using the Court's CM/ECF system which will send notification of such filing to all parties of record.

Dated: February 9, 2023

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

Counsel for Amicus Curiae