

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

TED ENTERTAINMENT, INC., et al.,
Plaintiffs,
v.
APPLE, INC.,
Defendant.

Case No. 26-cv-02936-RS

**ORDER DENYING MOTION TO
DISMISS****I. INTRODUCTION**

Plaintiffs Ted Entertainment, Inc. (“Ted”) and Matt Fisher (the “Plaintiffs”) bring this action on behalf of themselves and a putative class of content creators who upload and share videos on YouTube. Plaintiffs allege Defendant Apple Inc. (“Apple”) circumvented technological protection measures (“TPMs”) to scrape copyrighted videos from YouTube’s online viewing platform in violation of the Digital Millennium Copyright Act (“DMCA”), 17 U.S.C. § 1201. For the reasons explained below, Defendant’s motion to dismiss is denied.

II. BACKGROUND¹

Plaintiffs are content creators who upload original videos exclusively to YouTube, a video-sharing website. By uploading to YouTube, Plaintiffs—along with anyone else who uploads

¹ Unless otherwise stated, this order accepts well-pled factual allegations made in the complaint as true for the purposes of this motion.

1 videos to the platform—agree to allow website visitors (“users”) to access their videos consistent
 2 with YouTube’s Terms of Service (“YouTube’s Terms”). YouTube’s Terms prohibit users from
 3 “access[ing]... any Content except... as expressly authorized by the [Terms of] Service or... with
 4 prior written permission from YouTube and, if applicable, the respective rights holders.” Dkt. 29,
 5 Pl.’s Am. Compl. ¶ 76.

6 YouTube’s Terms permit users to watch videos only in the website’s authorized playback
 7 environment. There, users do not have “direct access to audiovisual works in their native or fixed
 8 form.” *Id.* at ¶ 44. Rather, users receive “segmented, time-limited portions of a work for
 9 ephemeral playback.” *Id.* All the while, the native video “remains within YouTube’s controlled
 10 delivery system” and is “never released in usable form.” *Id.* at ¶ 45–46. This system creates two
 11 URLs, one that links to the public webpage where users can watch video segments (the “page
 12 URL”) and another that links to the underlying, native video (the “file URL”).

13 This limitation ensures YouTube (and the content creators who upload videos to YouTube)
 14 receives compensation. YouTube’s authorized playback environment allows users to watch videos
 15 only in exchange for either money (purchasing a YouTube Premium account) or advertising
 16 impressions (watching commercials before, after, or during a video). Either way, YouTube earns
 17 money with each view. That income also benefits Plaintiffs because content creators earn money
 18 each time a user views one of their videos within the authorized playback environment. Plaintiffs
 19 rely on this business model when deciding whether to upload their content to YouTube.

20 To ensure users view YouTube videos within the authorized playback environment,
 21 YouTube employs several TPMs. YouTube’s TPMs include: (1) a rolling cipher, (2) session-
 22 bound, short-lived URLs, (3) CAPTCHA challenges, (4) proof-of-origin tokens, and (5) IP
 23 blocking and rate limiting. The rolling cipher is a complex, periodically changing algorithm that
 24 encrypts every native video’s URL. YouTube’s streaming architecture decrypts the rolling cipher,
 25 “unlocking” this file URL so users can access the video’s content within the authorized playback
 26 environment. Session-bound, short-lived URLs require users regularly to obtain new authorization
 27 to view video content, which allows YouTube to verify periodically a user’s behavior as consistent
 28

1 with YouTube’s Terms. YouTube presents CAPTCHA challenges—“tests designed to separate
 2 human users from bots,”—when, through constant traffic-pattern monitoring, user behavior looks
 3 suspicious or automated. *Id.* at ¶ 67. Proof-of-origin tokens are embedded in the video segments
 4 users view and ensure user requests “originat[e] from an authorized YouTube playback
 5 environment.” *Id.* at ¶ 71. YouTube also “monitors network behavior and” blocks IP addresses
 6 engaged in “excessive or abusive request patterns.” *Id.* at ¶ 61. Individually and collectively,
 7 YouTube’s TPMs are designed to “prohibit unauthorized access” to underlying videos. *Id.* ¶ at 76.

8 YouTube’s TPMs, however, do not create an impenetrable defense system, and Apple
 9 successfully accessed Plaintiffs’ underlying videos despite the TPMs. Apple overcame YouTube’s
 10 TPMs through a process called “scraping,” an automative process that accesses and downloads
 11 digital content—in this case, the native videos. *Id.* ¶ 101. To scrape YouTube’s platform, Apple
 12 began with a publicly available dataset called HD-VILA-100M, which is made up of millions of
 13 datapoints that can be used to identify various YouTube videos. Apple used HD-VILA-100M to
 14 create its own dataset, Panda-70M, which is similarly made up of millions of datapoints that can
 15 be used to locate underlying YouTube videos. With these datasets, Apple went outside YouTube’s
 16 authorized playback environment to locate, access, and download millions of underlying videos.

17 Apple relied on various scraping methods and mechanisms to download native videos at
 18 this scale. Apple used descrambling tools, like yt-dlp, to evade YouTube’s rolling cipher. Further,
 19 Apple implemented an IP rotation scheme meant to deceive YouTube’s IP-based monitoring and
 20 blocking system. Apple also employed additional, unauthorized circumvention tactics—
 21 regenerating valid links, obtaining fresh authorization parameters, spoofing or reusing proof-of-
 22 origin tokens—to evade YouTube’s session-bound, short-lived media URLs; CAPTCHA
 23 challenges; and proof-of-origin tokens.

24 III. LEGAL STANDARD

25 Rule 12(b)(6) governs motions to dismiss for failure to state a claim. Fed. R. Civ. P.
 26 12(b)(6). A complaint must contain “a short and plain statement of the claim showing that the
 27 pleader is entitled to relief.” *Id.* at 8(a)(2). While “detailed factual allegations” are not required, a
 28

complaint must have factual allegations sufficient to state a claim that is “plausible on its face.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555, 570 (2007)). Dismissal under Rule 12(b)(6) may be based on either the “lack of a cognizable legal theory” or on “the absence of sufficient facts alleged” under a cognizable legal theory. *UMG Recordings, Inc. v. Shelter Capital Partners LLC*, 718 F.3d 1006, 1014 (9th Cir. 2013) (citation omitted). When evaluating such a motion, the court must accept all material allegations in the complaint as true and construe them in the light most favorable to the non-moving party. *In re Quality Sys., Inc. Sec. Litig.*, 865 F.3d 1130, 1140 (9th Cir. 2017). It must also “draw all reasonable inferences in favor of the nonmoving party.” *Usher v. City of Los Angeles*, 828 F.2d 556, 561 (9th Cir. 1987).

IV. DISCUSSION

Enacted in 1998, the DMCA modernized federal copyright law to protect online service providers, encourage copyright holders to share their work through digital media, and discourage the dissemination of false copyright information. Congress intended for the DMCA to “provide effective legal remedies against the circumvention of protective technological measures used by copyright owners.” *MDY Indus., LLC v. Blizzard Ent., Inc.*, 629 F.3d 928, 942 (9th Cir. 2010).

Section 1201(a)(1)(A) of the DMCA prohibits the “circumvent[ion of] a technological measure that effectively controls access to a [copyright-protected] work.” 17 U.S.C. § 1201(a)(1)(A). Circumvention occurs when violators “descramble a scrambled work... decrypt an encrypted work, or otherwise... avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.” *Id.* at § 1201(a)(3)(A). To control access *effectively*, a measure must “in the ordinary course of its operation, require[] the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.” *Id.* at § 1201(a)(3)(B).

Plaintiffs allege Apple violated § 1201(a) by employing various scraping tools to view and download millions of YouTube videos outside YouTube’s authorized playback environment. Apple makes three arguments against these allegations. First, Apple argues YouTube’s TPMs are

not access controls and, thus, not regulated by § 1201(a). Second, Apple argues YouTube’s TPMs do not operate within the ordinary course of operations, again placing them outside § 1201(a)’s reach. Third, Apple argues its own behavior did not constitute “circumvention” as defined by the DMCA. As explained below, these arguments are unpersuasive at this stage of the litigation.

A. YouTube’s TPMs as Access Controls

Apple first argues Plaintiff’s claim should be dismissed because YouTube’s TPMs are not *access* controls. Rather, Apple asserts, the TPMs are *use* controls regulated by § 1201(b), on which Plaintiffs do not rely in asserting their claim. As noted, § 1201(a) regulates “technological measure[s] that effectively control[] access to a work.” In contrast, § 1201(b) regulates “technological measure[s] that effectively protect[]” the statutory rights of a copyright owner. 17 U.S.C. §§ 1201(a), (b). This difference, Apple contends, matters because “differently worded provisions must be read to ‘ensure[] that neither section is rendered superfluous.’” Dkt. 35, Def.’s Mot. to Dismiss, 13 (quoting *MDY Indus.*, 629 F.3d at 946).

While Congress likely intended each provision to do independent work, Apple’s suggestion that § 1201(a) applies to controls only that “prevent all uses of a work” asks too much of the canon against surplusage. The Ninth Circuit said just as much, explaining “[t]he statutory definition of the phrase ‘effectively control access to a work’ does not require... an access control [to] be strong or circumvention-proof. Rather, it requires an access control measure to provide some degree of control over access to a copyrighted work.” *MDY Indus.*, 629 F.3d at 954 n.17 (citing 17 U.S.C. § 1201(a)(2)). The Ninth Circuit also rejects Apple’s use-access binary, noting the DMCA “does not provide that a TPM cannot serve as both an access control and a use control.” *Disney Enters. v. VidAngel, Inc.*, 869 F.3d 848, 864 (9th Cir. 2017). Consequently, the appropriate inquiry is not whether YouTube’s TPMs are use controls or access controls, but whether YouTube’s TPMs “provide some degree of control over access to a copyrighted work.” *MDY Indus.*, 629 F.3d at 954 n.17 (citing 17 U.S.C. § 1201(a)(2)).

At this juncture, Plaintiffs’ allegations sufficiently show YouTube’s TPMs are access controls within the meaning of § 1201(a). First, YouTube’s rolling cipher decrypts the file URL,

which is “encrypted using a complex and periodically changing algorithm,” only when authorized users request to view a video within YouTube’s playback environment. Dkt. 29, at ¶ 59. YouTube uses a “proprietary logic embedded in the official YouTube player” to determine whether a request is authentic, allowing the rolling cipher to control whether a video’s content becomes accessible to a user. Dkt. 29, at ¶ 58. Second, YouTube uses IP-blocking technology to restrict or terminate user access when it detects suspicious browsing behavior. Third, YouTube uses session-bound, short-lived URLs to prevent users from using stale links to access videos outside the authorized playback environment. Fourth, users engaged in suspicious behavior are typically required to complete “tests designed to separate human users from bots” known as CAPTCHA challenges. Dkt. 29, at ¶ 58. Fifth and finally, “YouTube... restricts access to its platform by requiring that all requests for video segments include cryptographic proof-of-origin tokens that validate the request as originating from an authorized YouTube playback environment.” Dkt. 29, at ¶ 71. As described in the pleading, each of these tools limit who, where, how, and for how long users can access YouTube videos. A technology that limits access is, by statutory definition and common sense, an access control as described in § 1201(a).

Apple counters that, because YouTube videos are publicly accessible, the website’s TPMs offer *no* control over access to Plaintiffs’ copyrighted work. This argument defies logic and Ninth Circuit precedent. That any user can access videos through YouTube’s authorized streaming architecture does not undermine Plaintiffs’ arguments; rather, it affirms them. YouTube’s TPMs limit users’ access to a singular platform, the website’s authorized streaming architecture. Accessing YouTube videos in any other way violates YouTube’s Terms and circumvents its TPMs. Moreover, the Ninth Circuit addressed functionally the same question in *VidAngel*. There, the Ninth Circuit considered whether VidAngel’s practice of purchasing, decrypting, editing, and reselling DVDs violated § 1201(a) even though any original purchaser, using an authorized DVD player, could easily access the DVD’s content without violating the DMCA. In upholding a preliminary injunction against VidAngel, the Ninth Circuit reasoned, “[n]othing in [DMCA’s] legislative history suggests... VidAngel did not circumvent an access control simply because there

are authorized ways to access the [] works.” *VidAngel*, 869 F.3d at 865. Here, as in *VidAngel*, Plaintiffs’ copyrighted work is accessible through a valid viewing channel. Nevertheless, limiting access to that single, valid channel is an access control protected by and enforceable under § 1201(a).

B. YouTube TPMs Operate in the Ordinary Course of Operations

Apple next argues YouTube’s TPMs are not actionable under § 1201(a) because they “do not operate in the ordinary course of operation.” Dkt. 35, at 16. The DMCA prohibits circumventing protective measures that “effectively control[] access to” copyrighted work. 17 U.S.C. § 1201(a)(1)(A). In relevant part, the DMCA states “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 of treatment, with the authority of the copyright owner, to gain access to the work.” *Id.* at § 1201(a)(3)(B). Apple interprets this provision to mean an access control is only effective—and, thus, only enforceable under § 1201(a)—if a user must take an affirmative action to disarm it. If a user can access work uploaded to YouTube without taking an affirmative action like entering a password, Apple reasons, YouTube’s TPMs do not require “the application of information, or a process or a treatment... to gain access to the work” and are, thus, not actionable access controls under the DMCA. *Id.*

While Apple correctly observes most users do not affirmatively act to disarm YouTube’s TPMs, Apple is incorrect to say DMCA access controls necessarily require affirmative action. As a Central District of California court observed just weeks ago, “[n]othing in § 1201(a) requires an access control to take the form of a paywall, password prompt, or other measure requiring affirmative user input.” *Ted Ent. Inc. v. Snap Inc.*, No. 26 Civ. 754, 2026 WL 2435349, at *4 (C.D. Cal. Aug. 19, 2026). Rather, the DMCA only demands a technological measure—in this case, YouTube’s TPMs—require some “application of information, or a process or a treatment” “in the ordinary course of its operation” to access the protected work. 17 U.S.C. § 1201(a)(3)(B).

Ted plausibly alleges both that users encounter TPMs “in the ordinary course of [YouTube’s] operations” and that YouTube’s TPMs either require information from the user or employ a

platform-side process before users can access protected work. YouTube’s infrastructure constantly monitors network behavior, including “the number and frequency of requests originating from individual IP addresses against defined thresholds.” Dkt. 29, at ¶ 62. When its monitoring system detects suspicious behavior, YouTube’s servers may “cut off platform access from the offending IP address entirely” or require the user to provide additional information by way of CAPTCHA challenges. *Id.* Moreover, the rolling cipher affects *every* video request, requiring the “application of a specific computational process” before a user can obtain an audiovisual file. Dkt. 29, at ¶ 58. Further, YouTube requires “*all* requests for video segments [to] include cryptographic proof-of-origin tokens that validate the request as originating from an authorized YouTube playback environment.” *Id.* at ¶ 71 (emphasis added). As alleged, YouTube’s TPMs clearly employ authentication processes and request information from users “in the ordinary course of operations” to ensure users access videos only within the authorized playback environment.

To circumvent the controlling case law, Apple attempts to distinguish YouTube’s TPMs from the access controls reviewed in *VidAngel*. There, Apple notes, a DVD must be decrypted before a viewer can access its contents. Whether a viewer decrypts his DVD with an authorized DVD player or an unauthorized decryption software, he must always take an affirmative action before he can access the DVD’s contents. In contrast, Apple argues, YouTube often does not require users to complete a process or apply information to access YouTube videos. Many of YouTube’s TPMs, like CAPCHA tests or IP-blockers, confront users only when YouTube suspects the user is engaged in suspicious activity. Thus, in the ordinary course of operations, a YouTube user may never be confronted with an access control TPM.

Apple’s attempt to distinguish DVDs, the items *VidAngel* found employ DMCA access controls, is unavailing. Apple argues DVDs and YouTube videos are incomparably different because viewers must always decrypt DVDs while YouTube users are not required to go through any process or provide information to view YouTube videos. However, like DVDs and unlike Apple’s assertions, underlying YouTube videos are encrypted. *See* Dkt. 29, ¶ 59 (“The file URL is encrypted using a complex and periodically changing algorithm.”). Clicking an authorized link to

view a YouTube video is like inserting a DVD into an authorized DVD-player; the user himself does not do the decrypting, but decryption occurs in both situations. That a YouTube user can circumvent this encryption does not mean the protection doesn't apply "in the ordinary course" of YouTube's operations. 17 U.S.C. ¶ 1201(a)(3)(B); *see also VidAngel*, 869 F.3d at 865. Rather, it suggests only that, when a user encounters an unencrypted YouTube video, he is operating outside the ordinary, authorized scope of access.

C. Apple's Circumvention

Finally, Apple argues that, even if YouTube's TPMs are access controls, Apple's alleged actions do not constitute "circumvention" as defined by the DMCA. Apple begins with the text, noting that circumvention is defined differently in § 1201(a) and § 1201(b). Under § 1201(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." 17 U.S.C. § 1201(a)(3)(A). In contrast, the § 1201(b) definition for "circumvention" does not include descrambling or decrypting. *Id.* at § 1201(b)(2)(A). Relying on the canons of meaningful construction and *noscitur a sociis*, Apple argues this difference must mean § 1201(a) applies only to affirmative actions, such as "descrambling or decrypting the [copyrighted] work." Apple cites several out-of-circuit decisions to support this reading and concludes that, because Plaintiffs never assert Apple took an affirmative action to circumvent YouTube's TPMs, Apple's alleged behavior does not qualify as impermissible circumvention under the statute.

Apple's textual argument is unconvincing. As an initial matter, canons of statutory construction should be applied only to ambiguous text. *See e.g., Iancu v. Brunetti*, 588 U.S. 388, 397 (2019) (noting canons of statutory construction apply "only when ambiguity exists"). Here, Congress is clear: to circumvent, as used in § 1201(a), means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure." 17 U.S.C. § 1201(a)(3)(A). Though expansive, this definition is not ambiguous. As such, there is no need to interpret Congress' intent.

Nevertheless, were it appropriate, efforts to interpret Congress' intent beyond the plain meaning of the text could just as naturally yield an opposite conclusion. For example, Congress may have defined "circumvent" differently in § 1201(a) and § 1201(b) because each provision targets different bad behaviors to protect different rights. The former prohibits circumventing access controls specifically, protecting the right to control access to a copyrighted work, while the latter prohibits producing tools "primarily designed" to circumvent measures meant to protect a copyright holder's rights generally. *Id.* at § 1201(b)(2)(A). As even Apple highlights, "Congress intentionally" differentiated between provisions regulating access controls and provisions regulating the broader category of use controls "to maintain the balance between the rights of authors and the public interest." Dkt. 35, at 5 (citing U.S. COPYRIGHT OFF., THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998: U.S. COPYRIGHT OFF. SUMMARY 3–4 (Dec. 1998)). Applying that logic here, Congress may have determined the "balance between the rights of authors and the public interest" demands narrower behavior prohibitions when it comes to a copyright holder's entire bundle of rights and broader behavior prohibitions when it comes to a copyright holder's specific right to control access. *See id.* Whatever its motivation, Congress' choice to provide two different, equally clear definitions for two different statutory provisions does not require more than reading and applying the text, plainly understood, of each.

The differences between the present matter and the cases Apple cites to support its textual analysis do not vindicate Apple's argument. In all such cases, the defendant accessed copyrighted work through authorized channels. *See World Cable Inc.*, 893 F.Supp. 2d at 466 ("Defendants use of the normal process to decrypt the satellite signal did not avoid or bypass the conditional access system because they used the intended mechanism... in precisely the manner in which they were designed to function."); *see also LivePerson, Inc.*, 83 F.Supp. 3d at 509 ("Plaintiff alleges that Defendant already had [authorized] access to its backend system pursuant to Defendant's business relationship with Plaintiff" (emphasis added)); *Adobe Sys. Inc.*, 2015 WL 13022288, at *8 ("The serial license keys originated from Adobe and function precisely as intended.... To the extent there is any 'circumvention,' it is occasioned by Defendants' allegedly unauthorized distribution of

otherwise genuine and valid serial license keys.”). Because the defendants had authorized access, the ruling courts did not have to grapple with whether a given behavior constituted circumvention under § 1201(a). In contrast, Apple’s alleged “replicat[ing], spoof[ing],... reus[ing],” “regenerat[ing],” “cycling,” “bypass[ing],... “evad[ing],” “avoid[ing],” and “impair[ing]” looks significantly more like the illicit behavior considered in *VidAngel* and squarely satisfies the definition of circumvention laid out in § 1201(a)(3)(b). Dkt. 29, at ¶¶ 72, 115, 113, 102, 110, 57.

Moreover, and despite Apple’s protests, Plaintiffs *did* plead facts sufficient to conclude Apple circumvented YouTube’s TPMs, even under Apple’s constricted interpretation. First, Plaintiffs allege Apple used specific descrambling tools—yt-dlp or its equivalent—to bypass the rolling cipher and access the file URLs, which exist outside the authorized playback environment. This allegation alone overcomes Apple’s motion to dismiss: YouTube’s rolling cipher protects every file URL, and Apple’s tool descrambled that protective measure to access the copyrighted work. This scenario, adequately pled, makes out § 1201(a) circumvention claim.

Of course, that is not the only TPM Apple allegedly circumvented. Plaintiffs claim Apple rotated IP addresses to avoid YouTube’s IP-based monitoring and blocking system. They next assert Apple obtained fresh authorization parameters and regenerated valid links to evade YouTube’s session-bound, short-lived URLs—the only URLs users may validly use to access YouTube videos. Apple allegedly also used fresh authorization parameters and regenerated valid links to overcome YouTube’s session-bound restrictions. Finally, Plaintiffs claim Apple “extracted, replicated, spoofed, or reused token parameters outside the authorized” playback environment to evade detection. Dkt. 46, Pl.’s Opp. to Mot. to Dismiss, at 23. Each alleged behavior constitutes an “affirmative action against the alleged technological measures,” satisfying even Apple’s narrow conception of ¶ 1201(a). At this stage of litigation, Ted does not need to identify each specific process or tool Apple employed; rather, Ted’s allegations identifying scraping tools and tactics Apple plausibly could have employed to circumvent YouTube’s TPMs are sufficient to survive a motion to dismiss.

V. CONCLUSION

For the foregoing reasons, Defendant's motion to dismiss is denied.

IT IS SO ORDERED.

Dated: October 9, 2026



RICHARD SEEBORG
United States District Judge