

Rohit D. Nath (CA SBN 316062)
Michael Gervais (CA SBN 330731)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, California 90067
rnath@susmangodfrey.com
mgervais@susmangodfrey.com

Max Lalon Tribble, Jr (CA SBN 326851)
Justin Nelson (*pro hac vice* forthcoming)
SUSMAN GODFREY L.L.P.
1000 Louisiana Avenue, Suite 5100
Houston, Texas 77002
mtribble@susmangodfrey.com
jnelson@susmangodfrey.com

Rom Bar-Nissim (SBN 293356)
Rom@HeahBarNissim.com
HEAH BAR-NISSIM LLP
1801 Century Park East, Suite 2400
Los Angeles, California 90067
Telephone: (310) 432-2836

Attorney for Plaintiffs and the Proposed Class

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA**

TED ENTERTAINMENT, INC., MATT
FISHER, and GOLFHOLICS, INC., each
individually and on behalf of all others
similarly situated,

Plaintiffs,

v.

APPLE INC.,

Defendant

Case No. 3:26-CV-02936-RS

**PLAINTIFFS' OPPOSITION TO
APPLE'S MOTION TO DISMISS**

JURY TRIAL DEMANDED

TABLE OF CONTENTS

INTRODUCTION	1
BACKGROUND	3
I. The Digital Millennium Copyright Act and Section 1201(a).	3
II. YouTube’s Access Restrictions.	5
III. Apple's Circumvention of YouTube's Access Restrictions.....	6
LEGAL STANDARD	6
ARGUMENT	7
I. Plaintiffs Have Alleged Circumvention of Access Controls Under Section 1201(a)	7
a. Plaintiffs Have Alleged TPMs that Effectively Control Access to Their Works	7
b. YouTube’s TPMs Are Access Controls Even If They Do Not Prevent Users from Viewing the Works on YouTube’s Platform	10
c. YouTube’s TPMs Can Be Both Access and Use Controls	12
d. Courts Have Uniformly Rejected Apple’s Arguments About YouTube’s Measures After <i>VidAngel</i>	15
II. Apple’s “Ordinary Course” Argument Fails.....	16
III. Plaintiffs Adequately Allege that Apple Circumvented the Technological Measures .	22
IV. Plaintiffs’ Requested Relief is Proper Under 17 U.S.C. § 1203	24
CONCLUSION	25

TABLE OF AUTHORITIES**Page(s)****Cases**

<i>Adobe Sys. Inc. v. A&S Elec., Inc.</i> , 2015 WL 13022288 (N.D. Cal. Aug. 19, 2015).....	23
<i>Apple Inc. v. Psystar Corp.</i> , 658 F.3d 1150 (9th Cir. 2011).....	24
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662 (2009).....	6
<i>Ass’n for Info. Media & Equip. v. Regents of the Univ. of Calif.</i> , 2012 WL 7683452 (C.D. Cal. Nov. 20, 2012).....	14, 15
<i>CDK Global, LLC v. Tekion Corp.</i> , 2025 WL 1939951 (N.D. Cal. July 15, 2025).....	4
<i>Cordova v. Huneault</i> , 817 F.Supp.3d 819 (N.D. Cal. Jan. 23, 2026).....	2, 15, 16
<i>CouponCabin LLC v. Savings.com, Inc.</i> , 2016 WL 3181826 (N.D. Ind. June 8, 2016)	21, 22
<i>Craigslist, Inc. v. Naturemarket, Inc.</i> , 694 F.Supp.2d 1039 (N.D. Cal. 2010)	21
<i>Disney Enterprises, Inc. v. VidAngel, Inc.</i> , 869 F.3d 848 (9th Cir. 2017).....	<i>passim</i>
<i>Edland v. Basin Elec. Power Coop.</i> , 2021 WL 3080225 (D.S.D. July 21, 2021)	2, 16
<i>Green v. United States Dep’t of Just.</i> , 111 F.4th 81	4, 5
<i>Hattler v. Ashton</i> , 2017 WL 11634742 (C.D. Cal. Apr. 20, 2017)	13, 14
<i>hiQ Labs, Inc. v. LinkedIn Corp.</i> , 31 F.4th 1180, 1197 (9th Cir. 2022)	15
<i>I.M.S. Inquiry Mgmt. Sys. Ltd. v. Berkshire Info. Sys., Inc.</i> , 307 F.Supp.2d 521 (S.D.N.Y. 2004).....	24
<i>In re OpenAI</i> , 2025 WL 3635559 (S.D.N.Y. Dec. 15, 2025)	18

1	<i>Justice v. Suno, Inc.</i> ,	
2	2026 WL 2445362 (D. Mass. Aug. 20, 2026).....	2, 14
3	<i>Justice v. Uncharted Labs, Inc.</i> ,	
4	2026 WL 1430232 (S.D.N.Y. May 21, 2026).....	2, 15
5	<i>Koala v. Khosla</i> ,	
6	931 F.3d 887 (9th Cir. 2019).....	6
7	<i>Lasica v. AOL, Inc.</i> ,	
8	2015 WL 12791495 (C.D. Cal. Sept. 3, 2015).....	14
9	<i>Lexmark Int’l, Inc. v. Static Control Components, Inc.</i> ,	
10	387 F.3d 522 (6th Cir. 2004).....	18, 19
11	<i>MDY Indus., LLC v. Blizzard Ent., Inc.</i> ,	
12	629 F.3d 928 (9th Cir. 2010).....	<i>passim</i>
13	<i>Project Travel, LLC v. Terra Dotta, LLC</i> ,	
14	2026 WL 890422, at *7 (M.D. Fla. Apr. 1, 2026)	15
15	<i>Reddit v. SerpApi</i> ,	
16	2026 WL 2210094, at *3, *16 (S.D.N.Y. July 31, 2026)	21
17	<i>Sony Music Ent. v. Uncharted Labs Inc.</i> ,	
18	2026 WL 1019199 (S.D.N.Y. Apr. 15, 2026).....	2, 15, 16
19	<i>Ted Entertainment, Inc., et al. v. Snap, Inc.</i> ,	
20	2435349, at *1 (C.D. Cal. Aug. 19, 2026)	<i>passim</i>
21	<i>Ticketmaster L.L.C. v. Prestige Ent., Inc.</i> ,	
22	306 F.Supp.3d 1164 (C.D. Cal. 2018).....	6, 21
23	<i>Ticketmaster L.L.C. v. RMG Techs., Inc.</i> ,	
24	507 F.Supp.2d 1096 (C.D. Cal. 2007).....	21
25	<i>UMG Recordings v. Suno Inc.</i> ,	
26	2026 WL 2410184, at *5 (D. Mass. Aug. 18, 2026).....	2, 11, 23
27	<i>Yout, LLC v. Recording Indus. Ass’n of Am., Inc.</i> ,	
28	633 F.Supp.3d 650 (D. Conn. Sep. 30, 2022)	2, 10, 16
	Statutes	
	17 U.S.C. § 101	11
	17 U.S.C. § 1201(a)	<i>passim</i>
	17 U.S.C. § 1201(a)(1)(A)	4, 13

1	17 U.S.C. § 1201(a)(3).....	3
2	17 U.S.C. § 1201(a)(3)(A)	4, 22, 24
3	17 U.S.C. § 1201(a)(3)(B).....	<i>passim</i>
4	17 U.S.C. § 1201(d)	4
5	17 U.S.C. § 1203	24
6	Copyright Act.....	11
7	Digital Millennium Copyright Act.....	<i>passim</i>
8	Rules	
9		
10	Fed. R. Civ. P. 8	8, 16
11	Fed. R. Civ. P. 12(b)(6).....	6
12	Regulations	
13	37 C.F.R. 201.40(b)(1)(i)(A)	5
14	Other Authorities	
15	H.R. Rep. No. 105-551(I).....	3
16	H.R. Rep. No. 105-551 (II)	4
17	H.R. Rep. No. 105-551(II), (1998).....	12
18	<i>Report of the Register of Copyrights</i> (June 2017).....	<i>passim</i>
19	S. Rep. No. 105-190	3
20		
21		
22		
23		
24		
25		
26		
27		
28		

INTRODUCTION

Eight courts have considered and rejected the same arguments that Apple raises here: that YouTube’s technological measures cannot constitute access controls under 17 U.S.C. § 1201(a). *Infra* p.3 & n.1. Apple offers no reason for this Court to break from this line of authority, and its Motion should be denied.

Plaintiffs, three prominent YouTube creators, allege that Apple violated 17 U.S.C. § 1201(a) when it picked digital locks designed to prevent users from accessing audiovisual files outside of YouTube’s authorized streaming environment. AC ¶¶ 19–25; 58–73; 100–122. YouTube allows human users to view works through a controlled stream, but does not permit any user to download copies of the underlying video file or to view them outside of YouTube’s platform. *Id.* ¶¶ 42–46; 76–80. YouTube employs a series of technological measures to control access to video files. *Id.* ¶¶ 39–40; 42–67. These measures require a user’s browser to present credentials—akin to an access code—that confirm that the user seeks to access the file using a browser and YouTube’s authorized video player. *Id.* ¶¶ 47–52; 65–66; 71–73. YouTube also monitors unusual activity and automatically revokes access—or presents CAPTCHA challenges—when a user is engaged in bot- or scraping-related activity. *Id.* ¶¶ 52; 61–70. The Complaint alleges that Apple circumvented these technological measures using a tool to create bootleg credentials—this allowed Apple to get unauthorized access to videos by masquerading as a normal YouTube user—and by rotating IP addresses. *Id.* ¶¶ 100–122. These allegations present a straightforward, plausible violation of Section 1201(a), which proscribes any “circumvent[ion] of a “technological measure” that “effectively controls access” to a copyrighted work.

Apple’s lead argument is that YouTube’s technological measures do not effectively control access because YouTube users can watch videos through its authorized ad-supported streaming platform. Motion at 12–16. The Ninth Circuit rejected this argument in *Disney Enterprises, Inc. v. VidAngel, Inc.*, 869 F.3d 848 (9th Cir. 2017). *VidAngel* involved the circumvention of technological measures that provided exactly the type of “conditional” access that Apple claims is categorically excluded from Section 1201(a) protection—that is, one that allows users to view works through an authorized mechanism, but prevents a user from accessing the work in other

ways. *Id.* at 864. The *VidAngel* decision addressed whether a purchaser of DVDs—who, like YouTube users, could watch material through authorized means (*i.e.*, widely available DVD players)—violated Section 1201(a)(1) by decrypting the DVD’s encryption that controlled access to the underlying audiovisual files. The Court answered yes, holding that “us[ing] ... software to decrypt the TPMs to obtain a digital copy” of the underlying video file “is exactly like ‘breaking into a locked room in order to obtain a copy of a [movie]’” and violated Section 1201(a). *Id.* at 864-65. It added: “[n]othing in the legislative history suggests that VidAngel did not circumvent an access control simply because there are authorized ways to access the Studios’ works.” *Id.* at 865. That the DVD purchaser in *VidAngel* could already watch the film made no difference, and here, it makes no difference that ordinary YouTube users can watch Plaintiffs’ videos—least of all on a motion to dismiss.

Since *VidAngel*, courts have, over and over again, denied motions to dismiss in Section 1201(a) cases about the same YouTube measures at issue here. Consider *Ted Entertainment, Inc., et al. v. Snap, Inc.*, a case involving the Plaintiffs here and decided just days ago. 2026 WL 2435349, at *1 (C.D. Cal. Aug. 19, 2026). There, Judge Birotte rejected Snap’s argument that the “asserted TPMs are only ‘copy controls,’ not access controls,” and held that the complaint adequately alleged that YouTube’s TPMs “control access to the work[s] by ensuring access only through the permitted channel: the YouTube streaming architecture.” *Id.* at *4, 5. The previous day, Judge Saylor reached the same conclusion in *UMG Recordings v. Suno Inc.*, holding that Suno’s access vs. use control argument “cannot be resolved on the pleadings.” 2026 WL 2410184, at *5 (D. Mass. Aug. 18, 2026). In fact, every court that has addressed YouTube’s technological measures post-*VidAngel* rejected Apple’s arguments here.¹ At least eight separate decisions have considered and rejected Apple’s exact arguments, and Apple offers no reason why any of those courts were wrong.

¹ See *Justice v. Suno, Inc.*, 2026 WL 2445362, at *4 (D. Mass. Aug. 20, 2026); *Sony Music Ent. v. Uncharted Labs Inc.*, 2026 WL 1019199, at *3 (S.D.N.Y. Apr. 15, 2026); *Justice v. Uncharted Labs, Inc.*, 2026 WL 1430232, at *3 (S.D.N.Y. May 21, 2026); *Cordova v. Huneault*, 817 F.Supp.3d 819, 833–35 (N.D. Cal. Jan. 23, 2026); *Edland v. Basin Elec. Power Coop.*, 2021 WL 3080225, at *6 (D.S.D. July 21, 2021); *cf. Yout, LLC v. Recording Indus. Ass’n of Am., Inc.*, 633 F.Supp.3d 650, 676 (D. Conn. Sep. 30, 2022).

Nor does Apple’s discussion of “black boxes” and “glass boxes” move the needle. Nothing in Section 1201(a) or any of the cases interpreting it have incorporated Apple’s extended metaphor. The metaphor actually hurts Apple’s case, because the Complaint alleges technological measures that function as the type of “black box” that Apple admits is subject to Section 1201(a). Without satisfying the “rolling cipher” or providing proof-of-origin tokens, a user is denied any ability to stream a video. AC ¶¶ 58–75. That is the kind of “black box” that even Apple acknowledges satisfies Section 1201(a).

Apple’s remaining two arguments fare no better. That YouTube’s user authentication processes run in the background, rather than a direct prompt visible to the user, is irrelevant; the statute asks only whether the measure “requires the application of information, or a process or treatment . . . to gain access to the work.” 17 U.S.C. § 1201(a)(3). As Judge Birotte recognized in *Snap*, nothing in Section 1201(a) requires a user to “affirmatively interact with a visible barrier.” 2026 WL 2435349 (C.D. Cal. Aug. 19, 2026). And Apple’s argument that Plaintiffs fail to allege circumvention is equally meritless—the Complaint alleges that Apple used specific tools, like yt-dlp, to systematically pick YouTube’s digital locks.

At this stage, Plaintiffs need only plausibly allege that their works are protected by a “technological measure” that “effectively controls access,” and that Apple circumvented it to reach the works. Plaintiffs allege that Apple used descrambling tools, IP rotation, and automated workflows to defeat YouTube’s access protections and extract the underlying files of Plaintiffs’ works and many others. AC ¶¶ 85–120. As courts have consistently held in other cases about the same YouTube technological measures, these allegations easily state a claim for relief.

BACKGROUND

I. The Digital Millennium Copyright Act and Section 1201(a).

Congress enacted the DMCA to “create[] the legal platform for launching the global digital on-line marketplace for copyrighted works,” S. Rep. No. 105-190, at 8, and to “ensure a thriving electronic marketplace for copyrighted works on the Internet.” H.R. Rep. No. 105-551(I), at 9–10; *see also id.* at 10 (“When copyrighted material is adequately protected in the digital environment, a plethora of works will be distributed and performed over the Internet.”). Without protection,

1 “copyright owners will hesitate to make their works readily available on the Internet.” Congress
 2 therefore “‘backed with legal sanctions’ copyright owners’ use of ‘digital walls’ to protect their
 3 copyrighted works from piracy.” *Green v. United States Dep’t of Just.*, 111 F.4th 81, 89 (citation
 4 omitted). Those walls, called technological protection measures, or “TPMs,” limit both use of
 5 copyrighted works and access to them. *Id.*

6 Section 1201(a)(1)(A) provides that “[n]o person shall circumvent a technological measure
 7 that effectively controls access to a work protected under this title.” 17 U.S.C. § 1201(a)(1)(A).
 8 The statute defines “circumvention” as “to descramble a scrambled work, to decrypt an encrypted
 9 work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure,
 10 without the authority of the copyright owner.” *Id.* § 1201(a)(3)(A). And a measure “effectively
 11 controls access to a work” when it, “in the ordinary course of its operation, requires the application
 12 of information, or a process or a treatment, with the authority of the copyright owner, to gain
 13 access to the work.” *Id.* § 1201(a)(3)(B).

14 Section 1201(a) creates “a new anti-circumvention right” in favor of copyright owners that
 15 is “independent” of a copyright-infringement claim. *See MDY Indus., LLC v. Blizzard Ent., Inc.*,
 16 629 F.3d 928, 946 (9th Cir. 2010). Congress recognized that “the digital environment poses a
 17 unique threat to the rights of copyright owners” and that Section 1201(a) was needed to “mitigate
 18 the problems presented by copyright enforcement in the digital age.” *CDK Global, LLC v. Tekion*
 19 *Corp.*, 2025 WL 1939951, at *8 (N.D. Cal. July 15, 2025).

20 Congress understood that Section 1201(a) could sweep in some non-infringing fair uses
 21 along with the piracy it targeted. H.R. Rep. No. 105-551 (II), at 35-36, 41. For this reason,
 22 Congress built in statutory and regulatory exemptions. *See, e.g.*, 17 U.S.C. § 1201(d). And
 23 Congress created a rulemaking process to keep pace with the ever-changing nature of technology.
 24 “Under Section 1201(a)(1)(C), the Librarian of Congress conducts a triennial rulemaking
 25 proceeding to grant new exemptions to people who are likely to be ‘adversely affected’ by the
 26 anticircumvention provision in their ability to make noninfringing fair uses of copyrighted
 27
 28

materials.” *Green*, 111 F.4th at 90.² No exemption covers mass circumvention to download millions of YouTube videos for commercial use. Apple has neither sought nor received such an exemption.

II. YouTube’s Access Restrictions.

YouTube illustrates how Section 1201(a)’s balance fostered the “thriving electronic marketplace” Congress intended. Rightsholders—from major record labels to independent creators like Plaintiffs—upload content for streaming and rely on YouTube’s ad-supported model for revenue. AC ¶¶ 32–38.

YouTube attracts creators because they retain control through its content-sharing process: they can upload content for streaming through the authorized, ad-supported player while controlling how it is viewed and used. AC ¶ 34. Its Terms of Service prohibit users from “access[ing], reproduc[ing], download[ing], distribut[ing], transmit[ing], broadcast[ing], display[ing], sell[ing] licens[ing], alter[ing], modify[ing], or otherwise us[ing] any part of the Service or any Content except: (a) as expressly authorized by the Service; or (b) with prior written permission from YouTube and, if applicable, the respective rights holders.” *Id.* ¶ 76. Non-Premium viewers pay with attention to advertisements, while Premium subscribers pay money and creators receive a share based on Premium watch time. *Id.* ¶¶ 36–37. Creators therefore expect no uncompensated access outside of YouTube’s authorized players.

The Amended Complaint alleges at least five TPMs—the rolling cipher, IP-based blocking and rate limiting, session-bound, short-lived URLs, CAPTCHA challenges, and proof-of-origin tokens—that enforce YouTube’s Terms of Service and protect the underlying files. *Id.* ¶¶ 3, 44–49, 52–75. Together they form interlocking “digital walls” around the files on YouTube’s servers. The TPMs are described below. *See infra* at 9.

² Notable exemptions include, for example, an exemption that allows the circumvention of TPMs for the purpose of excerpting “short portions of . . . motion pictures . . . [f]or the purpose of criticism or comment . . . [f]or use in documentary filmmaking” or other films where the motion picture clip is used in parody or for its biographical or historically significant nature.” (codified at 37 C.F.R. 201.40(b)(1)(i)(A)).

1 **III. Apple's Circumvention of YouTube's Access Restrictions.**

2 Plaintiffs allege that Apple affirmatively and deliberately circumvented YouTube's TPMs
 3 to gain unauthorized access to underlying data files otherwise inaccessible to the public. AC ¶¶
 4 85–99. It systematically scraped millions of copyrighted videos to feed, train, improve, and
 5 commercialize its generative AI model, Apple AI Video, which allows users to generate videos
 6 from text and image prompts. AC ¶ 89. On information and belief, Apple used several tools and
 7 methods to do so, such as yt-dlp and IP rotation. *Id.* ¶¶ 105–113. Descrambling tools like yt-dlp
 8 automate stream ripping – a process that involves automatically accessing audio and visual files
 9 directly from a website's servers rather than viewing content through the site's authorized player
 10 – by deciphering YouTube's rolling cipher and extracting the underlying files from YouTube's
 11 servers. *Id.* ¶¶ 100–103, 105–108, 120. IP rotation uses virtual machines to cycle through IP
 12 addresses and evade blocking and monitoring. *Id.* ¶¶ 109–113. Automated activity circumvented
 13 CAPTCHA challenges and kept access alive despite session-bound, short-lived URLs. *Id.* ¶¶ 115–
 14 116. Apple could not have extracted millions of videos without circumventing YouTube's TPMs.
 15 *Id.* ¶ 100. Through circumvention, Apple gained unauthorized access to Plaintiffs' and the putative
 16 Class's content. *Id.* ¶¶ 86, 118–119. Scraping generated no advertising impressions or revenue
 17 (AC ¶ 127), no Premium watch time or subscription allocation (AC ¶ 128), and no view counts,
 18 watch time, or algorithmic signals (AC ¶ 130). It also displaced the market for the works (AC ¶
 19 131) and deprived creators of control over their files (AC ¶ 132).

20 **LEGAL STANDARD**

21 On a motion to dismiss under Rule 12(b)(6), a court must “accept the complaint's well-
 22 pleaded factual allegations as true, and construe all inferences in the plaintiff's favor[.]” *Koala v.*
 23 *Khosla*, 931 F.3d 887, 894 (9th Cir. 2019) (citation omitted). “[T]here are no heightened pleading
 24 requirements for a DMCA circumvention claim. [A plaintiff] only needs to allege facts that,
 25 accepted as true, ‘state a claim to relief that is plausible on its face.’” *Ticketmaster L.L.C. v.*
 26 *Prestige Ent., Inc.*, 306 F.Supp.3d 1164, 1174 (C.D. Cal. 2018) (quoting *Ashcroft v. Iqbal*, 556
 27 U.S. 662, 678 (2009)).
 28

ARGUMENT

I. Plaintiffs Have Alleged Circumvention of Access Controls Under Section 1201(a)

Apple argues that the alleged technological measures are not “access” controls under Section 1201(a) because they “form a glass box that (aims to) prevent unauthorized downloading but does nothing to stop access.” Motion at 13 (emphasis omitted). This is a mischaracterization of the allegations of the Complaint and a misstatement of the law. The technological measures alleged in the Complaint control all forms of access—both unauthorized streaming *and* downloading—and ordinary users encounter (and must satisfy) these same access controls when they watch YouTube videos. Furthermore, a rightsholder does not relinquish protection under Section 1201(a) simply because she has offered an authorized, controlled means of accessing her work. That is the law of this circuit after *VidAngel*. Read in any light—and certainly the light most favorable to the Plaintiffs—the Complaint easily alleges access controls under Section 1201(a).

a. Plaintiffs Have Alleged TPMs that Effectively Control Access to Their Works

The DMCA provides that “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.” 17 U.S.C. § 1201(a)(3)(B). Plaintiffs allege that is how YouTube’s TPMs work. Before anyone can access Plaintiffs’ works—whether to view those works on YouTube’s streaming platform *or* to reach the underlying video file—users first encounter a variety of gatekeeping mechanisms that they must satisfy through the application of information. Those TPMs are the “rolling cipher,” the “proof-of-origin” tokens, and the short-lived, session-bound URLs. AC ¶¶ 52, 58–60, 65–66, 71–75. YouTube also employs TPMs that can *revoke* access to YouTube if it suspects suspicious activity—like Apple’s “[l]arge-scale scraping operations.” *Id.* ¶ 68. Those TPMs are called “IP blocking” and “CAPTCHA challenges.” *Id.* ¶¶ 61–64, 67–70.

First, the “rolling cipher.” The “rolling cipher” is, in effect, a digital lock that constantly changes its combination. As Plaintiffs allege, YouTube maintains two URLs for each video: a page URL for streaming, and a file URL for the underlying file. AC ¶ 59. The file URL is encrypted with a complex, periodically changing algorithm called the rolling cipher. *Id.* To play a video,

1 users must receive a “client,” *i.e.* YouTube’s player software. *Id.* ¶ 58. Sent to the browser, that
 2 software uses a decryption routine to authenticate requests and as a proxy to confirm that the
 3 request originates from YouTube’s streaming environment. *Id.* The user can watch a video only if
 4 the rolling cipher is satisfied.

5 **Second**, proof-of-origin tokens similarly control access. YouTube’s official player
 6 generates session-tied tokens that accompany file requests, and servers validate them before
 7 delivering the stream. AC ¶ 71. Because proof-of-origin tokens are generated exclusively within
 8 YouTube’s authorized player environment, software operating outside that environment cannot
 9 obtain valid tokens through ordinary means. *Id.* ¶¶ 71–72. To retrieve audiovisual files at scale,
 10 automated scraping tools must therefore extract, replicate, or spoof the token parameters required
 11 for server authentication. *Id.* ¶ 72. Proof-of-origin tokens thus effectively control access by
 12 conditioning delivery of copyrighted works on proof that the requester is operating within
 13 YouTube’s authorized playback environment. *Id.* ¶¶ 72–73.

14 **Third**, the remaining access controls—IP blocking and rate limiting, CAPTCHA
 15 challenges, and session-bound URLs—similarly control access to the works. AC ¶¶ 65–66.
 16 YouTube uses automated processes to detect bot-and-scrapers activity like Apple’s, and responds
 17 by blocking IP addresses and presenting CAPTCHA challenges. *Id.* ¶¶ 67–70. These mechanisms
 18 control access to the works because they block a user from watching—or from any other access—
 19 to the audiovisual works. *Id.* ¶¶ 65–74.

20 Plaintiffs’ detailed allegations are far above the threshold under Rule 8(a), as Judge Birotte
 21 held in *Snap*. *Snap* involved the same Plaintiffs, same alleged technological measures, and the
 22 same arguments raised in a motion to dismiss. As here, *Snap* argued that Plaintiffs failed to plead
 23 access controls because “their works are freely accessible” on YouTube, and that YouTube’s
 24 controls were designed to “restrict download access.” 2026 WL 2435349, at *4. The Court
 25 rejected these arguments, holding that the system “performs background authentication and
 26 authorization processes before granting access to a video, and continued access remains subject to
 27 additional technological restrictions.” *Id.* at *5.

1 As *Snap* recognized, YouTube’s TPMs resemble the access controls at issue in *VidAngel*.
 2 *Id.* The *VidAngel* plaintiffs had made their works available on DVDs and Blu-ray discs which
 3 contained encryption measures. 869 F.3d at 853. To access the disc’s contents, those encryption
 4 measures had to be decrypted. Only a DVD player from a licensed manufacturer could “lawfully
 5 decrypt [the] disc’s content, and then only for playback, not for copying.” *Id.* The defendant,
 6 VidAngel, circumvented the DVD’s encryption measures to access and copy the discs’ contents
 7 without using an authorized player. VidAngel argued—as Apple argues here—that purchasers
 8 could watch the movies on licensed DVD players, so they already had “access” and the DVD
 9 encryption measures were only a “copy control” governed by Section 1201(b), not an “access
 10 control” under Section 1201(a). The Ninth Circuit rejected the Defendant’s position and held that
 11 the DVD’s encryption measures were access controls. *Id.* at 865.

12 YouTube’s TPMs operate similarly to the encryption measures on DVDs. To stream a
 13 YouTube video, the rolling cipher must first be decrypted and YouTube’s servers must receive
 14 valid proof-of-origin tokens. Only YouTube’s player software contains the keys to descramble the
 15 rolling cipher and to provide the proof-of-origin tokens, just as only an authorized DVD player
 16 contained the keys to decrypt the DVD’s encryption measures. But even then, the ordinary user
 17 has only gained access to the webpage where the video playback occurs, not to the underlying
 18 video file, just as the ordinary user in *VidAngel* only gained access to the DVD’s contents for
 19 playback, not for copying or viewing on an unauthorized device. In both cases, the TPMs control
 20 access to the underlying video file even though authorized viewing remains possible. To gain
 21 access to the underlying video file, Apple, like VidAngel, had to circumvent YouTube’s TPMs.

22 Apple’s attempts to escape *VidAngel* are unavailing. Apple argues that, because YouTube
 23 delivers works in sequential segments, users have “access” to the works, likening segmented
 24 streaming to reading a book a single page at a time. MTD at 7 n.2. But this analogy proves
 25 Plaintiffs’ point. The segments are ephemeral: they “are retrieved through a separate authorized
 26 request and discarded after playback.” AC ¶ 45. “At no point during ordinary streaming does the
 27 viewer’s device hold the assembled work in a form the viewer can locate, open, copy, or export.”
 28 *Id.* The viewer never possesses the work, nor the ability to view them outside of the ad-supported

1 streaming environment—which generates revenue for creators. Congress enacted Section 1201(a)
2 to protect exactly this type of “on-demand” model. *See MDY*, 629 F.3d at 947.

3 Apple also argues that because the rolling cipher encrypts the file URL rather than the file
4 itself, it does not control “access to a work” as Section 1201(a) requires. MTD at 9–10, 19. But
5 the file’s URL is the only means by which one can gain access to the work itself from YouTube’s
6 servers. The statute does not require that the work itself be encrypted – only that a technological
7 measure “effectively controls access to a work.” *See* 17 U.S.C. §1201(a)(3)(B). A lock on a door
8 controls access to the room’s contents even though the contents themselves are not encrypted.

9 **b. YouTube’s TPMs Are Access Controls Even If They Do Not Prevent Users**
10 **from Viewing the Works on YouTube’s Platform**

11 Apple argues that, because Plaintiffs’ works are viewable on YouTube’s platform, users
12 “access Plaintiffs’ works,” and Section 1201(a) offers nothing more for the underlying video file.
13 MTD at 13. As discussed, Apple is wrong—Plaintiffs have alleged that YouTube employs TPMs
14 that require users to apply a process to gain *any* access to the works, including to stream.
15 Regardless, Plaintiffs do not even need to allege that YouTube’s TPM prevent a user from
16 streaming the work to assert a Section 1201(a) claim. They need only allege that YouTube’s TPMs
17 *effectively control* how the user accesses Plaintiffs’ works.

18 Start with the plain language of the statute. Apple’s reading of the DMCA does not align
19 with the words Congress used. The statute says “access”; not “perceive,” “view,” or “watch.” *See*
20 17 U.S.C. §1201(a)(3)(B). “Access” includes the “freedom or ability to obtain or make use of
21 something.” *See Access*, Merriam-Webster.com, [https://www.merriam-](https://www.merriam-webster.com/dictionary/access)
22 [webster.com/dictionary/access](https://www.merriam-webster.com/dictionary/access) (last visited Aug. 24, 2026); *see also Yout*, 633 F.Supp.3d at 664
23 (citing Merriam Webster and concluding that TPMs “that restrain a YouTube user’s freedom or
24 ability to access the location where downloadable files are stored and download them” are
25 plausibly access controls). That is exactly what Plaintiffs allege: that YouTube employed TPMs
26 restricting users’ “freedom or ability to obtain” (*i.e.* “access”) the underlying audiovisual files, and
27 that Apple circumvented those controls to “obtain[] millions of videos from YouTube’s platform.”
28

1 AC ¶ 159. Accessing the underlying file is accessing the work. Viewing it through an authorized
 2 player does not erase the copyright owner’s right to bar unauthorized access to the file.

3 Apple’s attempt to collapse the distinction between viewing a work through YouTube’s
 4 streaming player and possessing the underlying audiovisual file misreads both the Amended
 5 Complaint and the Copyright Act. Apple points to the Amended Complaint’s statement that the
 6 audiovisual works are “not . . . ‘files’ distinct from those works.” AC ¶ 54. But that allegation
 7 addresses a different point: it refutes any suggestion that the files Defendant obtained are
 8 something other than copyrighted works. It does not mean that streaming access to a work through
 9 an authorized player is the same as possessing a permanent, machine-readable copy of that work.
 10 The Copyright Act itself recognizes that a single “work” may be embodied in multiple “copies,”
 11 each of which may be subject to different access conditions. See 17 U.S.C. § 101 (defining
 12 “copies” as “material objects . . . in which a work is fixed”). *VidAngel* confirms the point: DVD
 13 purchasers had authorized access to the work through an authorized player, but the Ninth Circuit
 14 nonetheless held that circumventing the disc’s encryption to obtain the underlying digital file
 15 constituted circumvention of an access control. 869 F.3d at 864–65. As Judge Birotte recognized
 16 in *Snap*, *VidAngel*’s logic controls here: “the Ninth Circuit rejected the proposition that a work
 17 ceases to be protected by an access control merely because consumers have authorized means of
 18 accessing it, observing ‘[n]othing in the legislative history suggests that VidAngel did not
 19 circumvent an access control simply because there are authorized ways to access the [] works.’”
 20 *Snap*, 2026 WL 2435349, at *5; see also *UMG Recordings*, 2026 WL 2410184, at *3 (“[T]o
 21 qualify as an ‘access control,’ the measure does not have to prevent all access.”). That Plaintiffs’
 22 works can be streamed does not mean they are freely accessible by any means or in any form.

23 Further, Apple’s “black box” metaphor reads far too much into the statute and contravenes
 24 its very purpose. Section 1201(a) covers a measure that “effectively *controls* access,” not
 25 “effectively *prevents* access.” As the Ninth Circuit explained, “[t]he statutory definition of the
 26 phrase ‘effectively control access to a work’ does not require that an access control be strong or
 27 circumvention-proof. Rather, it requires an access control measure to provide some degree of
 28 control over access to a copyrighted work.” *MDY*, 629 F.3d at 954 n.17 (citation omitted). Nothing

1 in Section 1201(a) requires a rightsholder to put their works into an impenetrable “black box”; in
2 fact, Congress intended exactly the opposite. With Section 1201(a), Congress sought to
3 “encourag[e] copyright owners to make their works available” over the internet in new formats,
4 while offering a “legal framework to ensure they can protect their work from piracy.” *MDY*, 629
5 F.3d at 947. (quoting H.R. Rep. No. 105-551(II), at 23 (1998)). Congress clearly had in mind that
6 Section 1201(a) would not just encompass access controls that prevent users from viewing the
7 works (such as paywall), but also those that protect streamers from piracy (by preventing users
8 from accessing and downloading the underlying video file, even if they could otherwise *view* the
9 work by streaming it). If Section 1201(a) did not extend to this latter type of “access control,” then
10 copyright owners like Plaintiffs would never make their works available for on-demand
11 streaming—on YouTube or any streaming platform—contrary to Congress’s intent.

12 Finally, Apple quotes the Amended Complaint’s statement that the Terms of Service “grant
13 license ... to other users of YouTube to access content through YouTube’s services,” MTD at 6,
14 to argue that Plaintiffs’ works are publicly available. But the Terms of Service explain that the
15 license “does not grant any rights or permissions for a user to make use of [the] Content
16 independent of the Service.” AC ¶ 77. In other words, the Terms of Service grant permission to
17 stream content through the authorized player. They do not grant permission to reach through the
18 wall and take the underlying files. The Terms of Service therefore reinforce, rather than defeat,
19 Plaintiffs’ Section 1201(a) claim.

20 **c. YouTube’s TPMs Can Be Both Access and Use Controls**

21 Apple further argues that because the alleged TPMs restrict downloading, they are use
22 controls, not access controls. *See, e.g.*, MTD at 12–16. But this both mischaracterizes the
23 allegations of the Complaint and is wrong on the law. First, the Complaint alleges that the
24 contested TPMs control all forms of access, not solely downloading. Apple would still be liable
25 for a Section 1201(a) claim had it circumvented the rolling cipher, for example, to stream
26 Plaintiffs’ videos from YouTube’s servers outside of the authorized playback environment, an act
27 that would similarly deprive Plaintiffs of advertising revenue. That Apple downloaded videos
28 instead of watching them after it circumvented the TPMs makes no difference.

Second, the Ninth Circuit has squarely rejected Apple’s assertion that there is a rigid, unyielding, distinction between access controls governed by Section 1201(a) and use controls governed by Section 1201(b). In *VidAngel*, the Ninth Circuit explained that “the statute does not provide that a TPM cannot serve as both an access control and a use control. . . . [W]hen a defendant decrypts the TPMs and then also reproduces that work, it is liable for both circumvention in violation of § 1201(a)(1)(A) and copyright infringement in violation of § 106(1).” 869 F.3d at 864. Similarly, in *MDY*, the Ninth Circuit acknowledged that a TPM could “both (1) control[] access and (2) protect[] against copyright infringement.” 629 F.3d at 946; *Snap*, 2026 WL 2435349, at *6 (“[I]t is irrelevant that the rolling cipher may also restrict download access since the statute does not provide that a TPM cannot serve as both an access control and a use control.”). The DMCA does not force a copyright owner to label each measure either an “access control” or a “copy control.” Indeed, even the Copyright Office has its own term for TPMs that do both jobs at once: “merged access and copy controls.” See U.S. Copyright Office, *Section 1201 of Title 17: A Report of the Register of Copyrights*, at 126 (June 2017).³

Against this authority, Apple points to *Hattler v. Ashton*, 2017 WL 11634742 (C.D. Cal. Apr. 20, 2017), an unpublished decision that pre-dates *VidAngel*, for the proposition that where access is provided, violation of the conditions of use are not circumvention of an access control because access was already provided. MTD at 13. But *Hattler* involved remarkably sparse (in fact, completely nonexistent) allegations about the technological measures at issue. While the plaintiff claimed that the defendants “circumvented the technological measures on [Plaintiff’s] sites,” he did not allege *anything* about what those technological measures were, nor did he allege that users encountered those measures before accessing and copying his works. See Request for Judicial Notice (RJN), Ex. A (operative complaint from *Hattler*). Equally importantly, *Hattler* predates

³ In its report, the Copyright Office further wrote that “[a] few commenters proposed that in *the many cases where access controls and copy controls are merged*, the rulemaking should treat the inquiry into the adverse effects on noninfringing uses differently,” such that “obtaining an exemption” under the DMCA “should be easier where the TPM at issue is merged.” *Id.* at 126–127. The Office rejected this argument, noting that “[t]he Office believes that section 1201(a)(1) is best read as protecting the integrity of access controls even where prohibited conduct would not be infringing.” *Id.*

1 *VidAngel* (as does *Lasica*, addressed below) and to the extent *Hattler* is premised on the view that
 2 a rightsholder relinquishes all Section 1201(a) protection when she allows a person to view her
 3 work, it is obsolete. By contrast, post-*VidAngel*, courts—both in the Ninth Circuit and across the
 4 country—have uniformly denied motions to dismiss addressing the same Section 1201(a) claims
 5 and the same YouTube measures at issue in this case. *See, e.g., Snap*, 2026 WL 2435349, at *1;
 6 *Justice v. Suno, Inc.*, 2026 WL 2445362, at *4 (D. Mass. Aug. 20, 2026); *supra* p.4 & n.1.

7 *Lasica v. AOL, Inc.*, 2015 WL 12791495 (C.D. Cal. Sept. 3, 2015)—another case on which
 8 Apple relies—is a *tentative* order involving a Section 1201(b) claim, *not* a Section 1201(a) claim.
 9 *Id.* at *1, 5. Regardless, *Lasica* is distinguishable. There, the defendant had copied a photo from a
 10 photo-sharing website. *Id.* at *1. The plaintiff had not alleged that the website employed any TPM
 11 to control access to the photograph; the plaintiff had only alleged that the photograph was subject
 12 to a licensing agreement which “explicitly prohibited the use of the [photograph] for commercial
 13 purposes.” Amended Compl. and Demand for Jury Trial, *Lasica*, No. 2:15-cv-04230, 2015 WL
 14 6669503, at ¶¶ 8, 44 (July 14, 2015) (*see* Pls. Request for Judicial Notice, Ex. C). Here, by contrast,
 15 Plaintiffs allege that Apple was not just prohibited from accessing creators’ videos by YouTube’s
 16 Terms of Service, but also that YouTube employed TPMs designed to enforce its Terms of Service.

17 Apple also cites *Lasica* for the premise that a “person who engages in prohibited usage of
 18 a copyrighted work to which [they have] lawful access does not fall afoul of any provision of [§]
 19 1201.” *See* MTD at 14 (quoting *Lasica*, 2015 WL 12791495, at *5). In other words, Apple argues
 20 that because it had one form of authorized access to Plaintiffs’ works (the ability to view them on
 21 YouTube), it could not run afoul of any provision of Section 1201. But *Lasica* relies on *Ass’n for*
 22 *Info. Media & Equip. v. Regents of the Univ. of Calif.*, 2012 WL 7683452, at *9 (C.D. Cal. Nov.
 23 20, 2012) for that premise, which is no longer good authority after *VidAngel*. There, the court held
 24 that the defendant did not violate Section 1201(a) when it circumvented technological measures
 25 on a DVD to copy its contents because the defendant already “had lawful access to the DVDs.”
 26 *Id.* at 9. *VidAngel* squarely rejected the argument that because a DVD-purchaser has “lawful”
 27 access to the DVD, it is “authorized . . . to decrypt [technological measures] to view the discs’

content.” 869 F.3d at 863. The Ninth Circuit said, “lawful purchasers have permission only to view their purchased discs with a DVD or Blu-Ray player licensed to decrypt the TPMs.” *Id.*⁴

The same logic applies here. The public has lawful access to view Plaintiffs’ works “through YouTube’s authorized streaming architecture” but it does not have permission to access the works in any other way—not to stream through a bootleg player and not to copy the underlying video files. *Snap*, 2026 WL 2435349, at *4 (C.D. Cal. Aug. 19, 2026). Just as the TPMs in *VidAngel* were designed to prevent the DVD purchaser from both viewing the DVD through an unlicensed mechanism *and* from accessing and reproducing the underlying video file saved on the DVD, here YouTube’s TPMs are designed to prevent users from viewing the videos outside of YouTube’s streaming platform *and* from accessing and reproducing the underlying video file. That YouTube’s access controls may *also* be use controls is no reason to dismiss Plaintiffs’ claims.

d. Courts Have Uniformly Rejected Apple’s Arguments About YouTube’s Measures After *VidAngel*

The case law confirms that Apple’s arguments are meritless. Unsurprisingly, and for many of the reasons addressed, district courts after *VidAngel* have uniformly rejected Apple’s arguments and denied motions to dismiss Section 1201(a) claims alleging circumvention of YouTube’s TPMs. *See Sony Music Ent. v. Uncharted Labs Inc.*, 2026 WL 1019199, at *3 (S.D.N.Y. Apr. 15, 2026) (the Complaint plausibly alleges that YouTube employs technological measures that regulate access to its content and that Defendant circumvented them Whether YouTube’s measures ultimately constitute access controls within the meaning of § 1201 requires a greater factual record than the pleadings contain,” citing *VidAngel*); *see also Justice v. Uncharted Labs, Inc.*, 2026 WL 1430232, at *3 (S.D.N.Y. May 21, 2026) (same); *Cordova*, 817 F. Supp. 3d at 832–35 (examining YouTube’s TPMs and denying the motion to dismiss); *Yout*, 633 F. Supp. 3d 650, 671 (“[T]he [complaint] suggests that YouTube’s technological measure is effective by alleging that YouTube has technology that functions to control access to downloadable files.”); *Edland*,

⁴ Apple’s other cited authorities are no more relevant. *Project Travel, LLC v. Terra Dotta, LLC*, involved a party who used a username and password as intended to gain access to information. 2026 WL 890422, at *7 (M.D. Fla. Apr. 1, 2026). And *hiQ Labs, Inc. v. LinkedIn Corp.*, is a CFAA case, not Section 1201(a). 31 F.4th 1180, 1197 (9th Cir. 2022); *see VidAngel*, 869 F.3d at 863 n.15 (declining to rely on CFAA authorities in interpreting Section 1201(a)).

2021 WL 3080225, at *6 (plaintiff “plausibly stated a claim for violation of [Section 1201(a)] of the DMCA” by alleging that the defendant “bypassed [YouTube’s] TPMs when it successfully, copied, reproduced, and distributed the [YouTube] Videos, all without [plaintiff’s] authorization”); *Snap*, 2026 WL 2435349, at *7 (“[T]he Court concludes that Plaintiffs have sufficiently alleged that each of the TPMs serve as access controls, not copy controls”).

In *Uncharted Labs*, for example, Judge Hellerstein addressed materially similar allegations about YouTube TPMs brought by major music labels and the same arguments in the defendant’s motion to dismiss. In denying the defendant’s motion to dismiss, he found that the complaint “plausibly alleges that YouTube employs technological measures that regulate access to its content and that Defendant circumvented Whether YouTube’s measures ultimately constitute access controls within the meaning of § 1201 requires a greater factual record than the pleadings contain.” 2026 WL 1019199, at *3. As in *Uncharted Labs*, the Complaint’s allegations are above and beyond the threshold under Rule 8 and the question of whether YouTube’s TPMs “effectively control access” to Plaintiffs’ works cannot be resolved on the pleadings.

Despite the mountain of relevant post-*VidAngel* precedent, Apple cites no post-*VidAngel* decision other than *Cordova* addressing YouTube’s TPMs. MTD at 20 n.10. But even there, Apple mischaracterizes *Cordova*. Apple incorrectly claims that *Cordova* treats any measure “intended to prevent unauthorized downloading” as an access control. MTD at 20 n.10. That is not what the court held; rather, the court explained that “measures that restrict *access to downloadable files*[] are sufficient for purposes of the second element of a § 1201(a)(1) claim.” *Cordova*, 817 F. Supp. 3d at 834. This Court should decline Apple’s request for an extraordinary departure from settled law to resolve this case on the pleadings, without any factual record or discovery.

II. Apple’s “Ordinary Course” Argument Fails

Given that YouTube’s TPMs are functionally identical to the access controls upheld in *VidAngel*, the Court should also reject Apple’s fallback argument about ordinary course. Apple claims that none of these measures are “access measures” because they “do not operate in the ordinary course.” MTD at 16-20. This is wrong.

For starters, Section 1201(a)(3)(B) covers a “technological measure” that “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.” The Complaint includes plausible, detailed allegations that users encounter YouTube’s TPMs in the ordinary course of using YouTube’s streaming service. Plaintiffs allege that “[v]iewing a work on YouTube . . . requires the application of a sequence of authorized processes, including the issuance and validation of session-specific tokens, execution of player-side instructions, and reconstruction of segmented media streams into a continuous audiovisual experience.” AC ¶ 51. Plaintiffs further allege that the rolling cipher is required “in the ordinary course of YouTube’s operation, for every playback of every video by every requestor” and that the servers never deliver files without a validly transformed signature. *Id.* ¶ 58. In short, the Complaint specifically alleges that the alleged technological measures require the application of information, process, or treatment—*i.e.*, information to satisfy the rolling cipher, or session-specific proof-of origin tokens—before the user gains any access to streaming of the work.

Apple argues that this is insufficient, because access controls require “some affirmative act such as entering a password.” Motion 16. But there is no support for this reading of Section 1201(a). As Judge Birotte held in *Snap*: “Nothing in § 1201(a) requires an access control to take the form of a paywall, password prompt, or other measure requiring affirmative user input. Rather, the statutory inquiry is whether the technological measure, ‘in the ordinary course of its operation,’ requires the application of authorized ‘information, or a process or a treatment’ to gain access to the work.” 2026 WL 2435349, at *4 (C.D. Cal. Aug. 19, 2026). The cases that Apple cites only reinforce why its argument is wrong. In *MDY*, for example, the Ninth Circuit addressed a bot-scanning software that automatically scanned a video game “player’s computer RAM” to “confirm the absence of any bots or cheats” before granting access to the online video game experience.⁵

⁵ The portion of *MDY* that Apple cites involve a situation not relevant here. There, the Court concluded that the bot-scanning software did not effectively control access to certain copyrightable elements—for example, certain visual images or sounds—that “could be accessed by a user without signing on to” the online game experience, and thus without encountering the bot-scanning software at all. *MDY*, 629 F.3d at 952. Here, Plaintiffs allege that YouTube users encounter the alleged technological measures in the ordinary course of viewing videos on YouTube.

1 The Court held that this was an effective access control measures that satisfied Section
 2 1201(a)(3)(B), even though the scanning software operated automatically and did not require any
 3 “affirmative act” from the player. *MDY*, 629 F.3d at 953-54.⁶

4 Apple’s invocation of the DVD encryption cases, like *VidAngel*, further undercuts its
 5 argument. MTD at 17-18. Apple may say DVDs are encrypted and YouTube videos are publicly
 6 accessible. But the Amended Complaint does not allege an open, available file. It alleges the
 7 opposite: “At no time is any audiovisual file available at a static, unsigned, publicly accessible
 8 location. Every request for audiovisual file data must present valid, unexpired, cryptographically
 9 signed parameters generated through YouTube’s authorized processes[.]” AC ¶ 59. The rolling
 10 cipher requires that signature transformation “in the ordinary course” for every playback of every
 11 video by every requester, and YouTube never streams the file without a validly transformed
 12 signature. AC ¶ 58. Session-bound URLs and proof-of-origin tokens impose additional access
 13 conditions. AC ¶¶ 65–66, 71-74. Those are locks of a different kind, but locks all the same.

14 Apple’s “front door/back door” argument from *Lexmark Int’l, Inc. v. Static Control*
 15 *Components, Inc.*, 387 F.3d 522 (6th Cir. 2004) fares no better. See MTD at 17-18. YouTube’s
 16 TPMs are different from those at issue in *Lexmark*. *Lexmark* made printers and toner cartridges.
 17 *Lexmark*, 387 F.3d at 530. The question in *Lexmark* was whether an authentication sequence was
 18 a technological measure that effectively controlled access to a Lexmark printer’s software, called
 19 the Printer Engine Program Code. *Id.* at 546–47. The Sixth Circuit said no, because a user did not
 20 need to encounter the authentication code to access the Printer Engine Program Code; anyone
 21 could “read the literal code of the Printer Engine Program directly from the printer memory, with
 22 or without the benefit of the authentication sequence.” *Id.* at 546. “No security device, in other
 23 words, protect[ed] access to the Printer Engine Program Code and no security device accordingly
 24 must be circumvented to obtain access to that program code.” *Id.* at 547.

25
 26 ⁶Nor does *In re OpenAI*, 2025 WL 3635559, at *4 (S.D.N.Y. Dec. 15, 2025), help Apple’s case.
 27 There, the plaintiff acknowledged that the proposed “access controls,” robots.txt directives, are
 28 “merely requests and do not effectively control access to copyrighted works.” *Id.* at *4. Apple
 also cites CFAA cases, Motion at 16, which have no bearing in interpreting Section 1201(a). See
VidAngel, 869 F.3d at 863 n.15.

1 That is nothing like this case. Here, there is no way for the ordinary user to access
 2 Plaintiffs’ works—whether to view on YouTube’s platform or to access the underlying video
 3 file—without encountering TPMs like the rolling cipher and proof-of-origin tokens. YouTube’s
 4 files are not sitting in an “open database.” They have cryptographic protections that must be
 5 overcome – or circumvented – before delivery. As *VidAngel* makes clear, the fact that YouTube
 6 offers an *authorized* way to view Plaintiffs’ works does not mean that Apple did not circumvent
 7 an access control when it circumvented YouTube’s TPMs to gain access to the underlying video
 8 file. *See VidAngel*, 869 F.3d at 864-865.

9 In addition to the rolling cipher, proof-of-origin tokens, and short-lived, session-bound
 10 URLs, YouTube also employs two measures—IP blocking and CAPTCHA challenges—that can
 11 *revoke* access to YouTube’s platform. As Plaintiffs allege, YouTube monitors network behavior
 12 and blocks IP addresses that exhibit patterns consistent with abusive behavior, so that the IP
 13 addresses lose access to the entire YouTube platform. AC ¶¶ 39, 61-64. IP rotation abandons the
 14 challenged address and resumes from a new one to circumvent IP blocking. YouTube also deploys
 15 CAPTCHA challenges (tests “often requiring identification of objects with grainy images”) when
 16 automated or suspicious activity is detected. *Id.* ¶¶ 67-70. These challenges “perform a
 17 gatekeeping function by prohibiting a certain type of user (a bot) from accessing the platform and
 18 the audiovisual works hosted on it.” *Id.* ¶ 67. YouTube deploys them when traffic looks automated
 19 or suspicious and denies continued streaming until the challenge is completed. Large-scale
 20 scraping necessarily triggers CAPTCHA challenges. *Id.* ¶ 68.

21 Apple argues that the CAPTCHA and IP blocking measures “discriminate between
 22 categories of users” rather than “control access.” MTD at 18. That is a distinction without a
 23 difference. The measures verify, throttle, challenge, or deny requesters, and the Plaintiffs allege
 24 that they were in place at *all* relevant times and that Apple could not have accessed the underlying
 25 files referenced in the datasets without circumventing them. AC ¶¶ 61–75. A measure that denies
 26 access to unauthorized users controls access. The Ninth Circuit has held that a measure need not
 27 be “strong or circumvention-proof” to effectively control access. *MDY*, 629 F.3d at 954 n.17.

1 Apple points out that CAPTCHA triggers only sometimes and that IP blocking follows
 2 “excessive or abusive” conduct. MTD at 18. But the Amended Complaint alleges that IP
 3 verification occurs at the outset of every request before any content is served and operates on every
 4 requestor, and that CAPTCHA and IP controls operate against the automatic activity alleged here.
 5 AC ¶¶ 58, 61, 63-70. Apple’s argument amounts to: “These measures were designed to stop
 6 entities like me from automatically scraping videos, but because they don’t affect typical users,
 7 they don’t count.” But that’s a misguided application of the DMCA. A burglar alarm operates in
 8 the ordinary course even when it stays silent for the homeowner.

9 Apple argues that neither CAPTCHA nor IP blocking count as access controls because
 10 they only “detect automated users who use YouTube’s service in allegedly ‘abnormal ways.’”
 11 MTD at 18. But the Ninth Circuit, in *MDY*, made clear that measures that *revoke* access can also
 12 be access controls under Section 1201(a). *MDY*, 629 F.3d at 943 (“[I]n our view, an access control
 13 measure can both (1) attempt to block initial access and (2) *revoke access* if a secondary check
 14 determines that access was unauthorized.”). *MDY* involved a TPM called “Warden,” which was
 15 designed to keep bots off World of Warcraft (“WOW”) servers. 629 F.3d at 942. Warden
 16 functioned by first “scan[ing] a [player’s] computer’s RAM prior to allowing the player to
 17 connect to WOW’s servers.” *Id.* If the Warden software detected a bot through that scan, it would
 18 not allow the player to connect and play. But if the bot was able to get through, Warden had a
 19 secondary component that ran “periodically in the background on a player’s computer when it is
 20 [was] connected to WOW’s servers” which “look[ed] for patterns of code associated with known
 21 bots or cheats.” *Id.* If Warden “detect[ed] a bot or cheat,” it would “boot[] the player from the
 22 game.” *Id.* The Ninth Circuit held that Warden was “an effective access control measure” with
 23 respect to certain copyrighted work. *Id.* at 945. YouTube, like Warden, monitors network behavior
 24 and employs TPMs, like IP blocking and CAPTCHA challenges that monitor behavior and will
 25 boot unauthorized users from the YouTube platform.

26 Indeed, Courts regularly recognize TPMs like CAPTCHA as access measures. *See, e.g.,*
 27 *Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F.Supp.2d 1096, 1112 (C.D. Cal. 2007) (“[B]ecause
 28 CAPTCHA ‘in the ordinary course of its operation, requires the application of information . . . to

gain access to the work,’ it is a technological measure that regulates access to a copyrighted work.”); *see also Ticketmaster v. Prestige*, 306 F.Supp.3d at 1174 (same); *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F.Supp.2d 1039, 1056 (N.D. Cal. 2010) (same). Judge Engelmayer’s recent decision in *Reddit v. SerpApi* is particularly on point. There, the court considered whether “SearchGuard,” a TPM used by Google, was an access control. SearchGuard works by “examin[ing] each [Google] search query to determine whether it is coming from a recognized or unrecognized source,” and “[i]f the source is unrecognized, SearchGuard sends a challenge or CAPTCHA that requires the browser to return information about the user generating the query.” 2026 WL 2210094, at *3, *16 (S.D.N.Y. July 31, 2026). The court concluded that SearchGuard was “a ‘process’ required ‘to gain access to the work,’” because “[i]t erects a gate between users and Google [search engine results pages], which, in the ordinary course, can be opened only by human users but which keeps out automated users,” and “thereby controls access . . . [by] restricting such access to human users who cannot engage in mass scraping of data.” *Id.* at *16 (citing *MDY*, 629 F.3d at 954). The same is true of YouTube’s CAPTCHA and IP blocking measures.

In the face of this authority, Apple relies on an out-of-circuit decision about grocery store coupons, *CouponCabin LLC v. Savings.com, Inc.*, 2016 WL 3181826, at *6 (N.D. Ind. June 8, 2016).⁷ But that case does not stand for the proposition that a measure that revokes access is not an access control under Section 1201(a). MTD at 16. In *CouponCabin*, the plaintiff had discovered “a marked increase in the amount of its unique content appearing on a number of competing websites,” and hired a security provider to block traffic “from certain . . . service providers identified as being used particularly heavily by the Defendants to conduct scraping activities.” *Id.* at *1, 3. In response, the defendants simply switched to other servers that hadn’t been blocked. *Id.*

⁷ Apple also cites a report from the U.S. Copyright Office that it claims “concluded that measures analogous to the alleged Automation Detectors ‘do not effectively control access to a work.’” MTD at 18. But the Copyright Office repeatedly emphasized the limited amount of information it had before it to assess whether IP address rotation systems effectively control access to a work. *See, e.g.*, Section 1201 Rulemaking: Ninth Triennial Proceeding Recommendation of the Register of Copyrights, at 125 (Oct. 2024) (“IP address rotation, *based on the thin record before the Office*, does not *appear* to involve the circumvention of an effective control”) (emphasis added).

1 at *6. The court dismissed the Section 1201(a) claim because the plaintiff's TPM was plainly
 2 ineffective, not because IP blocking is *per se* not an access control. *Id.* at *6. And even if
 3 *Couponcabin* could be read to stand for that proposition (it can't), it is neither binding on this court
 4 nor persuasive. The Ninth Circuit's decision in *MDY* is both.

5 Because YouTube's TPMs are precisely the type of measures that the Ninth Circuit already
 6 has held are access controls under Section 1201(a), Apple's arguments are meritless.

7 **III. Plaintiffs Adequately Allege that Apple Circumvented the Technological Measures**

8 Apple's final argument is that Plaintiffs fail to allege actual circumvention. Apple claims
 9 that the Amended Complaint is devoid of allegations that it affirmatively circumvented YouTube's
 10 TPMs because it simply walked through an "open back door." MTD at 17. Apple says it either
 11 never encountered the TPMs or simply used "valid" links and "valid" tokens. But the Amended
 12 Complaint alleges that Apple defeated YouTube's TPMs through tools and other measures to
 13 obtain the underlying files.

14 First, with respect to the Rolling Cipher, the Amended Complaint explains that Apple used
 15 descrambling tools like yt-dlp to defeat YouTube's rolling cipher and reach the underlying files
 16 outside of the authorized player. AC ¶¶ 105-108. That describes "descramble[ing] a scrambled
 17 work" or "decrypt[ing] an encrypted work." 17 U.S.C. § 1201(a)(3)(A).

18 Second, the Complaint explains that Apple rotated IP addresses so downloading could
 19 continue after YouTube detected and blocked an IP address. AC ¶¶ 109-113. The Amended
 20 Complaint explains why that matters: "Rotating IP addresses is not passive disregard of a
 21 technological measure; it is an affirmative technological act." *Id.* ¶ 110. "Each rotation
 22 manufactures and presents to YouTube's verification systems a new, artificial network identity,
 23 engineered so that a requestor that would ordinarily fail YouTube's IP verification is able to pass
 24 it instead. It is the digital equivalent of returning to a checkpoint in a fresh disguise bearing new
 25 credentials after having been turned away." *Id.*

26 Third, the Amended Complaint explains that Apple circumvented the session-bound, short-
 27 lived URLs by repeatedly obtaining fresh authorization parameters and regenerating valid links to
 28 keep access going despite the session-bound restrictions. AC ¶ 115. Generating file requests

1 outside the authorized player by replicating or extracting the parameters that YouTube’s player
2 generates is the type of conduct *VidAngel* condemned, *i.e.*, operating outside the authorized player
3 to reach the underlying files the TPM was designed to protect. AC ¶¶ 105-108.

4 The Amended Complaint further alleges that Apple’s large-scale scraping triggered
5 CAPTCHA challenges, and that Apple used IP rotation and distributed requests across multiple
6 machines to circumvent a CAPTCHA when it was triggered. AC ¶¶ 68-70; 112-116. These are
7 affirmative acts to “avoid” or “bypass” a TPM.

8 Finally, the Amended Complaint alleges that Apple extracted, replicated, spoofed, or
9 reused token parameters outside the authorized player to retrieve the underlying files. AC ¶¶ 71-
10 74, 117. Those are affirmative acts of circumvention. *Cf. VidAngel*, 869 F.3d at 864-65
11 (circumvention includes using technological tools to access content outside authorized channels,
12 regardless of whether the initial purchase was lawful).

13 These acts fit Section 1201(a)(3)(A)’s definition: “to descramble a scrambled work, to
14 decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a
15 technological measure.” Apple cannot turn these affirmative acts into passive non-encounters.

16 Moreover, “valid” credentials prove nothing by themselves. *UMG Recordings*, 2026 WL
17 2410184, at *5 (“Whether or not the user has permission to use the authorized process is not the
18 subject of §1201(a)(1)”). In *VidAngel*, the defendant also began with a valid means of access: it
19 lawfully purchased the DVDs. 869 F.3d at 854. The circumvention lay in using unauthorized tools
20 to operate outside the authorized player and reach the underlying files. The same is true here. Even
21 if Apple obtained “valid” URLs or token parameters, the Amended Complaint alleges that it
22 extracted or reused token parameters outside of their authorized context.

23 Apple relies on *Adobe Sys. Inc. v. A&S Elec., Inc.*, 2015 WL 13022288 (N.D. Cal. Aug.
24 19, 2015) for the proposition that using valid serial keys is categorically not circumvention. MTD
25 at 23-24. But in *Adobe*, the defendant distributed genuine, unmodified license keys that Adobe
26 itself had generated for authorized users. Here, by contrast, Apple did not simply enter a genuine,
27 unmodified password. It extracted, replicated, and repurposed authorization parameters generated
28 exclusively within YouTube’s authorized players and deployed them outside that environment

1 through automated tools. AC ¶¶ 71-74, 117. That is not “using an authorized password” – it is
 2 reverse-engineering the lock to forge a key. Apple’s reliance on *I.M.S. Inquiry Mgmt. Sys. Ltd. v.*
 3 *Berkshire Info. Sys., Inc.*, 307 F.Supp.2d 521, 532 (S.D.N.Y. 2004) is similarly misplaced. In
 4 *I.M.S.*, the defendant obtained a legitimate login credential from the plaintiff and used it as
 5 intended to access the plaintiff’s system. Here, Apple did not use the system as intended but instead
 6 used a variety of tools and methods to break the system. The Nimmer treatise passage Apple cites
 7 (§ 12A.06[C][5]) addresses a narrow scenario: “using an authorized password” given to another
 8 person. But YouTube never “gave” Apple proof-of-origin tokens or decrypted file URLs. Apple’s
 9 automated tools extracted these parameters by replicating YouTube’s proprietary processes—the
 10 very definition of circumvention under Section 1201(a)(3)(A).

11 Plaintiffs allege that Apple used descrambling tools, generated file requests outside the
 12 authorized player, rotated IP addresses to evade blocking, and extracted or reused token parameters
 13 outside of their authorized context. AC ¶¶ 105-117. Apple’s proposed analogy – “using a key
 14 given to you” – therefore collapses. Plaintiffs allege manipulation of the access environment, not
 15 mere use of an ordinary viewer credential. At a minimum, the nature of Apple’s specific acts is a
 16 factual question. But the allegations, accepted as true, plausibly describe circumvention within the
 17 meaning of Section 1201(a)(3)(A). *Id.* ¶¶ 85-120, 153-165.

18 **IV. Plaintiffs’ Requested Relief is Proper Under 17 U.S.C. § 1203**

19 Apple argues in a footnote that Plaintiffs’ request for impoundment and remedial
 20 destruction of the audiovisual files obtained through circumvention is improper. MTD at 11 n.5.
 21 Apple is wrong. Section 1203(b) of the DMCA expressly authorizes courts to grant “temporary
 22 and permanent injunctions on such terms as [the court] deems reasonable to prevent or restrain a
 23 violation.” 17 U.S.C. § 1203(b)(1); *Apple Inc. v. Psystar Corp.*, 658 F.3d 1150, 1161 (9th Cir.
 24 2011) (affirming injunction ordering destruction of infringing products under the DMCA). Apple’s
 25 reliance on the principle that the DMCA “does not concern itself with the use of materials after
 26 circumvention” conflates the elements of liability with the scope of available remedies.

CONCLUSION

For the foregoing reasons, the Court should deny Apple's motion to dismiss. If it concludes that Plaintiffs' claims are insufficiently pleaded, Plaintiffs request leave to amend.

Dated: August 24, 2026

Respectfully submitted,

/s/ Max L. Tribble

Rohit Nath (CA SBN 316062)
Michael Gervais (CA SBN 330731)
SUSMAN GODFREY L.L.P.
1900 Avenue of the Stars, Suite 1400
Los Angeles, California 90067
rnath@susmangodfrey.com
mgervais@susmangodfrey.com

Max Lalon Tribble, Jr (CA SBN 326851)
Justin Nelson (*pro hac vice* forthcoming)
SUSMAN GODFREY L.L.P.
1000 Louisiana Avenue, Suite 5100
Houston, Texas 77002
mtribble@susmangodfrey.com
jnelson@susmangodfrey.com

Rom Bar-Nissim (SBN 293356)
HEAH BAR-NISSIM LLP
1801 Century Park East, Suite 2400
Los Angeles, CA 90067
Tel: (310) 432-2836
Rom@HeahBarNissim.com

Tom Kherkher (*pro hac vice*)
Jarrett Lee Ellzey (*pro hac vice*)
Leigh S. Montgomery (*pro hac vice*)
Tyler Yagman (*pro hac vice*)
ELLZEY KHERKHER SANFORD
MONTGOMERY LLP
4200 Montrose Street, Suite 200
Houston, TX 77006
tkherkher@eksm.com
jellzey@eksm.com
lmontgomery@eksm.com

Attorneys for Plaintiffs and the Proposed Class