

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

Attorneys for Plaintiffs and the Proposed Class
Additional Counsel on signature page

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

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

Plaintiffs,

vs.

OPENAI, INC., OPENAI GP LLC, OPENAI
OPCO LLC, OPENAI GLOBAL LLC, OAI
CORPORATION, LLC, OPENAI GROUP PBC,
and OPENAI HOLDINGS, LLC,

Defendants.

Case No. 5:26-cv-2935-BLF

Honorable Beth Labson Freeman

**PLAINTIFFS' OPPOSITION TO
DEFENDANTS' MOTION TO DISMISS
PLAINTIFFS' CLASS ACTION
COMPLAINT**

Date: December 17, 2026

Time: 9:00 AM

Place: Courtroom 1, 5th Floor

Complaint Filed: April 3, 2026

TABLE OF CONTENTS

INTRODUCTION	1
BACKGROUND	3
I. The Digital Millennium Copyright Act and Section 1201(a)	3
II. YouTube’s Controlled Streaming Environment and Access Restrictions	5
III. OpenAI’s Circumvention of YouTube’s Access Restrictions	6
LEGAL STANDARD	7
ARGUMENT	7
I. OpenAI’s Motion Depends on Factual Disputes That Cannot Be Resolved Against Plaintiffs on the Pleadings	7
II. Public Streaming Through YouTube Does Not Eliminate Access Controls Over File-Level Retrieval	8
A. The Technological Gate Is Always Present—Every User Must Pass Through YouTube’s Access Controls	9
B. Authorization to Stream a Work Is Not Authorization to Obtain Its Underlying Audiovisual Files	11
C. Section 1201 Protects Access to a Work as Embodied in a Digital Copy	14
D. OpenAI Cannot Recast YouTube’s Alleged Access Controls as Mere Copy Controls	16
E. Plaintiffs Have Adequately Alleged DMCA Claims, Not Copyright Infringement	17
III. YouTube’s Alleged TPMs Plausibly Control Access	18
A. Rolling Cipher	19
B. IP Blocking and Rate Limiting	19
C. Session-Bound, Short-Lived URLs	21
D. CAPTCHA Challenges	22
E. Proof-of-Origin Tokens	23
IV. Plaintiffs Have Sufficiently Alleged That YouTube’s TPMs Were in Place When OpenAI Circumvented Them	24
CONCLUSION	25

TABLE OF AUTHORITIES

Cases

<i>Arizona Students’ Ass’n v. Arizona Bd. of Regents</i> , 824 F.3d 858 (9th Cir. 2016).....	7
<i>Bell Atl. Corp. v. Twombly</i> , 550 U.S. 544 (2007)	7
<i>CDK Global, LLC v. Tekion Corp.</i> , 2025 WL 1939951 (N.D. Cal. July 15, 2025).....	3, 4, 20
<i>Cordova v. Huneault</i> , 817 F. Supp. 3d 819 (N.D. Cal. 2026)	8, 11, 23, 25
<i>Craigslist, Inc. v. Naturemarket, Inc.</i> , 694 F. Supp. 2d 1039 (N.D. Cal. 2010)	22
<i>Disney Enters., Inc. v. VidAngel, Inc.</i> , 869 F.3d 848 (9th Cir. 2017).....	passim
<i>Echostar Satellite, L.L.C. v. Viewtech, Inc.</i> , 543 F. Supp. 2d 1201 (S.D. Cal. 2008).....	17
<i>Ets-Hokin v. Skyy Spirits, Inc.</i> , 225 F.3d 1068 (9th Cir. 2000).....	15
<i>Green v. United States Dep’t of Justice</i> , 111 F.4th 81 (D.C. Cir. 2024)	1, 4, 5, 18
<i>Hattler v. Ashton</i> , 2017 WL 11634742 (C.D. Cal. Apr. 20, 2017)	16, 17
<i>Hosseinzadeh v. Klein</i> , 276 F. Supp. 3d 34 (S.D.N.Y. 2017).....	17
<i>Justice v. Suno, Inc.</i> , 2026 WL 2445362 (D. Mass Aug. 20, 2026).....	1, 19
<i>Justice v. Uncharted Labs, Inc.</i> , 2026 WL 1430232 (S.D.N.Y. May 21, 2026).....	8
<i>Koala v. Khosla</i> , 931 F.3d 887 (9th Cir. 2019).....	7
<i>Leadsinger, Inc. v. BMG Music Publ’g</i> , 512 F.3d 522 (9th Cir. 2008).....	25

1	<i>Lexmark Int’l, Inc. v. Static Control Components, Inc.,</i>	
2	387 F.3d 522 (6th Cir. 2004).....	13
3	<i>Lopez v. Smith,</i>	
4	203 F.3d 1122 (9th Cir. 2000).....	25
5	<i>MDY Indus., LLC v. Blizzard Ent., Inc.,</i>	
6	629 F.3d 928 (9th Cir. 2010).....	passim
7	<i>Perfect 10, Inc. v. Amazon.com, Inc.,</i>	
8	508 F.3d 1146 (9th Cir. 2007).....	15
9	<i>RealNetworks, Inc. v. Streambox, Inc.,</i>	
10	2000 WL 127311 (W.D. Wash. Jan. 18, 2000).....	23, 24
11	<i>Reddit, Inc. v. SerpApi LLC,</i>	
12	2026 WL 2210094 (S.D.N.Y. July 31, 2026)	passim
13	<i>Sony Music Entertainment v. Uncharted Labs, Inc.,</i>	
14	2026 WL 1019199 (S.D.N.Y. Apr. 15, 2026).....	8
15	<i>Soo Park v. Thompson,</i>	
16	851 F.3d 910 (9th Cir. 2017).....	25
17	<i>Sullivan v. Flora, Inc.,</i>	
18	936 F.3d 562 (7th Cir. 2019).....	15
19	<i>Ted Entertainment, Inc. v. Saber,</i>	
20	2026 WL 2140274 (C.D. Cal. 2026).....	17
21	<i>Ted Entertainment, Inc., et al. v. Snap, Inc.,</i>	
22	2026 WL2435349 (C.D. Cal. Aug. 19, 2026).....	passim
23	<i>Ticketmaster L.L.C. v. Prestige Entertainment, Inc.,</i>	
24	306 F. Supp. 3d 1164 (C.D. Cal. 2018).....	8, 22, 23
25	<i>Ticketmaster L.L.C. v. RMG Techs., Inc.,</i>	
26	507 F. Supp. 2d 1096 (C.D. Cal. 2007).....	22
27	<i>Tohono O’odham Nation v. United States Dep’t of the Interior,</i>	
28	138 F.4th 1189 (9th Cir. 2025).....	7
	<i>UMG Recordings, Inc. v. Suno, Inc.,</i>	
	2026 WL 2410184 (D. Mass. Aug. 18, 2026).....	1, 10, 13
	<i>United States v. Elcom Ltd.,</i>	
	203 F. Supp. 2d 1111 (N.D. Cal. 2002)	17, 18

1		
2	<i>Universal City Studios, Inc. v. Corley</i> ,	
3	273 F.3d 429 (2d Cir. 2001).....	17
4	<i>Viral DRM LLC v. Seven West Media, Ltd.</i> ,	
5	768 F. Supp. 3d 1025 (N.D. Cal. 2025)	17
6	<i>Yout, LLC v. Recording Indus. Ass’n of Am., Inc.</i> ,	
7	633 F. Supp. 3d 650 (D. Conn. 2022)	11, 12
8	Statutes	
9	17 U.S.C. § 101	15
10	17 U.S.C. § 1201	passim
11	17 U.S.C. § 1201(a)	2, 3, 4, 20
12	17 U.S.C. § 1201(a)(1)	1, 4, 11
13	17 U.S.C. § 1201(a)(1)(A)	1, 4
14	17 U.S.C. §§ 1201(a)(1)(C), (d)–(j)	5, 18
15	17 U.S.C. § 1201(a)(3)(A)	20
16	17 U.S.C. § 1201(a)(3)(B).....	10, 19
17	17 U.S.C. § 1201(b)	4
18	Rules	
19	Fed. R. Civ. P. 15(a)(2)	25
20	Other Authorities	
21	H.R. Rep. No. 105-551(II)	4, 15
22	H.R. Rep. No. 105-551(I).....	4, 15
23	S. Rep. No. 105-190	4
24	U.S. Copyright Office, <i>Section 1201 of Title 17: A Report of the Register of Copyrights</i> 126	
25	(June 2017).....	4, 16
26	Section 1201 Rulemaking: Ninth Triennial Proceeding Recommendation of the Register of	
27	Copyrights, at 125 (Oct. 2024)	21
28		

INTRODUCTION

Congress enacted Section 1201 to permit copyright owners to make works readily available in the digital marketplace without surrendering technological control over access to those works. The statute therefore prohibits “circumvent[ing] a technological measure that effectively controls access to a work,” 17 U.S.C. § 1201(a)(1)(A)—a prohibition courts have aptly described as one against “digital trespass.” *Green v. United States Dep’t of Justice*, 111 F.4th 81, 89 (D.C. Cir. 2024).

YouTube makes videos publicly viewable without making the underlying audiovisual files freely retrievable. Critically, YouTube’s technological protection measures (“TPMs”) are not absent during ordinary playback. They always run. The operative complaint (“Complaint”) alleges that every user seeking to watch a YouTube video must encounter and satisfy YouTube’s rolling cipher, proof-of-origin requirements, and session-bound authorization process before YouTube’s servers deliver the audiovisual data. The difference is that an ordinary viewer passes through those gates by using YouTube’s authorized player, while Plaintiffs allege OpenAI circumvented the gatekeeping process to retrieve and retain the underlying audiovisual files outside that environment.

Three decisions issued within the last week confirm that OpenAI’s central premise is wrong. In *Ted Entertainment, Inc., et al. v. Snap, Inc.* (“*Snap*”), Case No. 2:26-cv-00754-AB-MBK, 2026 WL 2435349 (C.D. Cal. Aug. 19, 2026), the court denied dismissal of materially identical Section 1201 claims under Ninth Circuit law, holding that public availability does not eliminate YouTube’s access controls and that each of the same five TPMs alleged here—the rolling cipher, IP blocking and rate limiting, session-bound URLs, CAPTCHA challenges, and proof-of-origin tokens—were plausibly alleged to control access. In *UMG Recordings, Inc. v. Suno, Inc.* (“*UMG*”), 2026 WL 2410184 (D. Mass. Aug. 18, 2026) and *Justice v. Suno, Inc.* (“*Justice*”), 2026 WL 2445362 (D. Mass. Aug. 20, 2026), the court held that allegations that YouTube’s rolling cipher controls access to the underlying audiovisual file, and that YT-DL or YT-DLP was used to circumvent that measure to obtain AI training data, plausibly state a Section 1201(a)(1) claim. The court held that allegations that YouTube’s rolling cipher controls access to the underlying audiovisual file plausibly state a Section 1201(a)(1) claim. *UMG* so held in rejecting a futility challenge to a motion for leave to amend, on allegations that YT-DL and YT-DLP were used to circumvent the cipher; *Justice*

1 adopted that reasoning on a Rule 12(b)(6) motion. And those decisions address the central
2 arguments OpenAI makes here and strongly support denial of its motion (“Motion” or “MTD”).

3 Notably, OpenAI’s Motion mischaracterizes the conduct alleged in the Complaint by
4 treating OpenAI as though it simply visited YouTube and watched Plaintiffs’ videos like any other
5 viewer. Plaintiffs allege something materially different. To obtain the enormous volume of
6 audiovisual data needed to train its AI video-generation model, Sora, OpenAI allegedly: (1) used
7 automated tools to bypass YouTube’s player, authentication processes, and anti-bot protections; (2)
8 accessed and retrieved the underlying audiovisual files directly from YouTube’s servers; and (3)
9 retained permanent copies outside YouTube’s streaming environment, storing and using those files
10 for AI training. Complaint ¶¶ 66–75, 94–115, 141–44. OpenAI therefore did not access Plaintiffs’
11 works through the publicly authorized means on which its motion depends.

12 OpenAI nevertheless advances three arguments: (1) because Plaintiffs permit public
13 streaming, there can be no access control; (2) YouTube’s five TPMs are merely copy controls
14 outside Section 1201(a); and (3) Plaintiffs have not adequately alleged that those TPMs were in
15 place when OpenAI circumvented them. Each of these arguments fails, as detailed below.

16 *First*, many of OpenAI’s arguments depend on factual disputes that cannot be resolved
17 against Plaintiffs on the pleadings. OpenAI asks the Court to accept its own account of how
18 YouTube’s TPMs function and how OpenAI interacted with them. The Complaint identifies the
19 technological measures at issue, describes how they operate, alleges how OpenAI bypassed them,
20 and connects that circumvention to OpenAI’s retrieval of Plaintiffs’ audiovisual files. Complaint
21 ¶¶ 49–62, 94–115, 139–45. Whether OpenAI’s competing technical account is ultimately correct
22 is a question for a factual record, not a Rule 12(b)(6) motion.

23 *Second*, public streaming through YouTube does not eliminate access controls over file-
24 level retrieval. Authorization to stream Plaintiffs’ works through YouTube does not amount to
25 authorization to access the underlying audiovisual files outside YouTube’s controlled environment.
26 Nor does the distinction between a copyrighted “work” and the digital “copy” embodying the work
27 mean that Section 1201 cannot protect access to the audiovisual data stored on YouTube’s servers.
28 And OpenAI’s attempt to characterize YouTube’s TPMs as merely “copy controls” presents a false

choice: a technological measure may restrict copying while also controlling access. Finally, Plaintiffs have pleaded an anti-circumvention claim under Section 1201(a), not a copyright infringement claim. OpenAI cannot defeat a Section 1201 claim by pointing to copyright registration requirements or invoking fair use as though Plaintiffs had pleaded infringement.

Third, the Complaint plausibly alleges that YouTube’s five identified TPMs are access controls. Plaintiffs allege that the rolling cipher requires a technological process before YouTube will deliver audiovisual data; that IP blocking can terminate access from sources engaged in automated extraction; that session-bound URLs restrict retrieval through temporary authorization parameters; that CAPTCHA challenges condition continued access on human verification; and that proof-of-origin tokens require cryptographic information demonstrating that a request originates from an authorized client environment. Complaint ¶¶ 49–62. Plaintiffs further allege that OpenAI bypassed or evaded those measures to unlawfully access audiovisual files outside YouTube’s authorized playback environment. *Id.* ¶¶ 94–115. OpenAI’s disagreements with those allegations largely concern how the technologies actually operated and how its extraction tools interacted with them—issues that cannot be resolved in OpenAI’s favor at this stage.

Fourth, Plaintiffs have sufficiently alleged that YouTube’s TPMs were in place when OpenAI circumvented them. The Complaint expressly alleges that YouTube automatically applied TPMs when Plaintiffs’ works were published and that OpenAI later circumvented those measures to obtain the underlying files. Complaint ¶¶ 139–45.

Accordingly, OpenAI’s Motion should be denied.

BACKGROUND

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

As courts in this District have recognized, Congress enacted the Digital Millennium Copyright Act (“DMCA”) to “mitigate the problems presented by copyright enforcement in the digital age.” *CDK Global, LLC v. Tekion Corp.*, 2025 WL 1939951, at *8 (N.D. Cal. July 15, 2025) (citation omitted). Congress was concerned that copyright owners would “hesitate to make their works readily accessible on the Internet without reasonable assurance that they [would] be protected against massive piracy.” S. Rep. No. 105-190, at 8.

1 Congress thus enacted the DMCA to “create[] the legal platform for launching the global
 2 digital online marketplace for copyrighted works” and to “facilitate making available quickly and
 3 conveniently via the Internet the movies, music, software, and literary works that are the fruit of
 4 the American creative genius.” *Id.*; *see also* H.R. Rep. No. 105-551(II), at 23 (“[A] plentiful supply
 5 of intellectual property—whether in the form of software, music, movies, literature, or other
 6 works—drives the demand for a more flexible and efficient electronic marketplace.”); H.R. Rep.
 7 No. 105-551(I), at 9–10 (explaining that the DMCA was “intended to ensure a thriving electronic
 8 marketplace for copyrighted works”).

9 Section 1201(a)(1)(A) accordingly provides that “[n]o person shall circumvent a
 10 technological measure that effectively controls access to a work protected under this title.” 17
 11 U.S.C. § 1201(a)(1)(A). A measure “effectively controls access” when, “in the ordinary course of
 12 its operation,” access requires “the application of information, or a process or a treatment, with the
 13 authority of the copyright owner.” *Id.* § 1201(a)(3)(B). And “circumvent[ing]” includes
 14 “avoid[ing], bypass[ing], remov[ing], deactivat[ing], or impair[ing]” a technological measure
 15 without authority. *Id.* § 1201(a)(3)(A). Section 1201 thus “‘backed with legal sanctions’ copyright
 16 owners’ use of ‘digital walls’ to protect their copyrighted works from piracy.” *Green*, 111 F.4th at
 17 89 (citation omitted).

18 Section 1201 distinguishes between technological measures that control **access** to
 19 copyrighted works and those that protect the copyright owner’s exclusive rights to the work.
 20 Section 1201(a)(1) prohibits circumvention of technologies designed to circumvent measures that
 21 control access to a work. Section 1201(b) separately prohibits trafficking in technologies designed
 22 to circumvent measures that “effectively protect[] a right of a copyright owner.” The Ninth Circuit
 23 clarified that those categories are not mutually exclusive: “the statute does not provide that a TPM
 24 cannot serve as both an access control and a use control.” *Disney Enters., Inc. v. VidAngel, Inc.*
 25 (“*VidAngel*”), 869 F.3d 848, 864 (9th Cir. 2017). The Copyright Office also refers to TPMs
 26 performing both functions as “merged access and copy controls.” U.S. Copyright Office, *Section*
 27 *1201 of Title 17: A Report of the Register of Copyrights* 126 (June 2017).

28 Congress also understood that protecting technological access controls could sometimes

1 affect persons seeking to make noninfringing uses of copyrighted works. Rather than make fair use
 2 a general license to circumvent those controls, Congress enacted specific statutory exemptions and
 3 established a triennial rulemaking process through which the Librarian of Congress may exempt
 4 classes of users who are adversely affected in their ability to make noninfringing uses. *See* 17
 5 U.S.C. §§ 1201(a)(1)(C), (d)–(j); *Green*, 111 F.4th at 90.

6 **II. YouTube’s Controlled Streaming Environment and Access Restrictions**

7 YouTube exemplifies the digital marketplace Congress sought to foster through Section
 8 1201. Creators—including Plaintiffs—make their audiovisual works broadly available to the public
 9 for streaming through YouTube’s platform and derive value from viewership, advertising,
 10 sponsorships, licensing, and related monetization. Complaint ¶¶ 15–21, 34–39. But making a work
 11 available for public viewing on YouTube does not mean making the underlying audiovisual file
 12 freely available for retrieval. The Complaint alleges that users may watch and listen to videos solely
 13 through YouTube’s authorized playback environment and any other form of access (particularly to
 14 the underlying digital files) is strictly and expressly prohibited. *Id.* ¶¶ 35, 38–40.

15 That distinction is expressly stated in YouTube’s Terms of Service (“Terms”). Creators
 16 grant users access to their content “through YouTube’s services,” but that license expressly “does
 17 not grant any rights or permissions for a user to make use of [the] Content independent of the
 18 Service.” Complaint ¶ 37. The Terms likewise prohibit users from “access[ing], reproduc[ing],
 19 download[ing], distribut[ing], transmit[ing], broadcast[ing], display[ing], sell[ing], licens[ing],
 20 alter[ing], modify[ing] or otherwise us[ing]” content except as expressly authorized by YouTube
 21 or with appropriate permission. *Id.* ¶ 42 n.3; *see also id.* ¶¶ 36, 41–42. Even YouTube’s paid offline-
 22 viewing functionality is limited. YouTube Premium subscribers may save content for offline
 23 playback—but solely within the YouTube application; they are not given unrestricted possession
 24 of the underlying audiovisual files. The files remain within the app, cannot be transferred to another
 25 device, and cease to be available for offline playback after a limited period without renewed access
 26 to YouTube. *Id.* ¶¶ 43–45. Thus, while YouTube’s systems and Terms permit public viewing—
 27 and, in limited circumstances, offline viewing—they do not authorize access, extraction, and
 28 retention of the underlying audiovisual files outside YouTube’s authorized playback environment.

1 Importantly, YouTube uses TPMs to enforce those restrictions. The Complaint identifies at
 2 least five: (1) a rolling cipher that requires YouTube’s signature-transformation process to generate
 3 a usable media request; (2) IP-based monitoring, blocking, and rate limiting directed at high-
 4 volume automated access; (3) short-lived, session-bound media URLs containing authorization
 5 parameters; (4) CAPTCHA challenges triggered by automated or suspicious activity; and (5) proof-
 6 of-origin tokens used to verify that requests originate from an authorized playback environment.
 7 Complaint ¶¶ 49–62. Plaintiffs allege that these measures operate individually and together as
 8 technological gates governing whether and how audiovisual data may be retrieved from YouTube.
 9 *Id.* ¶ 49.

10 **III. OpenAI’s Circumvention of YouTube’s Access Restrictions**

11 Sora is OpenAI’s commercial text-to-video generative AI model. Complaint ¶¶ 1–2, 63–67.
 12 OpenAI disclosed that it trained Sora using “industry-standard machine learning datasets and web
 13 crawls,” but has declined to specify those sources. *Id.* ¶¶ 64–68. Based on that disclosure and the
 14 role of established video-training datasets in the field, the Complaint alleges that OpenAI used four
 15 widely adopted datasets—HD-VILA-100M, HD-VG-130M, Panda-70M, and HowTo100M—that
 16 collectively identify millions of YouTube videos and clips. *Id.* ¶¶ 68–93.

17 Those datasets do not contain the underlying audiovisual files. Instead, they function as
 18 maps or indexes identifying source material through YouTube URLs, video identifiers, timestamps,
 19 and related metadata. *Id.* ¶¶ 68, 74, 85–93. A developer seeking to use the referenced audiovisual
 20 material must therefore return to YouTube, retrieve the source videos, and, where necessary, isolate
 21 the designated clips. *Id.* ¶¶ 68, 73–76, 87, 90, 93. As the Complaint puts it, OpenAI’s models were
 22 not simply “watching” YouTube videos; the audiovisual data had to be accessed, downloaded, and
 23 supplied to OpenAI’s training pipeline. *Id.* ¶ 114.

24 Plaintiffs allege that OpenAI obtained this data through automated scraping and stream-
 25 ripping tools that circumvented YouTube’s TPMs. Complaint ¶¶ 94–115. OpenAI allegedly used
 26 YT-DLP or substantially similar software to replicate or extract YouTube’s signature-
 27 transformation process, allowing it to obtain the underlying audio and video files directly from
 28 YouTube’s servers and outside the authorized player environment. *Id.* ¶¶ 95, 99–102. Plaintiffs also

1 allege that OpenAI used rotating IP addresses and virtual-machine or similar infrastructure so that
 2 automated retrieval could continue when YouTube detected and blocked particular addresses. *Id.*
 3 ¶¶ 3, 103–07.

4 The Complaint further alleges that OpenAI’s automated extraction required bypassing
 5 YouTube’s other access restrictions, including its session-bound URLs, CAPTCHA protections,
 6 and proof-of-origin requirements. *Id.* ¶¶ 108–10. Through those methods, OpenAI allegedly
 7 obtained permanent audiovisual files outside YouTube’s controlled playback environment, stored
 8 those files in its own systems, and used them to assemble training corpora for Sora. *Id.* ¶¶ 73–75,
 9 94–98, 114, 141–44. OpenAI did not obtain the consent or authorization of YouTube or Plaintiffs
 10 to engage in this scraping activity. *Id.* ¶¶ 111–15.

11 LEGAL STANDARD

12 On a motion to dismiss under Rule 12(b)(6), a court must “accept the complaint’s well-
 13 pleaded factual allegations as true, and construe all inferences in the plaintiff’s favor[.]” *Koala v.*
 14 *Khosla*, 931 F.3d 887, 894 (9th Cir. 2019) (quoting *Arizona Students’ Ass’n v. Arizona Bd. of*
 15 *Regents*, 824 F.3d 858, 864 (9th Cir. 2016)). “To survive a motion to dismiss, a complaint must
 16 allege ‘enough facts to state a claim to relief that is plausible on its face.’” *Tohono O’odham Nation*
 17 *v. United States Dep’t of the Interior*, 138 F.4th 1189, 1199 (9th Cir. 2025) (quoting *Bell Atl. Corp.*
 18 *v. Twombly*, 550 U.S. 544, 570 (2007)).

19 ARGUMENT

20 **I. OpenAI’s Motion Depends on Factual Disputes That Cannot Be Resolved Against** 21 **Plaintiffs on the Pleadings**

22 OpenAI asks the Court to accept a technical account that is neither alleged in the Complaint
 23 nor properly resolved on a motion to dismiss. It asserts that a sophisticated browser user can obtain
 24 the underlying media URL notwithstanding the rolling cipher; that OpenAI used session credentials
 25 in their intended manner; that YouTube’s IP controls merely slowed requests rather than cutting
 26 off access; that OpenAI never encountered CAPTCHA challenges for Plaintiffs’ works; and that
 27 the TPMs may not have existed when OpenAI retrieved the videos. MTD at 15–19.

28 Multiple cases confirm that OpenAI’s factual arguments are fatal to its Motion. In *Sony*

1 *Music Entertainment v. Uncharted Labs, Inc.*, 2026 WL 1019199, at *3 (S.D.N.Y. Apr. 15, 2026),
 2 an AI developer that stream-ripped YouTube videos argued that YouTube’s rolling cipher was a
 3 copy control and that the plaintiffs had not adequately pleaded circumvention of an access control.
 4 The court disagreed, holding that the complaint “plausibly alleges that YouTube employs
 5 technological measures that regulate access to its content and that Defendant circumvented them
 6 under the pleading standard set by Rule 8(a).” *Id. Justice v. Uncharted Labs, Inc.*, 2026 WL
 7 1430232, at *2–3 (S.D.N.Y. May 21, 2026), reached the same result on materially similar
 8 allegations; *see also Snap*, 2026 WL 2435349 at * 5 (C.D. Cal. Aug. 19, 2026) (rejecting
 9 defendant’s factual challenges to the operation and effectiveness of YouTube’s TPMs as
 10 inappropriate at the pleading stage).

11 *Reddit* and *Cordova* are in accord. In *Reddit*, the defendant argued that the complaint failed
 12 to identify which automated queries were run, how they were run, when and how often they were
 13 run, and which copyrighted material was obtained. *Reddit, Inc. v. SerpApi LLC*, 2026 WL 2210094,
 14 at * 21-22 (S.D.N.Y. July 31, 2026). The court held that this improperly imported Rule 9(b)’s
 15 heightened standard into a Section 1201 claim. *Id.* The *Reddit* court relied on *Cordova v. Huneault*,
 16 817 F. Supp. 3d 819, 834 (N.D. Cal. 2026), which rejected the contention that a Section 1201
 17 plaintiff must identify in the complaint “the specific tools used to circumvent the technological
 18 measures, or a date on which those tools were used.” *See also Ticketmaster L.L.C. v. Prestige*
 19 *Entertainment, Inc.*, 306 F. Supp. 3d 1164, 1174 (C.D. Cal. 2018) (recognizing that “there are no
 20 heightened pleading requirements for a DMCA circumvention claim.”).

21 Here, the Complaint identifies five technological measures, describes the information or
 22 processes each requires, alleges how OpenAI bypassed them, and links that circumvention to
 23 OpenAI’s retrieval of Plaintiffs’ files. Complaint ¶¶ 49–62, 94–115, 139–45. Whether YouTube’s
 24 systems ultimately function as Plaintiffs allege, and whether (and how) OpenAI bypassed those
 25 systems are factual issues not suitable for determination at this stage.

26 **II. Public Streaming Through YouTube Does Not Eliminate Access Controls Over File-** 27 **Level Retrieval**

28 OpenAI’s principal argument is that because Plaintiffs permit the public to stream their

works on YouTube, the works are already “accessible” and therefore no technological measure can control access to them. MTD at 11–14. That argument depends on several related propositions OpenAI develops throughout its Motion: (1) that Plaintiffs authorized OpenAI to “access” their works by uploading them to YouTube; (2) that Section 1201 protects access to a “work,” rather than a particular file embodying that work; and (3) that measures restricting retrieval of the underlying audiovisual files are copy controls rather than access controls. In forming its opinion that the TPMs alleged in the Complaint are copy controls, OpenAI further suggests Plaintiffs’ claims are nothing more than obfuscated and deficient copyright infringement claims. *See id.* at 3, 6–14. OpenAI’s arguments fail.

A. The Technological Gate Is Always Present—Every User Must Pass Through YouTube’s Access Controls

OpenAI’s argument depends on a false factual premise: that YouTube’s technological gate remains down when an ordinary user watches a video and rises only when YouTube detects prohibited downloading or automated activity. To begin, this argument rests on a premise rejected by the Ninth Circuit, *i.e.*, that revoking access is not controlling access. *See MDY Indus., LLC v. Blizzard Ent., Inc.*, 629 F.3d 928, 943 (9th Cir. 2010) (“[I]n our view, an access control measure can both (1) attempt to block initial access and (2) revoke access if a secondary check determines that access was unauthorized.”).

Further, the Complaint alleges the exact opposite. Before YouTube delivers audiovisual data for ordinary playback, the requesting user must pass through several technological controls. The user’s browser must employ YouTube’s proprietary signature-transformation process to produce a valid media request, use a temporary, cryptographically signed URL tied to the particular session and client context, and present proof-of-origin tokens generated during playback and validated by YouTube’s servers before the data is delivered. Complaint ¶¶ 50–52, 57, 61.

An ordinary viewer ordinarily does not notice those measures because YouTube’s authorized player applies the required information and processes automatically. But an access control does not cease to exist merely because an authorized user possesses the key or because the authorized process operates seamlessly. The legitimate viewer passes through the technological

1 gate using YouTube’s approved player; OpenAI allegedly used automated tools to replicate, evade,
2 or bypass the gatekeeping processes and retrieve the underlying audiovisual files outside
3 YouTube’s authorized playback environment. Complaint ¶¶ 62, 94–110, 113.

4 *Snap* now squarely confirms this point under Ninth Circuit law. There, as here, the
5 defendant argued that publicly viewable YouTube videos could not be protected by access controls
6 because ordinary users encounter no paywall, password prompt, or other visible barrier. The court
7 outright rejected that argument. It held that “[n]othing in § 1201(a) requires an access control to
8 take the form of a paywall, password prompt, or other measure requiring affirmative user
9 input.” *Snap*, 2026 WL 2435349, at *4. Rather, YouTube’s “background authentication and
10 authorization processes” may control access even though they operate seamlessly for ordinary
11 viewers. *Id.* at * 5. The barriers may be “modest,” but “they are barriers nonetheless.” *Id.*

12 *UMG* reached the same conclusion. It held that free public streaming does not establish the
13 absence of an access control because “what matters is the process used to stream the videos.” *UMG*,
14 2026 WL 2410184, *5. The court further recognized the reasonable inference that YouTube’s
15 player must decrypt or descramble the protected file URL to locate and play the underlying
16 audiovisual file and held that disputes over how that process operates require factual development,
17 not dismissal. *Id.* at *5-6.

18 YouTube also employs protections, including IP-based blocking and CAPTCHA
19 challenges, that are triggered by excessive, suspicious, or automated activity. Complaint ¶¶ 53–60.
20 But the conditional operation of those additional protections does not alter the Complaint’s
21 allegation that the rolling cipher, session-bound URLs, and proof-of-origin tokens govern the
22 delivery of audiovisual data during ordinary playback. Complaint ¶¶ 50–52, 57, 61. Nor does it
23 matter that those controls permit an authorized user to watch the video after the required process
24 has been completed. A locked gate remains an access control when it opens for a person presenting
25 the proper credential. Section 1201 asks whether a technological measure requires “the application
26 of information or a process or a treatment” to gain access—not whether every unauthorized user is
27 ultimately denied access. 17 U.S.C. § 1201(a)(3)(B).

B. Authorization to Stream a Work Is Not Authorization to Obtain Its Underlying Audiovisual Files

The centerpiece of OpenAI’s Motion is its contention that because Plaintiffs’ works are “freely accessible” for streaming, there “are no access controls in place.” MTD at 11. But Plaintiffs do not claim that OpenAI violated Section 1201 by watching a video on YouTube. They allege that OpenAI bypassed the technological safeguards surrounding that YouTube player to extract the underlying audiovisual files that YouTube does not make available to ordinary users. Complaint ¶¶ 35–45, 73–75, 94–115, 141–44. Those are materially different forms of access.

Starting with the statutory language, Section 1201 says “access”—not “perceive,” “view,” or “watch.” “Access” includes the “freedom or ability to obtain or make use of something.” *Yout, LLC v. Recording Indus. Ass’n of Am., Inc.*, 633 F. Supp. 3d 650, 664 (D. Conn. 2022). And Section 1201 asks whether a technological measure “controls” access, not whether the measure wholesale prevents it. As *Yout* explained, “the plain meaning of a measure that ‘controls access’ to a protected work appears to be broader than a measure that ‘prevents’ access to a copyrighted work.” *Id.* In *Cordova*, 817 F. Supp. 3d 819, a court in this District likewise held that “measures that restrict access to downloadable files[] are sufficient for purposes of the second element of a § 1201(a)(1) claim.” *Id.* (emphasis added) Likewise, an access control need only provide “some degree of control” and need not be “strong or circumvention-proof.” *MDY Indus.*, 629 F.3d at 954 n.17.

Snap squarely rejected the same argument Open AI makes on the same YouTube architecture. There, the court held that YouTube’s five alleged TPMs plausibly controlled access even though the videos were freely available for public viewing, explaining that “YouTube’s TPMs condition access to the videos on use of YouTube’s authorized streaming architecture” and that public access “does not establish that the works are technologically unrestricted.” *Snap*, 2026 WL 2435349, at *5. *Yout* is also particularly instructive since it too addressed YouTube’s own architecture. The court explained that “YouTube directs users to stream videos and, by not making a download option readily available on the player page, restrains users’ ability to access and copy audio and video files.” 633 F. Supp. 3d at 669. The court therefore concluded that YouTube “exercise[s] restraining or directing influence over” its users in a manner limiting their “freedom

1 and ability” to access downloadable audiovisual files and make local copies. *Id.* That reasoning
 2 applies here. Plaintiffs allege that YouTube employs technological processes to restrict users’
 3 ability to obtain the underlying audiovisual files and that OpenAI circumvented those controls to
 4 retrieve those files directly. Complaint ¶¶ 49–62, 94–115, 141–45.

5 The Ninth Circuit’s decision in *VidAngel* forecloses OpenAI’s narrower conception of
 6 access. There, consumers who lawfully possessed DVDs or Blu-ray discs could view the
 7 copyrighted movies through authorized players. But VidAngel circumvented the discs’ TPMs to
 8 obtain digital copies of the underlying contents. The Ninth Circuit rejected the argument that the
 9 existence of authorized means of viewing eliminated the access control. Using software to decrypt
 10 the TPMs “to obtain a digital copy,” the court explained, was “exactly like ‘breaking into a locked
 11 room in order to obtain a copy of a [movie].’” *VidAngel*, 869 F.3d at 864.

12 The same distinction is alleged here. An ordinary YouTube user may view Plaintiffs’ works
 13 through YouTube’s authorized player. But Plaintiffs allege that the user is not thereby given
 14 unrestricted access to the underlying audiovisual files outside YouTube’s controlled playback
 15 environment. Complaint ¶¶ 35–45, 49–62. OpenAI allegedly used automated tools to obtain those
 16 underlying files directly, retain them outside YouTube, and use them to assemble AI-training
 17 corpora. *Id.* ¶¶ 73–75, 94–115, 141–45. Authorization to engage in the former does not establish
 18 authorization to engage in the latter.¹

19 *Reddit* confirms that ordinary human access and automated bulk access are not identical
 20 under Section 1201. In that case, Google’s SearchGuard system allowed ordinary users to access
 21 search results while challenging or blocking automated systems capable of mass scraping. The court
 22 held that the measure plausibly controlled access, explaining that “[n]othing in the DMCA’s text
 23 exempts from liability persons who circumvent TPMs aimed at protecting copyrightable material
 24

25
 26 ¹ This also debunks OpenAI’s statement that Plaintiffs “authorized OpenAI to access their videos.”
 27 MTD at 3. OpenAI misleadingly quotes only part of the authorization alleged in the Complaint.
 28 The YouTube license permits users to access content “through YouTube’s services,” while
 expressly stating that the license “does not grant any rights or permissions for a user to make use
 of [the] Content independent of the Service.” Complaint ¶37.

1 against bulk access merely because that material is accessible to an authorized individual.” *Reddit*,
2 2026 WL 2210094, at *17.

3 OpenAI’s heavy reliance on *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 387
4 F.3d 522 (6th Cir. 2004) is misplaced. MTD at 7-8, 12. *Lexmark* concerned whether an
5 authentication code was a TPM that effectively controlled access to a printer’s software. *Lexmark*,
6 387 F.3d at 546-47. The Sixth Circuit said no, because a user did not need to encounter the
7 authentication code to access the software. Anyone could “read the literal code of the Printer Engine
8 Program directly from the printer memory, with or without the benefit of the authentication
9 sequence.” *Id.* at 546. “No security device ... protect[ed] access to the Printer Engine Code and no
10 security device accordingly must be circumvented to obtain access to that program code.” *Id.* at
11 547.

12 Here, there is no way to access Plaintiffs’ works—whether on YouTube’s platform or the
13 underlying video file—without encountering the alleged TPMs. And as the Ninth Circuit explained
14 in *VidAngel*, the fact that YouTube offers an authorized way to view Plaintiffs’ works does not
15 mean OpenAI did not circumvent an access control when it circumvented YouTube’s TPMs to
16 access the underlying video file. 869 F.3d at 865 (“Nothing in the legislative history suggests that
17 *VidAngel* did not circumvent an access control simply because there are authorized ways to access
18 the Studios’ works.”). *Reddit* likewise rejected the broad reading of *Lexmark* on which OpenAI
19 relies. The court characterized *Lexmark*’s “front door/back door” language as dicta and explained
20 that applying it categorically to TPMs restricting automated bulk extraction would be “in tension,
21 if not outright antithetical,” to the DMCA’s purpose. *Reddit*, 2026 WL 2210094, at *17. *UMG*
22 likewise rejected application of *Lexmark* at the pleading stage because *Lexmark* applies when the
23 work is readily accessible through another route that never encounters the technological measure.
24 Where, as alleged here, ordinary YouTube playback itself passes through the rolling cipher, there
25 is no unprotected “front door.” *UMG*, 2026 WL 2410184, *4.

26 Nor does *MDY* support OpenAI’s theory. *MDY* held that Warden—a system that detected
27 bot use and denied or revoked access to protected portions of World of Warcraft—was an effective
28 access control. 629 F.3d at 942–43, 952–54. *MDY* therefore confirms that an access control may

1 provide authorized access to some users while denying or revoking access when prohibited activity
 2 is detected. *Id.* at 943. That principle is particularly relevant to the IP-blocking and CAPTCHA
 3 measures alleged here.

4 OpenAI also posits that *MDY* is supportive of its position because the court held that
 5 Warden did not control access to WoW's code (containing both copyrightable and non-
 6 copyrightable elements) because the code was already on the user's hard drive or otherwise
 7 accessible without connecting to Blizzard's servers. 629 F.3d at 952–53. By contrast, Warden
 8 controlled access to the game's dynamic copyrightable elements because users could not obtain
 9 those elements without connecting to Blizzard's servers and passing through the technological
 10 access process. *Id.* at 954. Plaintiffs allege the latter circumstance here. The underlying audiovisual
 11 files remain on YouTube's servers, and a requester cannot obtain them without satisfying or
 12 bypassing YouTube's server-side technological processes. Complaint ¶¶ 49–62.

13 OpenAI next argues that, by uploading videos to YouTube's platform and thereby
 14 subjecting them to YouTube's Terms, Plaintiffs somehow forfeited control over how their works
 15 are accessed. MTD. at 13-14. This misses the mark. To be clear, Plaintiffs' theory does not depend
 16 on violation of the Terms. Although YouTube's Terms confirm the scope of the authorized access
 17 path, Plaintiffs' Section 1201 claim rests on the technological gates YouTube interposes between
 18 every requester and the audiovisual data stored on its servers. Complaint ¶¶ 46–62.

19 **C. Section 1201 Protects Access to a Work as Embodied in a Digital Copy**

20 OpenAI also argues that a technological measure must control access to “the work,” not to
 21 a particular “file” embodying the work. MTD at 6–7, 11–12. According to OpenAI, since Plaintiffs'
 22 works may be viewed through YouTube's player, a measure restricting access to the underlying
 23 audiovisual file cannot control access to the “work.” That argument confuses the Copyright Act's
 24 distinction between a copyrighted work and the copy in which that work is fixed. The question here
 25 is whether a TPM controls access to the work as embodied in a particular copy.

26 Section 1201 necessarily operates upon copies in which copyrighted works are fixed.
 27 Indeed, the same legislative history on which OpenAI relies explains that Section 1201(a) applies
 28 where a person “has not obtained authorized access to a copy or a phonorecord of a work” protected

1 by a TPM. H.R. Rep. No. 105-551(I), at 19 (1998) (emphasis added). A “copy” is the material
 2 object in which a work is fixed and from which it can be perceived, reproduced, or communicated.
 3 17 U.S.C. § 101. The audiovisual files stored on YouTube’s servers are therefore digital copies in
 4 which Plaintiffs’ audiovisual works are fixed. A TPM that controls whether a requester may obtain
 5 the audiovisual data embodied in those copies also controls access to the copyrighted work itself.

6 *VidAngel* further forecloses OpenAI’s distinction. In that case, the encrypted DVDs (*i.e.*,
 7 the copies) embodied the same copyrighted movies that consumers could access through authorized
 8 means. Yet the Ninth Circuit held that circumventing the discs’ TPMs (*i.e.*, the TPMs on the copies)
 9 to obtain the digital contents violated Section 1201(a). 869 F.3d at 864–65.

10 OpenAI’s authorities do not hold otherwise. *Ets-Hokin v. Skyy Spirits, Inc.*, 225 F.3d 1068
 11 (9th Cir. 2000), *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007), and *Sullivan*
 12 *v. Flora, Inc.*, 936 F.3d 562 (7th Cir. 2019), discuss the distinction between a copyrightable work
 13 and a copy of that work in other Copyright Act contexts. None construe Section 1201(a), addresses
 14 a technological access control, or holds that a TPM cannot control access to a work through a
 15 particular digital embodiment.²

16 OpenAI’s construction would also undermine the digital-distribution model Congress
 17 enacted Section 1201(a) to protect. As *MDY* explains, Congress was “particularly concerned with
 18 encouraging copyright owners to make their works available in digital formats such as ‘on-demand’
 19 or ‘pay-per-view,’ which allow consumers effectively to ‘borrow’ a copy of the work for a limited
 20 time or a limited number of uses.” 629 F.3d at 947. Congress accordingly recognized that “[t]o
 21 operate in this environment, content providers will need both the technology to make new uses
 22 possible and the legal framework to ensure they can protect their work from piracy.” *Id.* (quoting
 23 H.R. Rep. No. 105-551(II), at 23). Under OpenAI’s rule, however, once a copyright owner permits
 24 streaming, the technological measures that make controlled streaming possible would lose Section

25
 26 ² OpenAI’s reliance on legislative history concerning “subsequent actions” after authorized access
 27 is likewise misplaced. MTD at 6–7. Plaintiffs do not allege that OpenAI first lawfully acquired the
 28 audiovisual files and later circumvented a separate technological restriction governing what it could
 do with them. They allege that circumvention was the means by which OpenAI obtained the
 underlying files in the first place. Complaint ¶¶ 49–62, 94–115, 141–45.

1201(a) protection simply because the work can be viewed through the authorized channel.

D. OpenAI Cannot Recast YouTube’s Alleged Access Controls as Mere Copy Controls

OpenAI further argues that because (in its view) the TPMs only restrict downloading, they are copy controls rather than access controls. *See, e.g.*, MTD at 1, 14–15. *First*, the Copyright Office recognizes “merged access and copy controls”—*i.e.*, technological measures that perform both functions at once. U.S. Copyright Office, *Section 1201 of Title 17: A Report of the Register of Copyrights* 126 (June 2017). In addressing such controls, the Copyright Office expressly concluded that “section 1201(a)(1) is best read as protecting the integrity of access controls even where prohibited conduct would not be infringing.” *Id.* at 126–27. *Second*, the Ninth Circuit has made clear that a TPM can function as both. *VidAngel*, 869 F.3d at 864 (“[T]he 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).”); *MDY*, 629 F.3d at 946 (recognizing that a technological measure may “both (1) control[] access and (2) protect[] against copyright infringement”). OpenAI itself concedes the point. MTD at 14 (“To be sure, under *MDY*, a TPM can serve as both a § 1201(a) access control and a § 1201(b) copy control . . .”).

OpenAI’s principal contrary authority, *Hattler v. Ashton*, 2017 WL 11634742 (C.D. Cal. Apr. 20, 2017), predates *VidAngel*. To the extent *Hattler* treated the public availability of streaming content as dispositive of whether a measure could also control access, that reasoning cannot be reconciled with *VidAngel*’s subsequent holding that “authorized ways to access” a copyrighted work do not eliminate another access control protecting the same work. 869 F.3d at 864–65. Indeed, *Hattler* itself acknowledged facts that cut against OpenAI’s categorical reading. The defendants there did “not dispute that, in order to download the [plaintiff’s] works for their use . . . they were required to circumvent technology expressly designed to prevent that form of access.” 2017 WL 11634742, at *6. The court analogized the situation to a locked home: “allowing members of the public access to the locked front door of your home does not constitute consent to their

manipulating the lock in a way that allows them to enter without your permission.” *Id.*³

E. Plaintiffs Have Adequately Alleged DMCA Claims, Not Copyright Infringement

OpenAI’s references to copyright registration, *Ted Entertainment, Inc. v. Saber*, 2026 WL 2140274, and *Hosseinzadeh v. Klein*, 276 F. Supp. 3d 34 (S.D.N.Y. 2017), do nothing to push Plaintiffs’ clearly alleged DMCA claims into copyright infringement territory.⁴

Section 1201(a) creates an anti-circumvention right independent of traditional copyright infringement. *MDY*, 629 F.3d at 945–47. Plaintiffs therefore need not plead infringement under Section 106 or satisfy Section 411(a)’s registration prerequisite to state an anti-circumvention claim. *See Viral DRM LLC v. Seven West Media, Ltd.*, 768 F. Supp. 3d 1025, 1031–32 (N.D. Cal. 2025); *Echostar Satellite, L.L.C. v. Viewtech, Inc.*, 543 F. Supp. 2d 1201, 1205 (S.D. Cal. 2008).

Nor does Section 1201(c)(1) create a fair-use defense to circumvention. That provision preserves “defenses to copyright infringement, including fair use”; it does not transform fair use into authorization to circumvent an otherwise effective access control. A defendant may contend that its downstream use would be fair in a copyright-infringement action and nevertheless violate Section 1201(a) in the manner by which it obtained the protected material. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 459 (2d Cir. 2001).⁵

³*Hattler* also involved remarkably sparse (in fact, completely nonexistent) allegations about the technological protection measures at issue. While the plaintiff’s second amended complaint asserted the conclusion that the defendants “circumvented the technological measures on [Plaintiff’s] sites,” it did not even say what technological measures existed on those sites. *See* Second Amended Complaint, *Hattler v. Ashton*, Case No. 2:16-cv-04099-GHK-KS, ECF No. 26 (C.D. Cal. Nov. 21, 2016). Thus, the *Hattler* court lacked any information about the TPMs at issue from which it could plausibly discern whether the websites at issue had access controls. Here, by contrast, the Complaint describes each of YouTube’s five TPMs and how they function. Complaint ¶¶ 49-62.

⁴ OpenAI cites *Saber*, for its fair-use ruling, and *Hosseinzadeh*, for Plaintiffs’ prior reliance on fair use. MTD at 2. Neither case addresses whether circumvention of an access control violates Section 1201(a), and neither supports importing fair use as a defense to such a claim.

⁵ OpenAI’s reliance on *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111 (N.D. Cal. 2002) (MTD at 7-8) is misplaced. *Elcom* involved a prosecution under Section 1201(b) for trafficking in software that removed use restrictions from e-books already lawfully acquired by purchasers. *Id.* at 1118–21. In explaining the statutory distinction, the court expressly recognized that Congress prohibited the act of circumventing *access controls* under Section 1201(a)(1), while declining to prohibit the

OpenAI therefore gets the statutory structure backwards when it characterizes Plaintiffs’ claim as an effort to “evade the fair use inquiry” by “recasting” a copying claim as a circumvention claim. MTD at 1–2, 9–10. Plaintiffs’ claim is not that OpenAI infringed their copyrights by making an unlawful downstream use. It is that OpenAI circumvented technological measures controlling access to their works—conduct Congress separately prohibited. Whether OpenAI might possess a fair-use defense to a hypothetical infringement claim is neither an element of nor a defense to the Section 1201(a) claim Plaintiffs have pleaded.

Thus, fair use is not applicable to Plaintiffs’ claims, but, even if it were, Congress addressed concerns about noninfringing circumvention through specific statutory exemptions and the triennial rulemaking process under Section 1201(a)(1)(C), through which the Librarian of Congress may exempt classes of users adversely affected in their ability to make noninfringing uses. *See* 17 U.S.C. §§ 1201(a)(1)(C), (d)–(j); *Green*, 111 F.4th at 90. OpenAI identifies no exemption applicable to the mass circumvention alleged here.

III. YouTube’s Alleged TPMs Plausibly Control Access

OpenAI attacks each of YouTube’s five alleged TPMs separately. MTD at 14–19. But OpenAI cannot obtain dismissal merely by showing that one particular measure may not independently qualify. Plaintiffs allege layered and overlapping technological measures, each of which independently or in combination control access to audiovisual data, and allege circumvention of those measures in connection with OpenAI’s retrieval of YouTube files. Complaint ¶¶ 49, 94–115. OpenAI’s TPM-by-TPM attack has now been considered and rejected on virtually identical allegations. In *Snap*, the court separately analyzed the rolling cipher, IP blocking and rate limiting, session-bound URLs, CAPTCHA challenges, and proof-of-origin tokens and concluded that plaintiffs had “sufficiently alleged that each of the TPMs serve as access controls, not copy controls.” *Snap*, 2026 WL 2435349, at *7.

act of circumventing *use restrictions* under Section 1201(b), in part to preserve fair use by persons who had already lawfully acquired the work. *Id.* at 1120–21. Plaintiffs here clearly allege the former, that is, circumvention of access controls as the means by which OpenAI unlawfully obtained the underlying audiovisual files in the first place.

1 **A. Rolling Cipher**

2 The rolling cipher is, in effect, a digital lock that constantly changes its combination. As
 3 Plaintiffs allege, YouTube maintains a page URL for the webpage where playback occurs and a
 4 separate location for the underlying audiovisual file. Complaint ¶¶ 50–51. YouTube withholds a
 5 usable media-file location unless the requesting client transforms an obfuscated signature parameter
 6 using proprietary logic embedded in YouTube’s official player. *Id.* The playback data contains a
 7 scrambled signature that must be processed to produce a valid media request; “[w]ithout performing
 8 this authorized transformation, the server will not deliver the audiovisual file.” *Id.* ¶ 50. YouTube
 9 periodically changes the algorithm, and its official player applies the transformation during
 10 controlled playback. *Id.* ¶ 51. Those allegations track Section 1201(a)(3)(B): obtaining the
 11 audiovisual data requires “the application of information, or a process or a treatment” before
 12 YouTube’s server will deliver it. 17 U.S.C. § 1201(a)(3)(B). And recent cases confirm that the
 13 rolling cipher, as alleged here, is an access control (*see Snap*, 2026 WL 2435349, at *6) or that the
 14 question presents a factual dispute that cannot be resolved on the pleadings. *See Justice*, 2026 WL
 15 2445362, at *4.

16 OpenAI responds that “sophisticated users of an ordinary web browser can obtain the URL
 17 for the underlying file regardless of the rolling cipher.” MTD at 15. That factual assertion appears
 18 nowhere in the Complaint and contradicts Plaintiffs’ allegation that a requester cannot obtain a
 19 usable file location without performing the requisite transformation. Complaint ¶¶ 50–52. It cannot
 20 be credited over Plaintiffs’ well-pleaded allegations on a Rule 12(b)(6) motion. Regardless, the
 21 argument does not justify dismissal. Section 1201 does not require a TPM to be secret,
 22 impenetrable, or impossible for a sophisticated user to defeat. An effective TPM need only provide
 23 “some degree of control” and need not be “strong or circumvention-proof.” *MDY*, 629 F.3d at 954
 24 n.17.

25 **B. IP Blocking and Rate Limiting**

26 OpenAI improperly collapses two related but distinct functions: reducing request frequency
 27 and revoking access from an offending source. Plaintiffs allege that YouTube monitors request
 28 behavior and may throttle, deny, or entirely block an IP address exhibiting automated or abusive

1 patterns, preventing further retrieval of audiovisual content from that source. Complaint ¶¶ 53–56.
2 OpenAI allegedly used rotating IP addresses so that its extraction process could continue despite
3 those restrictions. *Id.* ¶¶ 103–07.

4 *MDY* confirms that a measure may control access by revoking it after detecting
5 unauthorized activity. In *MDY*, Warden monitored users for bots and disconnected users when
6 prohibited software was detected, which the Ninth Circuit held was an effective access control as
7 to the game’s protected copyrightable elements. 629 F.3d at 942–43, 954. As the court explained,
8 “an access control measure can both (1) attempt to block initial access and (2) revoke access if a
9 secondary check determines that access was unauthorized.” *Id.* at 943. YouTube’s alleged IP-
10 blocking system performs the same type of gatekeeping function by monitoring request behavior
11 and denying further access from sources identified as automated or abusive. Complaint ¶¶ 53–56.
12 *Snap* confirms Plaintiffs’ reading of *MDY*. See *Snap*, 2026 WL 2435349, at *6.

13 This District’s decision in *CDK Global* points in the same direction. That case involved a
14 TPM similar to YouTube’s IP blocking measure: the plaintiff employed a “technological measure
15 of restricting access to its copyrighted material to approved IP networks,” and the court agreed that
16 the defendant’s alleged circumvention of that TPM plausibly supported a Section 1201(a) claim.
17 *CDK Global*, 2025 WL 1939951, at *9. YouTube’s IP-blocking TPM is in the same vein: it
18 monitors IP addresses and cuts off platform access from the offending IP address entirely,
19 preventing any further retrieval of audiovisual content from that IP address. Complaint ¶¶ 53-56.

20 OpenAI also understates what IP rotation allegedly accomplished. Section 1201(a)(3)(A)
21 defines circumvention to include “avoid[ing]” and “bypass[ing]” a technological measure.
22 Plaintiffs allege that OpenAI rotated IP addresses precisely to evade YouTube’s restrictions and
23 continue retrieving content. Complaint ¶¶ 103–07. *Reddit* held that proxies, shifting IP addresses,
24 false or altered requester information, and technology designed to mimic ordinary human activity
25 plausibly “avoid[ed]” or “bypass[ed]” an access control when deployed to evade detection and
26 blocking. *Reddit*, 2026 WL 2210094, at *20.

27 On rate-limiting, OpenAI leans heavily on the Copyright Office’s 2024 triennial rulemaking
28 recommendation. MTD at 16-18. But the Copyright Office repeatedly emphasized, in that report,

1 the limited amount of information it had before it to assess whether rate-limit enforcement systems
2 effectively control access to a work. *See, e.g.*, Section 1201 Rulemaking: Ninth Triennial
3 Proceeding Recommendation of the Register of Copyrights, at 125 (Oct. 2024) (“IP address
4 rotation, *based on the thin record before the Office*, does not appear to involve circumvention of an
5 effective control”) (emphasis added). A recommendation issued on a “thin record” in an exemption
6 rulemaking cannot displace Plaintiffs’ well-pleaded factual allegations at the motion to dismiss
7 stage. More importantly, those materials do not resolve the distinct allegation here that YouTube
8 may entirely block an offending source from further audiovisual retrieval. Complaint ¶¶ 53–56.

9 C. Session-Bound, Short-Lived URLs

10 YouTube further controls access by issuing temporary, cryptographically signed URLs tied
11 to a particular playback session, client context, and expiration window. Complaint ¶¶ 57–58. Once
12 the authorization window expires, YouTube’s server will no longer deliver the audiovisual file in
13 response to that URL. *Id.* ¶ 57. An automated system seeking persistent file retrieval cannot rely
14 indefinitely on a static media link; it must obtain fresh parameters and regenerate valid media
15 requests. *Id.* ¶¶ 58, 108.

16 OpenAI responds that Plaintiffs merely allege that it “programmatically renew[ed] expired
17 credentials and initiat[ed] new authorized sessions,” and argues that using such “valid” credentials
18 cannot constitute circumvention. MTD at 17. But OpenAI conflates YouTube’s server accepting a
19 credential as technically valid with authorization to obtain and use that credential in the manner
20 alleged. A credential may be accepted by YouTube’s system without making OpenAI’s alleged
21 automated generation and use of that credential authorized.

22 Here, the Complaint alleges that the URLs are tied to a particular playback session and
23 client context that are designed to prevent persistent retrieval outside ordinary playback. Complaint
24 ¶¶ 57–58. Plaintiffs further allege that OpenAI’s automated tools repeatedly regenerated or renewed
25 the required parameters to continue obtaining audiovisual files. Plaintiffs further allege that OpenAI
26 did so in conjunction with tools that replicated YouTube’s signature process and extracted,
27 replicated, or reused authentication information outside its intended playback context. *Id.* ¶¶ 61–
28 62, 99–100, 108, 110. At minimum, whether OpenAI simply used credentials in the manner

1 YouTube designed or instead replicated and bypassed the session-bound gatekeeping process is a
 2 factual dispute that cannot be resolved in OpenAI's favor at this stage. *See Snap*, 2026 WL
 3 2435349, at *6.

4 **D. CAPTCHA Challenges**

5 The Complaint alleges that YouTube presents CAPTCHA challenges when traffic patterns
 6 indicate automated or suspicious activity. Complaint ¶ 59. Until the challenge is successfully
 7 completed, the requesting client cannot continue retrieving the information necessary to obtain
 8 audiovisual data. *Id.* The CAPTCHA therefore conditions continued access on application of
 9 information verifying that the requester is a human rather than an automated system. Plaintiffs
 10 further allege that the scale at which OpenAI operated would trigger those challenges and that
 11 OpenAI configured or distributed its systems to evade detection and prevent CAPTCHA
 12 enforcement from halting retrieval. *Id.* ¶¶ 60, 109.

13 As OpenAI points out, courts have routinely recognized CAPTCHA as a technological
 14 access measure where it conditions further access on information supplied through a human-
 15 verification process. *See Ticketmaster L.L.C. v. RMG Techs., Inc.*, 507 F. Supp. 2d 1096, 1112
 16 (C.D. Cal. 2007); *Prestige Ent., Inc.*, 306 F. Supp. 3d at 1174; *Craigslist, Inc. v. Naturemarket,*
 17 *Inc.*, 694 F. Supp. 2d 1039, 1050, 1056 (N.D. Cal. 2010). OpenAI attempts to distinguish those
 18 cases on the ground that the CAPTCHAs there supposedly “controlled all access to the material.”
 19 MTD at 18. *Reddit* directly rejects that distinction. SearchGuard examined incoming requests and
 20 presented a challenge only to unrecognized or suspicious traffic; ordinary human users generally
 21 accessed the material without seeing a CAPTCHA. *Reddit*, 2026 WL 2210094, at *15–16. The
 22 court nevertheless held that SearchGuard was a “process” required “to gain access to the work”
 23 because it erected a technological gate that permitted human users to proceed while restricting
 24 automated systems. *Id.*

25 OpenAI separately argues that Plaintiffs' CAPTCHA allegations are “speculative” because
 26 Plaintiffs do not allege that a CAPTCHA was “actually presented with respect to any of Plaintiffs’
 27 specific works.” MTD at 18. OpenAI's argument calls for specificity that Rule 8 does not require
 28 on a Section 1201 circumvention claim. *See Ticketmaster*, 306 F. Supp. 3d at 1174; *Reddit*, 2026

1 WL 2210094, at *21–22; *Cordova*, 817 F. Supp. 3d at 834. Plaintiffs’ allegations of large-scale
 2 automated extraction triggering CAPTCHA and technological evasion of it are sufficient at this
 3 stage.⁶ *See Snap*, 2026 WL 2435349, at *7.

4 **E. Proof-of-Origin Tokens**

5 On proof-of-origin tokens, Plaintiffs allege that YouTube requires requests for video
 6 segments to include cryptographic tokens demonstrating that the request originates from an
 7 authorized client environment operating within the intended playback context. Complaint ¶ 61.
 8 YouTube’s servers validate those tokens before delivering audiovisual data, and requests lacking
 9 appropriate tokens, or presenting replayed or otherwise improper token information, are denied or
 10 degraded. *Id.* Automated tools operating outside YouTube’s official playback environment
 11 allegedly must extract, replicate, or reuse the required token parameters to retrieve the files directly.
 12 *Id.* ¶¶ 62, 110.

13 OpenAI’s response—that an ordinary viewer need not personally enter a token because
 14 YouTube’s webpage and player automatically supply what the browser needs for playback, MTD
 15 at 18–19—is beside the point. The statute does not require manual human input. The alleged
 16 automated cryptographic process remains a “process.” *VidAngel* is instructive here as well.
 17 Authorized DVD and Blu-ray players automatically performed the decryption necessary to access
 18 encrypted discs. The ordinary consumer did not personally type in a decryption key, yet the Ninth
 19 Circuit had no difficulty concluding that CSS and AACS were access controls. 869 F.3d at 853,
 20 863–65. Plaintiffs allege that OpenAI replicated or reused that process outside the approved
 21 playback environment to retrieve the underlying audiovisual files. Complaint ¶¶ 61–62, 110.

22 OpenAI’s own case, *RealNetworks, Inc. v. Streambox, Inc.*, 2000 WL 127311 (W.D. Wash.
 23 Jan. 18, 2000), provides a close analogue. MTD at 7. There, a RealServer would transmit streaming
 24 content only after an authorized RealPlayer supplied the server with information through a

25
 26 ⁶ OpenAI’s reliance on the Copyright Office’s discussion of “backoff techniques” assumes a factual
 27 account not pled in the FAC. MTD at 17–18. Plaintiffs do not allege that OpenAI merely complied
 28 with YouTube’s limits by slowing the rate of its requests, rather, that OpenAI configured automated
 infrastructure to “evade detection, distribute requests across multiple machines, or otherwise
 prevent CAPTCHA enforcement from halting access.” Complaint ¶ 60; *see also id.* ¶¶ 103–09.

1 proprietary authentication sequence known as the “Secret Handshake.” *RealNetworks, Inc.*, 2000
 2 WL 127311 at *2, *7. The court held that this process effectively controlled access because a user
 3 had to employ the authorized player, which supplied the requisite information to the server before
 4 the media would be delivered. *Id.* at *7-8. The defendant circumvented that measure by mimicking
 5 the authorized RealPlayer and causing the server to treat its request as originating from an approved
 6 client. *Id.* at *3-4. Here, Plaintiffs allege that YouTube requires proof-of-origin tokens
 7 demonstrating that a request originates from an authorized client environment, validates those
 8 tokens before delivering audiovisual data, and denies or degrades requests lacking appropriate
 9 token information. Complaint ¶¶ 61-62. OpenAI allegedly operated outside that authorized
 10 environment and extracted, replicated, or reused the token parameters necessary to obtain the files.
 11 *Id.* ¶¶ 62, 110.

12 * * * *

13 Taken together, the Complaint alleges multiple TPMs that require specific information or
 14 processes before YouTube’s servers deliver audiovisual data, as well as measures that deny or
 15 revoke access when automated extraction is detected. Complaint ¶¶ 49-62. OpenAI’s arguments to
 16 the contrary either rest on the mistaken legal premise or on factual disputes concerning how
 17 YouTube’s systems and OpenAI’s extraction tools operated. Neither supports dismissal.

18 **IV. Plaintiffs Have Sufficiently Alleged That YouTube’s TPMs Were in Place When** 19 **OpenAI Circumvented Them**

20 Finally, OpenAI argues that Plaintiffs have not alleged “when YouTube implemented” its
 21 TPMs or “whether they were in place when OpenAI allegedly downloaded the videos.” MTD at
 22 19. The same timing argument was rejected in *Snap*. There, the defendant argued that plaintiffs
 23 failed to allege when YouTube implemented the five TPMs or whether they existed when the videos
 24 were accessed. *See Snap*, 2026 WL 2435349, at *7. The court held it sufficient that the complaint
 25 alleged the TPMs existed when the defendant scraped the YouTube videos. *Id.* Plaintiffs allege the
 26 same here. Complaint ¶¶ 139-45.

27 OpenAI’s argument is also contradicted by the Complaint’s express allegations. Plaintiffs
 28 allege that “[w]hen published, YouTube automatically applied TPMs that control access to and

1 prevent unauthorized copying or downloading of these audiovisual files.” Complaint ¶ 139.
2 Plaintiffs identify five specific TPMs, describe how each functions, and allege how OpenAI
3 circumvented them. *Id.* ¶¶ 49–62, 68–75, 93–115, 139–45. Section 1201 claims are analyzed under
4 Rule 8 and require plausibility and fair notice. They do not require discovery-level proof. *See also*
5 *Reddit*, 2026 WL 2210094, at *21–22; *Cordova*, 817 F. Supp. 3d at 834. Plaintiffs’ allegations
6 plausibly establish that YouTube’s TPMs were operating when the alleged circumvention occurred.
7 Indeed, one cannot circumvent a measure that is not there.

8 The Complaint’s allegations are particularly sufficient because information such as when
9 OpenAI made particular requests, which versions of its extraction tools it employed, and what
10 technological responses those requests encountered, are solely within OpenAI’s possession and
11 control. *See Soo Park*, 851 F.3d at 928 (permitting allegations on information and belief where the
12 facts are particularly within the defendant’s possession or where the belief rests on factual
13 information making the allegation plausible).

14 CONCLUSION

15 The three most recent courts to confront the central arguments advanced by OpenAI have
16 rejected it at the pleading stage, including a court applying Ninth Circuit law to the same five
17 YouTube TPMs alleged here. *See Snap*, 2026 WL 2435349, at *7. For these reasons, OpenAI’s
18 Motion should be denied in its entirety. However, if the Court concludes that Plaintiffs’ claim is
19 insufficiently pleaded in any respect, Plaintiffs respectfully request leave to amend because
20 OpenAI’s arguments turn largely on pleading specificity, and any perceived deficiencies could be
21 cured by amendment. *See Fed. R. Civ. P. 15(a)(2); Lopez v. Smith*, 203 F.3d 1122, 1130 (9th Cir.
22 2000) (leave to amend should be granted unless amendment would be futile); *Leadsinger, Inc. v.*
23 *BMG Music Publ’g*, 512 F.3d 522, 532 (9th Cir. 2008).

1 Dated: August 24, 2026

Respectfully submitted,

2 /s/ Rom Bar-Nissim

3 Rom Bar-Nissim (SBN 293356)

4 **HEAH BAR-NISSIM LLP**

1801 Century Park East, Suite 2400

Los Angeles, CA 90067

5 Tel: (310) 432-2836

6 Rom@HeahBarNissim.com

7 Jarrett Lee Ellzey*

8 Tom Kherkher**

Leigh S. Montgomery*

9 **ELLZEY KHERKHER SANFORD**

MONTGOMERY LLP

4200 Montrose Street, Suite 200

10 Houston, TX 77006

11 JEllzey@EKSM.com

TKherkher@EKSM.com

12 LMontgomery@EKSM.com

13 William J. Edelman (SBN 285177)

14 **MILBERG, PLLC**

227 W. Monroe Street, Suite 2100

15 Chicago, IL 60606

16 Tel: (866) 252-0878

wedelman@milberg.com

17 Michael A. Acciavatti*

18 **MILBERG, PLLC**

405 East 50th Street

19 New York, NY 10022

20 Tel: (212) 594-5300

macciavatti@milberg.com

21 James E. Cecchi**

22 Kevin G. Cooper**

23 **CARELLA BYRNE CECCHI**

BRODY & AGNELLO, P.C.

5 Becker Farm Rd.

24 Roseland, NJ 07068

25 Tel: (973) 994-1700

jcecchi@carellabyrne.com

26 kcooper@carellabyrne.com

27 * *pro hac vice* forthcoming

28 ** admitted *pro hac vice*

CERTIFICATE OF SERVICE

I hereby certify that on August 24, 2026, I caused a true and correct copy of the foregoing to be electronically filed with the Clerk of the Court using the CM/ECF system, which will send notification to the attorneys of record, and is available for viewing and downloading.

/s/ Rom Bar-Nissim