

Dale M. Cendali (SBN 1969070)
Joshua L. Simmons (*pro hac vice*)
Josh Berlowitz (*pro hac vice*)
KIRKLAND & ELLIS LLP
601 Lexington Avenue
New York, NY 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900
dale.cendali@kirkland.com
joshua.simmons@kirkland.com
josh.berlowitz@kirkland.com

Attorneys for Defendant Apple Inc.

Additional Counsel Listed on Signature Page

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

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

Plaintiffs,

v.

APPLE INC.,

Defendant.

CASE NO. 3:26-CV-02936-RS

**DEFENDANT APPLE INC.'S NOTICE OF
MOTION AND MOTION TO DISMISS
AMENDED COMPLAINT**

Judge: Hon. Richard Seeborg

Amended Complaint Filed: July 14, 2026

Hearing Date: October 1, 2026

Time: 1:30 p.m. Pacific

Courtroom: Courtroom 12, 19th Floor

1 TO THE COURT, ALL PARTIES, AND THEIR ATTORNEYS OF RECORD:

2 PLEASE TAKE NOTICE that on October 1, 2026 at 1:30 p.m. Pacific, or as soon thereafter as
3 the matter may be heard by the Honorable Richard Seeborg of the above-titled Court, located at
4 Courtroom 12, 19th Floor, 450 Golden Gate Avenue, San Francisco, California 94102, Defendant Apple
5 Inc. will and hereby does move the Court for an order dismissing with prejudice under Federal Rule of
6 Civil Procedure 12(b)(6) Plaintiffs Ted Entertainment, Inc., Matt Fisher, and Golfholics, Inc.'s
7 ("Plaintiffs") First Amended Class Action Complaint. Dkt. 29 ("FAC"). This Motion is made pursuant
8 to the Federal Rules and is based upon this Notice; the attached Memorandum of Points and Authorities;
9 any reply papers filed by Apple; the pleadings filed with this Court; and such other evidence, oral or
10 documentary, and argument as may be presented at or before the hearing.

11 As set forth in the Motion, the FAC should be dismissed with prejudice because Plaintiffs fail to
12 state a claim for circumvention of effective access controls pursuant to 17 U.S.C. § 1201(a)(1)(A).
13 Because Plaintiffs already have amended their complaint but have not remedied the fundamental problems
14 with their legal theory, Apple requests that the Court dismiss the FAC with prejudice.

15 DATED: July 28, 2026

Respectfully submitted,

17 /s/ Dale M. Cendali

18 Dale M. Cendali (SBN 1969070)
dale.cendali@kirkland.com

19 Attorney for Defendant
20 Apple Inc.

TABLE OF CONTENTS

I.	PRELIMINARY STATEMENT	1
II.	STATEMENT OF ISSUES TO BE DECIDED	3
III.	BACKGROUND	3
A.	The DMCA Created a Qualified Right Against Circumvention of Access Controls.....	3
B.	Plaintiffs Allege That They Made Their Audiovisual Works Available to the Public	6
C.	Apple Allegedly Accessed Plaintiffs’ Publicly Accessible Works.....	10
IV.	ARGUMENT.....	11
A.	The Alleged Technological Measures Are Not Access Controls	12
B.	The Alleged Technological Measures Do Not Operate in the Ordinary Course ...	16
C.	Apple Is Not Alleged to Have “Circumvented” the Technological Measures	20
V.	CONCLUSION	25

TABLE OF AUTHORITIES¹**Page(s)****Cases**

<i>Adobe Sys. Inc. v. A&S Elecs., Inc.</i> , No. 15 Civ. 2288, 2015 WL 13022288 (N.D. Cal. Aug. 19, 2015).....	12, 21, 23, 24
<i>Airs Aromatics, LLC v. Victoria's Secret Stores Brand Mgmt., Inc.</i> , 744 F.3d 595 (9th Cir. 2014)	7
<i>Ambrozewicz v. 6Sense Insights, Inc.</i> , 804 F. Supp. 3d 1026 (N.D. Cal. 2025)	11, 12
<i>Ass'n for Info. Media and Equip. v. Regents of the Univ. of Cal.</i> , No. 10 Civ. 9378, 2012 WL 7683452 (C.D. Cal. Nov. 20, 2012).....	12, 14
<i>Burroughs Payment Sys., Inc. v. Symco Grp.</i> , No. 10 Civ. 3029, 2011 WL 13217738 (N.D. Ga. Dec. 13, 2011)	12, 23
<i>Caviness v. Horizon Cmty. Learning Ctr., Inc.</i> , 590 F.3d 806 (9th Cir. 2010)	12
<i>Columbia Pictures Indus., Inc. v. Fung</i> , 710 F.3d 1020 (9th Cir. 2013)	13, 20
<i>Conservation Force v. Salazar</i> , 646 F.3d 1240 (9th Cir. 2011)	11
<i>Cordova v. Huneault</i> , 817 F. Supp. 3d 819 (N.D. Cal. 2026)	20
<i>Couponcabin LLC v. Savings.com, Inc.</i> , No. 14 Civ. 39, 2016 WL 3181826 (N.D. Ind. June 8, 2016).....	12, 16, 24
<i>Coupons, Inc. v. Stottlemire</i> , No. 07 Civ. 3457, 2008 WL 3245006 (N.D. Cal. July 2, 2008).....	12, 16
<i>Digit. Drilling Data Sys., LLC v. Petrolink Servs., Inc.</i> , 965 F.3d 365 (5th Cir. 2020)	24
<i>DISH Net., LLC v. Dimarco</i> , No. 11 Civ. 1962, 2012 WL 917812 (D. Nev. Mar. 14, 2012).....	11
<i>DISH Net. LLC v. World Cable Inc.</i> , 893 F. Supp. 2d 452 (E.D.N.Y. 2012)	12, 21, 23

¹ All internal quotation marks and citations have been omitted unless otherwise noted.

1	<i>Disney Enters., Inc. v. VidAngel, Inc.</i> ,	
2	869 F.3d 848 (9th Cir. 2017)	4, 15
3	<i>Egilman v. Keller & Heckman, LLP</i> ,	
4	401 F. Supp. 2d 105 (D.D.C. 2005)	12
5	<i>Emmerich Newspapers, Inc. v. Particle Media, Inc.</i> ,	
6	No. 23 Civ. 26, 2025 WL 2146609 (S.D. Miss. July 29, 2025)	12
7	<i>Google LLC v. SerpApi, LLC</i> ,	
8	No. 25 Civ. 10826, Dkt. 42 (N.D. Cal. July 20, 2026)	23
9	<i>Ground Zero Museum Workshop v. Wilson</i> ,	
10	813 F. Supp. 2d 678 (D. Md. 2011)	12
11	<i>Hattler v. Ashton</i> ,	
12	No. 16 Civ. 4099, 2017 WL 11634742 (C.D. Cal. Apr. 20, 2017)	12, 13, 20, 22
13	<i>hiQ Labs, Inc. v. LinkedIn Corp.</i> ,	
14	31 F.4th 1180 (9th Cir. 2022)	14, 16
15	<i>Horgan v. Macmillan, Inc.</i> ,	
16	789 F.2d 157 (2d Cir. 1986)	7
17	<i>I.M.S. Inquiry Mgmt. Sys. Ltd. v. Berkshire Info. Sys., Inc.</i> ,	
18	307 F. Supp. 2d 521 (S.D.N.Y. 2004)	21, 23
19	<i>Lasica v. Am. Online, Inc.</i> ,	
20	No. 15 Civ. 4230, 2015 WL 12791495 (C.D. Cal. Sept. 3, 2015)	14
21	<i>Lexmark Int’l, Inc. v. Static Control Components, Inc.</i> ,	
22	387 F.3d 522 (6th Cir. 2004)	<i>passim</i>
23	<i>LivePerson, Inc. v. 24/7 Customer, Inc.</i> ,	
24	83 F. Supp. 3d 501 (S.D.N.Y. 2015)	12, 20, 21
25	<i>MDY Indus., LLC v. Blizzard Ent., Inc.</i> ,	
26	629 F.3d 928 (9th Cir. 2010)	<i>passim</i>
27	<i>MGE UPS Sys., Inc. v. GE Consumer and Indus., Inc.</i> ,	
28	622 F.3d 361 (5th Cir. 2010)	11
	<i>Navistar, Inc. v. New Baltimore Garage, Inc.</i> ,	
	No. 11 Civ. 6269, 2012 WL 4338816 (N.D. Ill. Sept. 20, 2012)	12
	<i>In re NVIDIA Corp. Sec. Litig.</i> ,	
	No. 08 Civ. 4260, 2011 WL 4831192 (N.D. Cal. Oct. 12, 2011), <i>aff’d</i> , 768 F.3d	
	1046 (9th Cir. 2014)	25

1	<i>In re OpenAI, Inc. Copyright Infringement Litig.</i> ,	
2	No. 25 Civ. 4315, 2025 WL 3635559 (S.D.N.Y. Dec. 15, 2025).....	12, 17, 21, 24
3	<i>Project Travel, LLC v. Terra Dotta, LLC</i> ,	
4	No. 24 Civ. 2817, 2026 WL 890422 (M.D. Fla. Apr. 1, 2026)	12, 13
5	<i>Russell v. U.S. Dep’t of the Army</i> ,	
6	191 F.3d 1016 (9th Cir. 1999)	12
7	<i>Sullivan v. Flora, Inc.</i> ,	
8	936 F.3d 562 (7th Cir. 2019)	8
9	<i>TD Ameritrade, Inc. v. Matthews</i> ,	
10	No. 16 Civ. 136, 2017 WL 4812035 (D. Alaska Oct. 25, 2017)	12, 24
11	<i>U.S. v. Elcom Ltd.</i> ,	
12	203 F. Supp. 2d 1111 (N.D. Cal. 2002)	5
13	<i>Universal City Studios, Inc. v. Reimerdes</i> ,	
14	111 F. Supp. 2d 294 (S.D.N.Y. 2000).....	17, 22
15	<i>Universal City Studios v. Corley</i> ,	
16	273 F.3d 429 (2d Cir. 2001).....	5, 11, 16
17	<i>Van Buren v. U.S.</i> ,	
18	593 U.S. 374 (2021).....	16
19	<i>Yates v. U.S.</i> ,	
20	574 U.S. 528 (2015).....	21
21	Statutes	
22	17 U.S.C. § 101.....	8
23	17 U.S.C. § 102.....	8
24	17 U.S.C. § 106.....	13, 20
25	17 U.S.C. § 1201.....	<i>passim</i>
26	Rules	
27	Fed. R. Civ. P. 12.....	11
28	Other Authorities	
	Exemption to Prohibition on Circumvention of Copyright Protection Systems for	
	Access Control Technologies, 89 Fed. Reg. 85437, 85437 (Oct. 28, 2024).....	19
	H.R. REP. NO. 105-551 (1998).....	2, 4, 15

1	Melville B. Nimmer & David Nimmer, Nimmer on Copyright	6, 15, 18, 23
2	S. REP. NO. 105-190 (1998)	3, 4, 16
3	U.S. Copyright Off., Section 1201 Rulemaking: Ninth Triennial Proceeding to	
4	Determine Exemptions to the Prohibition of Circumvention (Oct. 2024),	
5	https://www.copyright.gov/1201/2024/2024_Section_1201_Registers_	
	Recommendation.pdf	18
6	U.S. COPYRIGHT OFF., THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998: U.S.	
7	COPYRIGHT OFF. SUMMARY (Dec. 1998)	5
8	U.S. COPYRIGHT OFFICE, SECTION 1201 OF TITLE 17: A REP. OF THE REG. OF	
9	COPYRIGHTS (June 2017)	5
10	<i>WIPO Copyright Treaties Implementation Act, and Online Copyright Liability</i>	
11	<i>Limitation Act: Hearing Before the H. Subcomm. on Courts and Intellectual</i>	
12	<i>Property of the H. Comm. on the Judiciary, 105th Cong. (1997).....</i>	3

MEMORANDUM OF POINTS AND AUTHORITIES

I. PRELIMINARY STATEMENT

Plaintiffs’ First Amended Complaint, like their original complaint, suffers from a fatal flaw: the Digital Millennium Copyright Act (“DMCA”) does not prohibit the conduct to which they object. Congress long has differentiated between controlling *access* to a work and controlling *use* of it. The question of whether a copyright owner has granted access thus differs from the question of whether that owner has permitted use. A painting might be kept under lock and key, hidden away in a box painted an opaque *black* on all sides that prevents anyone from seeing inside it from any angle. This black box is an “access control”: it protects against accessing the work inside at all; and by controlling access, the box forecloses all uses. Or the painting might be loaned to a museum; the museum in turn displays it inside a transparent *glass* box, for protection. The glass box is a “use control”: it controls some uses of the painting (like running it through a photocopier) but not others (like viewing it). Whereas an access control must address *all* uses of a work, a use control may address *specific* uses without necessarily affecting others.

The DMCA translated this framework into the digital environment. One DMCA provision, 17 U.S.C. § 1201(a), regulates black boxes: technological measures that effectively control all *access* to a work. Another provision, 17 U.S.C. § 1201(b), regulates glass boxes: technological measures that control certain *uses* of a work. Section 1201(a) thus covers breaking into a locked room to gain access, and § 1201(b) applies to what happens once inside.

Despite Plaintiffs’ revised complaint, the FAC still asserts a § 1201(a) black box claim for works that it alleges are protected, if anything, by only a § 1201(b) glass box. Plaintiffs allege that they posted audiovisual works to YouTube, and that any member of the public can see them there. No encryption. No password. No lock, with no key. Allegedly, YouTube employs technological measures to prevent unauthorized *downloading*. But because YouTube provides public *access* to Plaintiffs’ works, the alleged technological measures do not control access, as § 1201(a) requires.

In view of Plaintiffs’ allegations, the FAC continues to fail to state a claim for three independent reasons. *First*, the technological measures identified by the FAC are not alleged to control *access*. Instead, they control certain *uses*. To allow Plaintiffs’ claim to proceed would collapse § 1201’s two provisions in defiance of the Ninth Circuit’s express holding that § 1201 must be read so “neither section

1 is rendered superfluous.” *MDY Indus., LLC v. Blizzard Ent., Inc.*, 629 F.3d 928, 946 (9th Cir. 2010).
 2 Here, the FAC’s alleged technological measures all presuppose access: the FAC repeatedly and tellingly
 3 refers to the measures at issue as designed to “prohibit scraping, unauthorized downloading, bulk
 4 extraction, or other forms of data mining.” *E.g.*, FAC ¶¶ 76, 155. These are all types of *use*, not access.
 5 Plaintiffs cannot use technological jargon to overcome the FAC’s repeated concessions that YouTube
 6 provides public access to the works. The access alleged in the FAC is not limited by encryption,
 7 scrambling, passwords, or any other purported technological measures. Plaintiffs thus continue to assert
 8 a § 1201(a) black box claim for works that allegedly are protected, if anything, by only a § 1201(b) glass
 9 box: you can look, but you cannot copy. Section 1201(a) does not recognize such a claim.

10 **Second**, the alleged technological measures are not covered by § 1201(a) for the additional reason
 11 that the public allegedly need not encounter them to access Plaintiffs’ works. Section 1201(a)(3)(B)
 12 provides that a technological measure “effectively controls access” only when it, “in the ordinary course
 13 of its operation, requires” the application of information or a process to access the work. But *by Plaintiffs’*
 14 *own allegations*, members of the public in the ordinary course do not have to do anything to confront the
 15 alleged technological measures. As the statute’s plain language demands that a measure “*requires*” action
 16 in the ordinary course of operation, the alleged technological measures fall outside § 1201(a)’s scope.

17 **Third**, according to the FAC, Apple allegedly accessed the works without taking affirmative action
 18 to circumvent the alleged technological measures. Yet, the DMCA’s definition of “circumvention”
 19 requires an affirmative act taken against the technological measure analogous to descrambling or
 20 decrypting, or “breaking into a locked room in order to obtain a copy of a book.” *See* H.R. REP. NO. 105-
 21 551, pt. 1, at 17 (1998). This statutory requirement means that circumvention does not include
 22 *disregarding* a technological measure, nor does it include *complying* with one, including the reuse of valid
 23 passwords or other keys by unauthorized persons. Although Plaintiffs conclusorily refer to
 24 “circumvention,” the FAC contains no factual allegations of encrypted, scrambled, or otherwise locked
 25 *works*. Instead, it alleges that Apple disregarded or complied with YouTube’s measures, such as by using
 26 “valid” links. The DMCA requires more. Apple must have done something to the technological measures;
 27 looking into a glass box is not the same as breaking into a black box. And as discussed below, a box that
 28 is glass on five sides does not become a black box because its bottom is opaque. Plaintiffs’ failure to

1 allege that Apple circumvented a technological measure protecting their works dooms their claim.

2 The FAC thus fails thrice over, and for the same reasons as Plaintiffs' original complaint failed as
 3 well. Indeed, Apple's original motion to dismiss alerted Plaintiffs to these deficiencies, identifying the
 4 same three independent ways in which Plaintiffs failed to state a § 1201(a) claim. *See* Dkt. 28 (Mot.
 5 Dism.). Rather than curing these problems, Plaintiffs doubled down on them, attempting to use jargon to
 6 obscure these fatal flaws. Because Plaintiffs already have tried and failed to conform their allegations to
 7 the law, Apple respectfully requests that this Court dismiss the FAC with prejudice.

8 **II. STATEMENT OF ISSUES TO BE DECIDED**

- 9 • Whether Plaintiffs' First Amended Complaint should be dismissed with prejudice because it fails to
 10 state a claim under 17 U.S.C. § 1201(a), including because (1) the alleged technological measures are
 11 not access controls; (2) they do not operate in the ordinary course; and (3) disregarding or complying
 12 with technological measures is not "circumvention" within the meaning of § 1201(a)?

13 **III. BACKGROUND**

14 **A. The DMCA Created a Qualified Right Against Circumvention of Access Controls**

15 As the name suggests, the Digital Millennium Copyright Act brought two centuries of copyright
 16 principles into a new digital millennium. As then-Register of Copyrights Marybeth Peters testified during
 17 the DMCA's House hearing:

18 It has long been accepted in U.S. law that a copyright owner has the right to control access
 19 to his work, and may choose not to make it available to others or to do so only on set terms.
 20 This means not only that a copyright owner may keep a work forever unpublished, but also
 that he can publish it while controlling the conditions under which others are allowed to
 see it such as charging a fee or imposing restrictions on how the work may be used.

21 *WIPO Copyright Treaties Implementation Act, and Online Copyright Liability Limitation Act: Hearing*
 22 *Before the H. Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary*, 105th
 23 Cong., at 49 (1997) (statement of Marybeth Peters, Register of Copyrights, Copyright Office of the United
 24 States) ("Peters Testimony"). Before Congress passed the DMCA, however, the Copyright Act did not
 25 protect against unauthorized access: "the conduct of circumvention was never before made unlawful."
 26 S. REP. NO. 105-190, at 12 (1998).

27 In the mid-1990s, Congress determined that compliance with two recently ratified treaties made it
 28 "necessary" to create a new right against digital circumvention, distinct from an author's rights to control

1 use of copyrighted works. S. REP. NO. 105-190, at 12. In doing so, Congress recognized that U.S. law
 2 **already** balanced significant protections for authors with the public interest. Copyright already protected
 3 against certain unauthorized uses of works, and telecommunications laws and the Computer Fraud and
 4 Abuse Act (CFAA) already covered certain types of unauthorized access to works. *See* H.R. REP. NO.
 5 105-551, pt. 1, at 18 (citing 47 U.S.C. §§ 553, 605; 17 U.S.C. § 1002); S. REP. NO. 105-190, at 19 (citing
 6 18 U.S.C. § 1030). To balance these protections and non-copyright owners’ interest in maintaining access
 7 to published works, Congress “endeavored to specify, with as much clarity as possible, how the right
 8 against anti-circumvention would be qualified.” *See* H.R. REP. NO. 105-551, pt. 2, at 26 (1998).

9 Against this backdrop, the DMCA has two anti-circumvention provisions, only one of which is at
 10 issue in this case. Section 1201(a) applies to circumvention of technological measures designed to be
 11 “access controls,” and § 1201(b) applies to trafficking in devices that circumvent technological measures
 12 designed to be “use controls.” *Disney Enters., Inc. v. VidAngel, Inc.*, 869 F.3d 848, 863–64 (9th Cir.
 13 2017). These must be understood as different so “neither section is rendered superfluous.” *MDY*, 629
 14 F.3d at 946. More specifically, as a prohibition on circumvention of access controls, § 1201(a)(1) has
 15 been “analogized to the equivalent of a law against breaking and entering.” Peters Testimony at 49. “For
 16 example, if unauthorized access to a copyrighted work is effectively prevented through use of a password,
 17 it would be a violation of this section to defeat or bypass the password and to make the means to do so.”
 18 S. REP. NO. 105-190, at 11. Section 1201(a)(1) crucially “**does not apply** to the subsequent actions of a
 19 person once he or she has obtained authorized access to a copy of a work . . . **even if** such actions involve
 20 circumvention of additional forms of technological protection measures.” H.R. REP. NO. 105-551, pt. 1,
 21 at 18 (emphasis added). Section 1201(a) also prohibits trafficking in devices that enable circumvention
 22 of access controls, *see* § 1201(a)(2), but there are no allegations in this case about such conduct.

23 Section 1201(b), by contrast, “deals with measures that prevent acts of infringement, rather than
 24 access. **Such measures might include a technology that blocks users from downloading copies.**” Peters
 25 Testimony at 48 (emphasis added); *see also Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 387
 26 F.3d 522, 545 (6th Cir. 2004) (Section 1201(b) “prohibits devices aimed at circumventing technological
 27 measures that allow some forms of ‘access’ but restrict other uses of the copyrighted work, **such as**
 28 **streaming media**, which permits users to view or watch a copyrighted work but prevents them from

1 downloading a permanent copy of the work.” (emphasis added)). And in contrast to § 1201(a), § 1201(b)
 2 contains only a trafficking prohibition; “circumventing use restrictions is not unlawful.” *U.S. v. Elcom*
 3 *Ltd.*, 203 F. Supp. 2d 1111, 1121 (N.D. Cal. 2002). This was by design: as the Copyright Office concluded
 4 in its contemporaneous analysis of the DMCA, Congress intentionally prohibited the act of circumventing
 5 access controls, but not the act of circumventing use controls, to maintain the balance between the rights
 6 of authors and the public interest. *See* U.S. COPYRIGHT OFF., THE DIGITAL MILLENNIUM COPYRIGHT ACT
 7 OF 1998: U.S. COPYRIGHT OFF. SUMMARY 3–4 (Dec. 1998). Because both § 1201(a) and § 1201(b) focus
 8 narrowly on *circumvention* of specific technological measures (or trafficking in devices that enable
 9 circumvention), ultimate use of the work is not an element of a claim under either provision: the DMCA
 10 “does not concern itself with the *use* of [copyrighted] materials after circumvention has occurred” at all.
 11 *Universal City Studios v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001). As the Ninth Circuit held in *MDY*,
 12 claims dealing with potentially unlawful uses of a work—*i.e.*, infringement claims—therefore are
 13 “distinct” from § 1201 claims. *See MDY*, 629 F.3d at 950–52.

14 The technological measures at issue in these two provisions can be compared to an opaque black
 15 box and a transparent glass box. A § 1201(a) access control, like a black box, locks a work away from
 16 view altogether. Without opening the black box, the work remains entirely out of reach: a user must
 17 overcome the black box before the work can be read, viewed, or otherwise used in any way at all. An
 18 access control blocks *all* use. By contrast, a § 1201(b) use control, like a glass box, limits only specific
 19 uses. A user may be able admire a painting inside a glass box, but cannot run it through a photocopier.
 20 *See* U.S. COPYRIGHT OFF., SECTION 1201 OF TITLE 17: A REP. OF THE REG. OF COPYRIGHTS 6 (June 2017)
 21 (§ 1201(b) measures “include, for example, technology preventing the copying of an e-book after it has
 22 been downloaded to a user’s device.”). Quoting the Senate’s DMCA committee report, the Ninth Circuit
 23 thus held that § 1201(a) and § 1201(b) “*are not interchangeable*”:

24 If [a technological measure] does nothing to prevent access to the plain text of the work,
 25 but is designed to prevent that work from being copied, then a potential cause of action
 26 against the manufacturer of a device designed to circumvent the measure lies under
 27 § 1201(b)(1), but not under § 1201(a)(2). Conversely, if an effective technological
 28 protection measure limits access to the plain text of a work only to those with authorized
 access, but provides no additional protection against copying, displaying, performing or
 distributing the work, then a potential cause of action against the manufacturer of a device
 designed to circumvent the measure lies under § 1201(a)(2), but not under § 1201(b).

MDY, 629 F.3d at 946–47 (quoting S. REP. NO. 105-190, at 12) (emphasis added). Or, as the leading copyright treatise writes, § 1201(a) regulates breaking into a digital “house,” to see a work, whereas § 1201(b) focuses “on violating the ‘house rules.’” 4 Nimmer on Copyright § 12A.03[C].

B. Plaintiffs Allege That They Made Their Audiovisual Works Available to the Public

Plaintiffs’ allegations break from this foundation. Plaintiffs allege that they “are content creators who upload their audiovisual content to YouTube.” FAC ¶ 9. They do not allege that they independently implemented any anti-circumvention measures of their own. Instead, when they uploaded their content to YouTube, they allegedly “authoriz[ed] and instruct[ed] YouTube to provide protection to the video content through YouTube’s anti-circumvention software.” *Id.* ¶ 10.

Plaintiffs allege that when they uploaded videos to YouTube, they accepted YouTube’s Terms of Service. Through these Terms of Service, “content creators such as Plaintiffs who upload content onto YouTube *grant license[s] . . . to other users of YouTube to access content* through YouTube’s services.” FAC ¶ 77 (emphasis added). The Terms of Service distinguish this access license from a use license: according to the FAC, YouTube’s “license makes clear that it ‘does not grant any rights or permissions for a user *to make use* of [the] Content independent of the Service.’” *Id.* (quoting “Terms of Service,” YouTube, <https://www.youtube.com/t/terms>). YouTube’s Terms of Service also allegedly prohibit specific forms of use, including “scraping, unauthorized downloading, bulk extraction, or other forms of data mining of audiovisual content.” *Id.* ¶¶ 76, 81, 84, 125, 155; *see also id.* ¶ 146 (d) (allegedly common issue to proposed class is “[w]hether Defendant retrieved, scraped, downloaded or otherwise acquired” proposed class members’ videos). Plaintiffs thus repeatedly allege that YouTube users have access to any work uploaded to YouTube. *E.g., id.* ¶¶ 34 (“A ‘public’ video may be viewed by anyone.”); 35 (“YouTube’s ‘users’ . . . can watch and listen to videos without paying money.”), 42 (“YouTube permits members of the public to view audiovisual works through its platform. . . .”), 55 (“YouTube grants the public one narrow form of access to a given work.”); 78 (all users have “the ability to view (*i.e.*, stream) through YouTube’s controlled environment”), 93 (“YouTube allows users to stream content. . . .”).

When a creator uploads a video to YouTube, YouTube allegedly hosts the file for the video on its servers. *See* FAC ¶ 11. YouTube, in turn, “transmits segmented, time-limited portions of a work for

ephemeral playback” whenever a user demands it. *Id.* ¶ 44.² When YouTube does this, a user “experiences continuous playback” of the work, *id.* ¶ 45, but allegedly “the underlying file is still never released.” *Id.* ¶ 46. Thus, YouTube “hand[s] the user” “[a]ccess to the work” but not a “copy of the audiovisual file.” *Id.* YouTube does this by allegedly connecting a “page URL” that a user visits to an encrypted (or signed) and static “file URL” at which the file is stored. *Id.* ¶ 59.

Yet, just like the original complaint, Plaintiffs do not allege that the *files* are encrypted, scrambled, or otherwise protected at these digital locations; only the URLs are. FAC ¶ 59. And these file URL locations remain just URLs: they are publicly accessible Internet locations that can be accessed by anyone with an Internet connection. *Id.* Plaintiffs also do not allege that the videos a user watches are encrypted or scrambled. Rather, access to them is provided to YouTube users; that is the purpose of YouTube.³

Importantly, although Plaintiffs repeatedly seek to distinguish “videos,” “content,” and “files,” all of these terms represent the same allegedly copyright-protected audiovisual “works”: the “audiovisual works themselves” are “not . . . ‘files’ distinct from those works.” FAC ¶ 54. That means that although each audiovisual work may appear as a video or a file, or even as multiple video segments, it remains a single audiovisual work.⁴ And because Plaintiffs concede that they have made their *works* publicly

² Plaintiffs’ allegations about “segments” mean only that “the complete audiovisual file is never made available as a complete usable file on the viewer’s device.” FAC ¶ 45. But just as a reader looking at a single page of a book, or a music fan listening to a song that is delivered over the course of four minutes over a radio, would be said to have access to a work, so too access to segments of Plaintiffs’ videos over time is still access to the works at issue. *Cf. Horgan v. Macmillan, Inc.*, 789 F.2d 157, 162–63 (2d Cir. 1986) (use of small portion of larger work may infringe copyright in larger work). Plaintiffs do not allege that users can only ever see part of any work on YouTube; instead, entire works are accessible in sequential segments, which is exactly how a user would watch them anyway.

³ Plaintiffs also allege that a video may be designated “public,” “unlisted,” or “private.” FAC ¶ 34. All three types of videos, however, are accessible to people with knowledge of their *page* URLs for YouTube’s playback environment. *Id.* And Plaintiffs do not allege that the privacy designation for a video has any effect on its *file* URL, or that toggling between these settings somehow qualifies as a § 1201(a) technological measure. Regardless, the different privacy settings are immaterial as Plaintiffs’ videos must be public given that they had “over 4 billion views.” *Id.* ¶ 19.

⁴ Plaintiffs’ allegations about controlled access in YouTube’s “streaming architecture” (also called the playback environment), *e.g.*, FAC ¶¶ 2–3, do not change their allegations that the control is limited and focused on use, *id.* ¶ 105, or that the works are publicly available outside the playback environment, *id.* ¶ 48. Any attempt to allege other facts would be foreclosed by Plaintiffs’ prior representation to the Court that the files and videos represent the same work, regardless of where located or accessed. *See* Dkt. 1 (Compl.) ¶ 33; *see also* *Airs Aromatics, LLC v. Victoria’s Secret Stores Brand Mgmt., Inc.*, 744 F.3d 595, 600 (9th Cir. 2014) (“A party cannot amend pleadings to directly contradic[t] an earlier assertion made in the same proceeding.”). As a practical matter, to distinguish videos from files would make no sense: just as a person who can view a painting through a glass box has access to it even if the physical canvas cannot be touched, so too a person who can view a video

accessible, the gravamen of the FAC is that YouTube “protect[s] against file level access” by employing measures “to deter unauthorized *uses*.” *Id.* ¶ 47; *see also id.* ¶ 39 (“To enforce its *prohibitions on downloading* content, YouTube uses technological processes and tools to detect and block access to files for unauthorized downloading.” (emphasis added)).

Specifically, Plaintiffs reference five technological measures that fall into two categories. *First*, YouTube allegedly employs two *Automation Detectors* that are designed to differentiate among categories of users of YouTube’s playback environment:

- IP Blocking and Rate Limiting: Allegedly, YouTube “monitors network behavior” to prevent “excessive or abusive” use. FAC ¶ 61. YouTube thus allegedly “conditions continued [*i.e.*, preexisting] access to all content on the platform on compliance with YouTube’s authorized access parameters,” *i.e.*, its house rules. *Id.* If YouTube finds a violation, it allegedly then “blocks that IP address”—which already had access—from *further* “accessing *the YouTube platform*.” *Id.* (emphasis added). Plaintiffs do not allege that YouTube somehow blocks IP addresses from the otherwise-accessible file URLs (where the works also are located), or that a blocked user cannot access YouTube’s services exactly as intended, from a different IP address; instead, they allege some users do exactly that. *Id.* ¶ 68.
- CAPTCHA Challenges: When YouTube detects “automated or suspicious activity,” it allegedly “typically” (*i.e.*, sometimes but not always) “requires completion of a CAPTCHA challenge before allowing further requests to proceed.” *Id.* ¶ 67. In other words, when YouTube does not detect automated or suspicious activity, the CAPTCHA does not appear. And, when it does, the CAPTCHA challenge merely attempts to distinguish “human users from bots.” *Id.* As with YouTube’s alleged IP Blocking and Rate Limiting, Plaintiffs concede that YouTube’s CAPTCHA challenges will not trigger for a user who accesses YouTube from a

has access to the audiovisual work it represents regardless of the file location. Plaintiffs’ tautological allegation that a “work” is the “embodiment of the work,” FAC ¶ 51, thus is wrong both as a matter of common sense and as a matter of law. *See* 17 U.S.C. §§ 101 (distinguishing “works” from “copies” or “phonorecords”), 102 (distinguishing “original works of authorship” from “any tangible medium of expression”); *see also Sullivan v. Flora, Inc.*, 936 F.3d 562, 567–68 (7th Cir. 2019) (distinguishing works from copies). Moreover, the DMCA applies to measures that effectively control access to *works*, not copies. *See* 17 U.S.C. § 1201(a)(1)(A).

different IP address. *Id.* ¶ 68. Instead, such a user can access videos exactly as YouTube intends “without ever responding to” a CAPTCHA challenge. *Id.*

Second, YouTube allegedly employs three ***Playback Connectors*** that connect its playback environment to the files hosted on its servers. As discussed above, although YouTube allegedly hosts video files on the Internet at static, public locations, it allegedly “withhold[s]” that “usable file ***location***,” *i.e.*, the file URL, from users. FAC ¶ 58 (emphasis added). These alleged measures thus work like maps, revealing where on the Internet to find the (unencrypted) files.

- **Rolling Cipher**: The rolling cipher applies to the video file URL (the video’s “location”), not the video file itself (the work at issue). FAC ¶¶ 58–59. Plaintiffs do not allege that the file itself is encrypted, scrambled, or otherwise protected; or that users cannot access the video files directly. Instead, allegedly, “the file URL” is “encrypted”; YouTube’s playback environment allegedly decrypts the URL to reveal a different, static file URL. *Id.* ¶ 59. Thus, the rolling cipher “protects the true media file ***URL***” when accessed in YouTube’s playback environment; but because the rolling cipher protects only the URL and not the file itself, “valid file requests” to access the file may be generated “outside” the playback environment. *Id.* ¶ 105 (emphasis added). Once a user has a file URL, whether from a dataset or using a tool, the user can retrieve “the underlying video and audio file[] directly from YouTube’s servers” without decrypting or descrambling anything. *Id.* ¶ 106. A descrambling tool, if used, would reveal the file URL, but that says nothing about the video file located at that URL, which is delivered by YouTube’s servers notwithstanding the rolling cipher.
- **Session-Bound, Short-Lived URLs**: Similarly, YouTube allegedly issues “temporary” session-bound URLs that allow YouTube’s playback environment to retrieve the unencrypted files at these locations. *Id.* ¶ 65. The URLs thus allegedly “limit[] when and from where the file may be requested.” *Id.* Notably, the short-lived, generated URL is different from the static file URL: YouTube “generate[s]” it “***after*** a valid media URL is generated.” *Id.* (emphasis added). Thus, notwithstanding any alleged design by YouTube to connect its playback environment to the file URL circuitously, the file URL does not change. Further, these session-bound URLs can be renewed when they expire, and then function as intended. *Id.* ¶ 66.

- Proof-of-Origin Tokens: Plaintiffs allege that “requests for video segments include cryptographic proof-of-origin tokens that validate the request as originating from an authorized YouTube playback environment.” *Id.* ¶ 71. Allegedly, the tokens guide “data” from the file URL to the page URL because “YouTube’s servers validate these tokens before delivering any audiovisual data” *within* YouTube’s playback environment. *Id.* Yet, valid tokens also are validated the same for users “operating entirely outside the authorized playback environment” as they are for users operating within it. *Id.* ¶ 73. Valid tokens also can be “reuse[d].” *Id.*

C. Apple Allegedly Accessed Plaintiffs’ Publicly Accessible Works

Plaintiffs further allege that Apple accessed their publicly accessible videos notwithstanding the alleged technological measures described above. Plaintiffs allege two theories: either Apple accessed file URLs directly, or Apple complied with what the technological measures requested. **First**, although all the alleged technological measures apply *within* YouTube’s glass box playback environment, Plaintiffs allege Apple accessed their content “entirely *outside*” that environment by going “directly” to the file URLs. FAC ¶¶ 5, 41, 100–01, 105, 107, 115, 117, 128, 156 (emphasis added). Apple did this by “scraping” or “stream ripping” “video files directly from [YouTube’s] servers rather than viewing the content through the provider’s authorized playback environment.” *Id.* ¶ 101. Apple was able to do this because, according to the FAC, it allegedly had access to a dataset “compiled from . . . YouTube videos” that “functions as a map or index file identifying specific YouTube videos and clips by URL” and other identifiers. *Id.* ¶¶ 91, 93. The dataset thus “consist[s] entirely of pointers” but allegedly requires anyone in possession of it to retrieve “every referenced video directly from YouTube” at the listed URL. *Id.* ¶ 92. That is because the dataset allegedly does not “contain[] the underlying audiovisual files”—just the locations for them. *Id.* ¶ 98. Plaintiffs allege that Apple “used this dataset to initiate millions of individual downloads of protected YouTube content.” *Id.* ¶¶ 96, 98. Plaintiffs allege that their videos were logged in this map file, and that Apple thus accessed their videos by going to the locations specified therein without decrypting or descrambling anything at all. *Id.* ¶¶ 19, 22, 24.

Second, the FAC alleges that “[b]ulk extraction of YouTube videos at the scale alleged here” necessarily implicated YouTube’s purported technological measures. FAC ¶ 100. Plaintiffs thus allege that the Automation Detectors did not activate because Apple “implemented an IP-rotation scheme” “by

cycling through different IP addresses” that YouTube’s playback environment would validate in the same way it would validate any other IP address. *Id.* ¶¶ 109–13, 116. Plaintiffs further allege that the Playback Connectors did not activate because Apple “generate[d] valid file requests,” “obtain[ed] fresh authorization parameters and regenerate[d] valid links” to “maintain[] uninterrupted [*i.e.*, preexisting] access,” and “reus[ed]” valid tokens. *Id.* ¶¶ 73, 105–06, 115, 117. Plaintiffs allege that, having either not encountered or complied with these technological measures, Apple without authorization then downloaded, copied, used, or otherwise infringed their works. *E.g., id.* ¶¶ 1, 6–7, 13, 16–18, 38, 68, 82, 99–103, 106, 112–13, 115, 117–18, 120, 123–25, 131, 135–36, 140, 146, 149, 152, 159, 163. In other words, Plaintiffs’ objection is the unauthorized use of the works.

On April 3, 2026, Plaintiffs filed suit on behalf of themselves and a proposed class of content creators. Dkt. 1 (Compl.). Apple moved to dismiss, or, alternatively, strike Plaintiffs’ prayer for injunctive relief against infringement given that Plaintiffs asserted a single cause of action for circumvention, rather than infringement. Dkt. 28 (Mot. Dism.). On July 14, 2026, Plaintiffs filed the FAC, which reasserted the same cause of action. Dkt. 29 (FAC). Apple now moves to dismiss again.⁵

IV. ARGUMENT

“A motion to dismiss . . . under Rule 12(b)(6) tests the legal sufficiency of the claims alleged in the complaint.” *Ambrozewicz v. 6Sense Insights, Inc.*, 804 F. Supp. 3d 1026, 1030 (N.D. Cal. 2025). Dismissal may be based on either the “lack of a cognizable legal theory” or “the absence of sufficient facts alleged under a cognizable legal theory.” *Conservation Force v. Salazar*, 646 F.3d 1240, 1242 (9th Cir. 2011). “When evaluating such a motion, the court must accept all material allegations in the complaint

⁵ Despite Plaintiffs’ revision to their requested relief, they continue to allege that Apple “profited substantially from its **infringement**” (not from alleged circumvention), and they “seek[] an injunction and damages” for an infringement claim that they did not plead. *See* FAC ¶¶ 17–18 (emphasis added). Plaintiffs also now demand “impoundment and remedial destruction” of “audiovisual files obtained” as a result of circumvention. FAC at 35 ¶ d. The DMCA, however, “does not concern itself with the **use** of [copyrighted] materials **after** circumvention has occurred.” *Corley*, 273 F.3d at 443 (emphasis added); *see also* *MGE UPS Sys., Inc. v. GE Consumer and Indus., Inc.*, 622 F.3d 361, 366 (5th Cir. 2010) (DMCA “does not apply to the use of copyrighted works **after**” circumvention). Plaintiffs thus cannot seek this relief here. *See* *DISH Net., LLC v. Dimarco*, No. 11 Civ. 1962, 2012 WL 917812, at *5–6 (D. Nev. Mar. 14, 2012) (impounding devices used to violate § 1201(a)(2); finding “Plaintiffs recognize” that other products they requested be impounded “are not the proper targets of impoundment under the DMCA”); Dkt. 28 (Mot. Dism.) 23 (DMCA does not authorize injunction against “infringement”). Given these infirmities, Plaintiffs’ requested relief remains improper, and should be struck under Rule 12(f) for the reasons outlined in Apple’s original motion. *See* Dkt. 28 (Mot. Dism.) 22–24. If the FAC is not dismissed, Apple will re-raise this issue.

as true and construe them in the light most favorable to the non-moving party.” *Ambrozewicz*, 804 F. Supp. 3d at 1030. “[C]onclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to dismiss for failure to state a claim.” *Caviness v. Horizon Cmty. Learning Ctr., Inc.*, 590 F.3d 806, 812 (9th Cir. 2010). “[D]ismissal without leave to amend is appropriate where further amendment would be futile.” *Russell v. U.S. Dep’t of the Army*, 191 F.3d 1016, 1020 (9th Cir. 1999).

Because of the limited scope of § 1201(a), courts routinely dismiss § 1201(a) claims and deny amendment as futile where “the conduct alleged . . . is not actionable.” *Adobe Sys. Inc. v. A&S Elecs., Inc.*, No. 15 Civ. 2288, 2015 WL 13022288, at *8 (N.D. Cal. Aug. 19, 2015) (dismissing § 1201(a) claim for failure to allege “circumvention”); *see Hattler v. Ashton*, No. 16 Civ. 4099, 2017 WL 11634742, at *8 (C.D. Cal. Apr. 20, 2017) (dismissing § 1201(a) claim where the works were “accessible to the public”); *TD Ameritrade, Inc. v. Matthews*, No. 16 Civ. 136, 2017 WL 4812035, at *4 (D. Alaska Oct. 25, 2017) (dismissing § 1201(a) claim for failure to plead “facts to indicate that his hard drive had encryption technology that was circumvented”); *Ass’n for Info. Media and Equip. v. Regents of the Univ. of Cal.*, No. 10 Civ. 9378, 2012 WL 7683452, at *9–10 (C.D. Cal. Nov. 20, 2012) (dismissing § 1201(a) claim where “Plaintiffs essentially allege improper usage”); *Coupons, Inc. v. Stottlemire*, No. 07 Civ. 3457, 2008 WL 3245006, at *2–3 (N.D. Cal. July 2, 2008) (dismissing § 1201(a) claim after finding Plaintiff engaged in “Impermissible Blurring of § 1201(a) and § 1201(b)”).⁶

Here, the FAC should be dismissed with prejudice for three independent reasons.

A. The Alleged Technological Measures Are Not Access Controls

The FAC first should be dismissed because it does not contain allegations of technological measures that control *access*, just measures that purport to control *use*. As discussed above, § 1201(a) covers “technological measure[s] that effectively control[] access to a work,” whereas § 1201(b) covers

⁶ See also, e.g., *Project Travel, LLC v. Terra Dotta, LLC*, No. 24 Civ. 2817, 2026 WL 890422, at *6–7 (M.D. Fla. Apr. 1, 2026); *In re OpenAI, Inc. Copyright Infringement Litig.*, No. 25 Civ. 4315, 2025 WL 3635559, at *4–5 (S.D.N.Y. Dec. 15, 2025); *Emmerich Newspapers, Inc. v. Particle Media, Inc.*, No. 23 Civ. 26, 2025 WL 2146609, at *17–18 (S.D. Miss. July 29, 2025); *Couponcabin LLC v. Savings.com, Inc.*, No. 14 Civ. 39, 2016 WL 3181826, at *6 (N.D. Ind. June 8, 2016); *LivePerson, Inc. v. 24/7 Customer, Inc.*, 83 F. Supp. 3d 501, 510–11 (S.D.N.Y. 2015); *DISH Net. LLC v. World Cable Inc.*, 893 F. Supp. 2d 452, 464–66 (E.D.N.Y. 2012); *Navistar, Inc. v. New Baltimore Garage, Inc.*, No. 11 Civ. 6269, 2012 WL 4338816, at *4 (N.D. Ill. Sept. 20, 2012); *Ground Zero Museum Workshop v. Wilson*, 813 F. Supp. 2d 678, 692 (D. Md. 2011); *Burroughs Payment Sys., Inc. v. Symco Grp.*, No. 10 Civ. 3029, 2011 WL 13217738, at *5–6 (N.D. Ga. Dec. 13, 2011); *Egilman v. Keller & Heckman, LLP*, 401 F. Supp. 2d 105, 113 (D.D.C. 2005).

1 “technological measure[s] that effectively protect[] a right of a copyright owner under this title in a work
 2 or a portion thereof.” *Contrast* § 1201(a)(1)(A), with § 1201(b)(1)(A); *see supra* 3. These textual
 3 differences matter: as the Ninth Circuit has held, these differently worded provisions must be read to
 4 “ensure[] that neither section is rendered superfluous.” *See MDY*, 629 F.3d at 946.

5 The Ninth Circuit accordingly has rejected requiring a “nexus” to infringement for a § 1201(a)
 6 claim. *Id.* at 947. The Ninth Circuit, looking to the DMCA’s legislative history to confirm that the textual
 7 difference between § 1201(a) and § 1201(b) was intentional, held that “Congress created a new
 8 anticircumvention right in [§ 1201(a)] independent of traditional copyright infringement.” *Id.* at 946.
 9 Thus, “***where § 1201(a)(1) refers to technological measures that control ‘access’ to a protected work,***
 10 ***that section should be interpreted narrowly to exclude technologies that permit access to copyrighted***
 11 ***work, but restrict copying.*”** *Hattler*, 2017 WL 11634742, at *8; *cf. Columbia Pictures Indus., Inc. v.*
 12 *Fung*, 710 F.3d 1020, 1034 (9th Cir. 2013) (unauthorized “downloading” is a use that implicates the right
 13 of reproduction under § 106). And where access is provided, even under conditions that allow some uses
 14 but prohibit others, violation of those conditions of *use* is not a circumvention of an *access* control because
 15 access already was provided. *See Project Travel*, 2026 WL 890422, at *6 (“Importantly, [§ 1201(a)] is
 16 not concerned with people exceeding the alleged limits of their authority once given valid access.”).
 17 Section 1201(a) thus is a provision concerned with black boxes that prevent *all* uses of a work (infringing
 18 or not); it is § 1201(b) that regulates glass box technological measures that control *specific* uses. *See*
 19 *MDY*, 629 F.3d at 947 (noting “that bypassing a password and breaking into a locked room in order to
 20 read or view a copyrighted work would not infringe on any of the copyright owner’s exclusive rights under
 21 § 106,” yet may violate § 1201(a)).

22 According to the FAC, the technological measures at issue here generally do not require anything
 23 to access Plaintiffs’ works—they together form a glass box that (aims to) prevent unauthorized
 24 ***downloading*** but does nothing to stop access. Although Plaintiffs asserted a cause of action for
 25 circumvention of access controls, *see* FAC ¶ 18, their factual allegations describe purported use controls.
 26 For example, Plaintiffs allege that their intellectual property was “copied and used” due to purported
 27 circumvention—not that it was impossible to access the works at all absent circumventing the alleged
 28 technological measures. *Id.* ¶ 13; *see also id.* ¶ 86 (“YouTube implemented [its purported measures] in

its effort *to impede the downloading* of audiovisual content from its platform.” (emphasis added)). This makes sense, because Plaintiffs concede YouTube is designed to provide public access to works posted thereto. *E.g., id.* ¶ 55 (“YouTube grants the public one narrow form of access to a given work.”). Plaintiffs further allege that YouTube’s Terms of Service—which “describe and reinforce YouTube’s” technological measures—“expressly prohibit scraping, unauthorized downloading, bulk extraction, or other forms of data mining of audiovisual content.” *Id.* ¶¶ 76, 81, 84, 125; *see also id.* ¶ 146 (d) (allegedly common issue to proposed class is “[w]hether Defendant retrieved, scraped, downloaded or otherwise acquired” proposed class members’ videos). Yet Plaintiffs concede that these Terms of Service required them to “grant license . . . to other users of YouTube to access content.” *Id.* ¶ 77.

All of the acts YouTube allegedly prohibits thus presuppose access: without prior access, there is no data to mine and no video to download or otherwise use. *Cf. hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1197–98 (9th Cir. 2022) (“scraping” a public website is not “analogous to breaking and entering”). Claiming violation of the Terms of Service for use *after* access, however, is not sufficient to state a § 1201(a) claim. *See Ass’n for Info. Media and Equip.*, 2012 WL 7683452, at *9–10 (dismissing § 1201(a) claim where “Plaintiffs essentially allege improper usage” after access); *see also Lasica v. Am. Online, Inc.*, No. 15 Civ. 4230, 2015 WL 12791495, at *5 (C.D. Cal. Sept. 3, 2015) (§ 1201(b) case where “Plaintiff provided access to the Photograph—to Defendant as well as the general public—through Flickr.com”; holding that a “person who engages in prohibited usage of a copyrighted work to which [they have] lawful access does not fall afoul of any provision of [§] 1201”). Notably absent from the uses YouTube’s Terms of Service prohibit is access; instead, Plaintiffs allege the exact opposite: that YouTube’s Terms of Service expressly *authorize access*. FAC ¶ 77. Plaintiffs cannot state a § 1201(a) claim for circumvention of technological measures that—by design—presuppose and allow public access. And because Plaintiffs also have conceded that the audiovisual works at issue here are the same whether represented as a video or a file, *supra* 7 & n.4, that means YouTube places restrictions only on particular uses of works posted to its website. In other words, the alleged technological measures here fall under § 1201(b), if they are covered by the DMCA at all.

Consistent with the technological measures not controlling access, Plaintiffs allege that they control only certain—rather than all—*uses* of content. As to the Automation Detectors, YouTube

“conditions *continued* access” with a set of house rules that “automated . . . activity” is likely to violate. FAC ¶¶ 61, 67 (emphasis added). “*Continued* access” presupposes initial access, and as the well-known Nimmer treatise explains, § 1201(b), *not* § 1201(a), regulates the “house rules” that place conditions on use after initial access. 4 Nimmer on Copyright § 12A.03[C]. The Automation Detectors do nothing to stop access to the works themselves, which remain on YouTube’s public website, and, by Plaintiffs’ own allegations, are triggered only when YouTube detects particular categories of user behavior rather than for every user or request. *E.g.*, FAC ¶ 67. The Playback Connectors are even further afield, as they allegedly affect only URLs, not works themselves. As alleged, the Playback Connectors are three ways in which YouTube obscures file URLs when its playback environment tries to retrieve the unencrypted files stored at these locations. *E.g.*, FAC ¶¶ 58, 65, 71. Plaintiffs do not allege that these URLs are anything other than readily accessible on the Internet, and similarly they do not allege that the files available at these URLs are in any way protected. At best, the Playback Connectors explain how YouTube’s playback environment retrieves “data” from file URLs; but Plaintiffs do not allege they have any impact on users who go straight to the file URL to retrieve the work directly. It is the playback environment which in turn restricts downloading, like a glass box. *Id.* ¶¶ 36–38, 103.

As the House Report on the DMCA made clear, § 1201(a)(1) “does not apply to the subsequent actions of a person once he or she has obtained authorized access to a copy of a work . . . *even if* such actions involve circumvention of additional” technological measures. H.R. REP. NO. 105-551, pt. 1, at 18 (emphasis added). By giving the public access to their works via YouTube, Plaintiffs thus foreclosed their § 1201(a) claim. Both the files and the videos—two forms of the same work—are accessible by any member of the public at static URLs at any time.⁷ The alleged technological measures do nothing to control access. Rather, they seek to impose conditions on users who already have access, to limit their use of what they have access to: these are house rules, not locks on the house’s door.⁸

⁷ Because both the video and the file are not “distinct” but rather the same work, they are not separate “elements” of the work, as was the case in *MDY*. *Compare MDY*, 629 F.3d at 942–43 (differing access to “literal elements,” “individual non-literal elements,” and “dynamic non-literal elements”), *with Lexmark*, 387 F.3d at 546 (access to computer program’s “literal code” only).

⁸ Plaintiffs cannot save their claim by asserting that these alleged technological measures serve as both access and use controls. For that to be plausible, the technological measures would have to *first* control access (*e.g.*, by encrypting the work), *and then* also limit potential uses after access (*e.g.*, by allowing viewing but not downloading). *See Disney Enters.*, 869 F.3d at 864–65. Here, however, Plaintiffs allege that they gave the public access to their works notwithstanding the technological measures.

1 Because Plaintiffs admit that, by posting their videos to YouTube, they made the videos accessible
 2 to the public, the FAC does not state a claim under § 1201(a). *See Coupons*, 2008 WL 3245006, at *2–3
 3 (dismissing § 1201(a) claim alleging “security products prevent[ing] unauthorized **copying**” on the ground
 4 that it “blur[red] the carefully constructed distinction” between access controls and use controls).

5 **B. The Alleged Technological Measures Do Not Operate in the Ordinary Course**

6 In addition to (allegedly) protecting only use rather than access, the technological measures at
 7 issue do not operate in the ordinary course of operation; they therefore do not “**effectively** control[] access”
 8 to Plaintiffs’ works. As defined by 17 U.S.C. § 1201(a)(3)(B), “a technological measure ‘effectively
 9 controls access to a work’ if the measure, **in the ordinary course of its operation, requires** the application
 10 of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the
 11 work.” Effectively controlling access thus means that, in the **ordinary course of operation**, a user cannot
 12 even see the work without some affirmative act such as entering a password. Put otherwise, the access-
 13 control “box” must be a black box in the ordinary course of operation—it cannot be akin to a transition
 14 lens, where it starts out and may forever stay transparent glass until and unless something happens. *See*
 15 *Couponcabin*, 2016 WL 3181826, at *6 (dismissing § 1201(a) claim where “even after the Plaintiff’s
 16 implementation of ‘technological safeguards and barriers,’ its website remains accessible to users of
 17 servers and/or internet service providers that have not been blocked by the Plaintiff’s technology”).

18 If a user need not encounter the technological measure to view the work, the measure does not
 19 effectively control access. As Register Peters testified during the DMCA hearings, the “ordinary course
 20 of its operation” requirement means that § 1201(a) “exclude[s] technologies that may have the incidental
 21 or unintended effect of controlling access, or do so only when used in an unusual way.” Peters Testimony
 22 at 47. In the CFAA context, the Supreme Court and Ninth Circuit have referred to access restrictions as
 23 involving a “gates-up-or-down approach.” *Compare Van Buren v. U.S.*, 593 U.S. 374, 390 (2021); *hiQ*
 24 *Labs*, 31 F.4th at 1198, *with Corley*, 273 F.3d at 435 (DMCA measures are “digital walls”); *cf.* S. REP.
 25 NO. 105-190, at 19 (citing CFAA to explain new provisions of DMCA). DMCA cases have applied a
 26 similar understanding. In *MDY*, for example, the Ninth Circuit considered one alleged DMCA
 27 technological measure and held that because “a player need not encounter Warden to access [the works at
 28 issue,] Warden does not effectively control access.” *MDY*, 629 F.3d at 952. Likewise, the *OpenAI* court

1 considered another such alleged DMCA measure and held that “Robots.txt files instructing web crawlers
 2 to refrain from scraping certain content do not ‘effectively control’ access to that content any more than a
 3 sign requesting that visitors ‘keep off the grass’ effectively controls access to a lawn” because a user “may
 4 access the content without taking any affirmative step other than impertinently disregarding the request.”
 5 2025 WL 3635559, at *4. The Sixth Circuit thus has elaborated that the DMCA “requires the measure to
 6 control . . . access ‘effectively,’ and it seems clear that this provision does not naturally extend to a
 7 technological measure that restricts one form of access but leaves another route wide open.” *Lexmark*,
 8 387 F.3d at 547. For a technological measure to “effectively control access” to a work in the ordinary
 9 course of its operation, it therefore must be encountered by **all users**, and all users must **do something** to
 10 overcome it before they can access the work. For a technological measure to “effectively control access,”
 11 it must be the only gate, it must start down, and all users must pass through it; if a user can access the
 12 work by an open back door, a technological gate out front does not count.

13 A DVD example is instructive, as courts have held that DVDs control access by requiring
 14 decryption to view works contained on them. Possessing the DVD is not enough: one must decrypt it to
 15 see the content. In *Universal City Studios, Inc. v. Reimerdes*, for example, the court explained that “[o]ne
 16 **cannot** gain access to a CSS-protected work on a DVD **without** application of the three keys that are
 17 required by the software.” 111 F. Supp. 2d 294, 317–18 (S.D.N.Y. 2000) (emphasis added), *aff’d sub*
 18 *nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 437 (2d Cir. 2001) (“Without the player keys
 19 and the algorithm, a DVD player **cannot** access the contents of a DVD.” (emphasis added)). Relying on
 20 the DMCA’s legislative history, it explained that CSS “effectively controls access” to works on DVDs
 21 because, in the ordinary course of operation, it requires application of information or a process before the
 22 contents of DVDs become viewable, let alone copyable. *Id.* at 318. It thus found CSS “effectively controls
 23 access” based on the technology’s function, rather than its success rate. *Id.*; *see also Lexmark*, 387 F.3d
 24 at 547 (collecting cases considering measures effective where they “blocked access”; finding “access-
 25 control measure [that] left [a version of the work] freely readable” did not “effectively control[] access”).

26 Here, by contrast, the alleged technological measures, in the ordinary course of operation, do not
 27
 28

1 **require** any process or application of information to access Plaintiffs’ works.⁹ As an initial matter,
 2 YouTube controls two paths to the works—the videos and the files—and by design leaves the files
 3 available and unprotected. A user can “scrap[e]” the files notwithstanding **anything** the alleged
 4 technological measures purport to do. *E.g.*, FAC ¶ 101. Plaintiffs thus have alleged themselves into the
 5 front door/back door problem that the Sixth Circuit in *Lexmark* held precludes a DMCA claim. *See* 387
 6 F.3d at 547; *see also MDY*, 629 F.3d at 952–53 (Ninth Circuit quoting *Lexmark* for this proposition).

7 Beyond that, Plaintiffs allege that individual users need not apply any information or process to
 8 get past the alleged technological measures; they thus are **not** equivalent to locks or gates. The Automation
 9 Detectors, as the name indicates, merely detect automated users who use YouTube’s service in allegedly
 10 “**abnormal**” ways. FAC ¶ 61 (emphasis added). Then, and only then, they “typically” (but not always)
 11 require some users to enter information to continue seeing a work. *Id.* ¶ 67. The Automation Detectors
 12 presuppose access, and then allegedly seek to interrupt “**continued**” access if and only if they detect a
 13 user’s YouTube use is “excessive or abusive.” *Id.* ¶ 61 (emphasis added). Thus, **access** does not depend
 14 on passing through the gate; only use does. For all users of YouTube’s public playback environment, the
 15 gate starts up, allowing access; for some users, based on use, it allegedly may subsequently come down.
 16 Because the DMCA “affords no protection to technologies designed to discriminate between categories
 17 of users,” Plaintiffs cannot state a claim for measures that allegedly do just that. *See* 4 Nimmer on
 18 Copyright § 12A.06[C][5]. And because Plaintiffs also do not ever allege that the Automation Detectors
 19 have any effect whatsoever on a user seeking to access the works as they are stored at the file URL, the
 20 Automation Detectors have no effect on access to YouTube videos in the ordinary course of operation.
 21 Unsurprisingly, the Copyright Office already has concluded that measures analogous to the alleged
 22 Automation Detectors “**do not effectively control access** to a work” because “[t]hey do not require ‘the
 23 application of information, or a process or a treatment’—but instead require that users refrain from
 24 [certain] conduct.” U.S. Copyright Off., Section 1201 Rulemaking: Ninth Triennial Proceeding to
 25 Determine Exemptions to the Prohibition of Circumvention (“§ 1201 Rulemaking Rep.”) at 125 (Oct.

26 ⁹ Plaintiffs do not contend, nor reasonably could they, that watching advertisements would qualify as
 27 the application of information or a process. Plaintiffs do not allege, for example, that any of the
 28 purported technological measures YouTube employs affect YouTube’s delivery of advertisements.
 And Plaintiffs concede that no advertisements would appear when “accessing the underlying files of
 the work.” *See* FAC ¶ 35.

2024), https://www.copyright.gov/1201/2024/2024_Section_1201_Registers_Recommendation.pdf; *see also* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 89 Fed. Reg. 85437, 85437 (Oct. 28, 2024) (final rule adopting recommendations).

The Playback Connectors similarly do not require a user to do anything to access the **works**. The rolling cipher, for example, ensures only that YouTube’s playback environment is able to deliver a requested work. FAC ¶ 59. It does not protect the work itself, nor does it limit the ability of a user to access the file at the static file URL. Instead, within the playback environment, session-bound URLs allegedly are generated *after* a valid file URL is requested, and YouTube’s playback environment decrypts the file URL to allow the unencrypted work stored there to be viewed at the unencrypted page URL. *Id.* ¶¶ 59, 65; *see also id.* ¶ 71 (proof-of-origin tokens enable delivery of data from file URL to page URL). The Playback Connectors thus allegedly affect how YouTube’s two URLs for a work interact; they do not, however, protect access to the **work** itself, as the DMCA requires. *See* 17 U.S.C. § 1201(a)(1)(A). That is because, even with the benefit of amendment, Plaintiffs still do not allege that YouTube scrambles or encrypts the files themselves; instead, Plaintiffs have now alleged YouTube encrypts the content itself *only* when a user downloads it through unspecified means into their YouTube application for offline viewing. FAC ¶ 46. *But see* Dkt. 28 (Mot. Dism.) at 7–8 (alerting Plaintiffs that their original Complaint failed to allege works themselves are encrypted). Outside of that isolated use case (which Plaintiffs do not allege is at issue in this litigation, FAC ¶ 103), videos remain publicly accessible on YouTube’s free-to-watch website, and files remain publicly accessible on the Internet without descrambling or decryption.

The alleged technological measures do not control access to Plaintiffs’ works in the ordinary course of the measures’ operation because streaming—which Plaintiffs indisputably authorized the public to do—*is* access, and because none of them affect access to the corresponding files at the locations where those files are stored. As the technological measures do not control access in the ordinary course of operation, the FAC fails to state a claim for relief. *See MDY*, 629 F.3d at 952–53 (“[I]t does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works.” (quoting *Lexmark*, 387 F.3d at 547)); *see also Lexmark*, 387 F.3d at 546 (finding measures did not qualify for protection where “[a]nyone who buys a Lexmark printer may read the literal code of the Printer Engine Program directly from the printer memory, with or without the benefit of the authentication sequence, and

the data from the program may be translated into readable source code after which copies may be freely distributed”); *Hattler*, 2017 WL 11634742, at *8 (dismissing § 1201(a)(1) claim, and denying leave to amend as futile, where it was “uncontested that the Works are accessible to the public”).¹⁰

C. Apple Is Not Alleged to Have “Circumvented” the Technological Measures

In addition to the fact that the alleged technological measures are not covered by § 1201(a) for the two reasons discussed above, Apple is not alleged to have “circumvented” them as that term is defined in § 1201(a). “Circumvention” requires an affirmative act akin to breaking and entering; it cannot be accomplished by merely walking through an open back door. *See MDY*, 629 F.3d at 947; *see also LivePerson*, 83 F. Supp. 3d at 509 (“[A] person circumvents a technological measure only when he affirmatively performs an action that disables or voids the measure that was installed to prevent them from accessing the copyrighted material.”). Under § 1201(a), “to ‘circumvent a technological measure’ means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.” 17 U.S.C. § 1201(a)(3)(A). This definition differs from the one provided in § 1201(b), which defines “to circumvent protection afforded by a technological measure” as “avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure.” *Id.* § 1201(b)(2)(A). Under the canon of meaningful variation, “circumventing” for purposes of § 1201(a) must be different from the differently defined yet identical term in § 1201(b). *See MDY*, 629 F.3d at 945. The key difference between the two provisions is that § 1201(a) defines circumvention by reference to two examples that are absent from § 1201(b): “to descramble a scrambled *work*” and “to decrypt an encrypted *work*.” *See id.* (discussing the specific examples provided in § 1201(a)) (emphasis added).

The more general examples of circumvention in § 1201(a) thus must be understood with reference

¹⁰ That Plaintiffs have pleaded themselves out of a claim distinguishes this case from others involving YouTube. In *Cordova v. Huneault*, for example, the court found that the defendants “ignore[d] the allegations of” that complaint. 817 F. Supp. 3d 819, 833 (N.D. Cal. 2026). Here, it is what Plaintiffs alleged, not what they failed to allege, that precludes their claim. Moreover, Judge DeMarchi held that “whether the videos may be viewed by the public is immaterial [because the complaint] refers to technological measures intended to prevent unauthorized downloading.” *Id.* at 834. *But see Fung*, 710 F.3d at 1034 (“downloading” implicates the right of reproduction under 17 U.S.C. § 106); *supra* 3, 12 (technological measures controlling rights protected by § 106 are governed by § 1201(b), not § 1201(a)). And Plaintiffs also admit that downloading (*i.e.*, copying or using) and access in the form of streaming are “different value propositions” altogether. FAC ¶ 79.

1 to the two specific examples provided: descrambling and decrypting a **work**. Under the canon of *noscitur*
2 *a sociis*, “a word is known by the company it keeps”; thus, a court should “avoid ascribing to one word a
3 meaning so broad that it is inconsistent with its accompanying words.” *Yates v. U.S.*, 574 U.S. 528, 543
4 (2015). The other types of circumvention described, such as “avoid” or “bypass,” must be understood to
5 require some affirmative act akin to descrambling or decrypting the work; it is not enough for a § 1201(a)
6 defendant simply to have disregarded, or not encountered, an alleged technological measure altogether.
7 *See World Cable*, 893 F. Supp. 2d at 466 (“[T]he use of the words ‘avoid’ and ‘bypass’ in the statute, as
8 well as the remainder of the words describing circumvent, imply that a person circumvents a technological
9 measure only when he **affirmatively performs an action** that disables or voids the measure that was
10 installed to prevent them from accessing the copyrighted material.”); *see also LivePerson*, 83 F. Supp. 3d
11 at 509 (same). Similarly, the affirmative act must circumvent the “technological
12 measure *qua* technological measure”; “avoid[ing] and bypass[ing] **permission** to engage and move
13 through the technological measure from the measure’s author” does not suffice. *I.M.S. Inquiry Mgmt. Sys.*
14 *Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004).

15 Because “circumvention” requires an affirmative act analogous to descrambling or decrypting,
16 courts have refused to allow § 1201(a) claims where the defendant did nothing to disable the alleged
17 technological measure. In *World Cable*, for example, the court held that although “lying to convince the
18 Plaintiffs to open the door and then stealing, copying, and selling the content of the books inside the room
19 may violate other laws, they do not violate the DMCA.” 893 F. Supp. 2d at 465. Thus, it is not sufficient
20 for a defendant to convince a plaintiff to disable the technological measure; the defendant itself must do
21 so. Similarly, in *OpenAI*, the court held that “[a]t most, [Plaintiff] alleges that [Defendant] **disregarded**
22 the instructions” provided to its web crawler. 2025 WL 3635559, at *5 (emphasis added). The court then
23 held that “[t]his is not ‘circumvention’ under the DMCA,” and accordingly dismissed Plaintiff’s § 1201(a)
24 claim. *Id.* And in *Adobe*, Judge Armstrong dismissed a § 1201(a) claim with prejudice given the futility
25 of amending a complaint against “allegedly unauthorized distribution of otherwise genuine and valid serial
26 license keys.” 2015 WL 13022288, at *8. Where a defendant is not alleged to have done anything besides
27 disregard or comply with a technological measure, a claim for circumvention will not lie. Thus, selling
28 an unauthorized lock-picking set may violate § 1201(a), but using a valid key purchased secondhand does

not. Alternatively, a defendant must break a lock on a black box, not simply approach a mostly glass box from its side or use a valid key to unlock it.

The DVD example is again instructive. DVDs encrypt content, such that possession of the disc is insufficient to access content contained on it; a user also must decrypt the content. *See Reimerdes*, 111 F. Supp. 2d at 310 (“only players and drives containing the appropriate keys are able to decrypt DVD files and thereby play movies stored on DVDs”). A DVD is like a black box: a user cannot see the content inside without opening it. By contrast, the content on YouTube is, by Plaintiffs’ own allegations, readily accessible without decryption or any similar process. *Supra* 6. Plaintiffs do not, and cannot, allege that the files are encrypted either, because they are not. The alleged technological measures here allow access at all times to users who use the playback environment as YouTube intends or go to the file URL; they are analogous to a glass box painted black on some sides, and left transparent on others—if a user rotates the box, the work is accessible. Section 1201(a), however, does not cover alleged technological measures that leave a work accessible. *See MDY*, 629 F.3d at 952–53 (quoting *Lexmark*, 387 F.3d at 547).

As a result, Plaintiffs’ § 1201(a) claim also fails because they do not and cannot allege that *Apple* took any action to impair the alleged technological measures *qua* technological measures. Tellingly, even after amending their complaint, Plaintiffs still do not allege descrambling, decrypting, or any other affirmative form of circumvention. Instead, Plaintiffs continue to try to shoehorn their claim into § 1201(a) by using the terms “*avoidance and bypassing*.” FAC ¶ 160 (emphasis added). Because even these forms of circumvention require more than disregarding alleged technological measures, Plaintiffs’ conclusory invocation of these terms fails to state a claim. Indeed, Plaintiffs’ formulaic repetition throughout the FAC of statutory elements fails to state a claim where the substantive allegations do not describe a § 1201(a) violation. *See Hattler*, 2017 WL 11634742, at *3 (“A pleading that offers ‘labels and conclusions’ or ‘a formulaic recitation of the elements of a cause of action will not do.’” (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009))).

As to the Automation Detectors, Plaintiffs do not explain how these would have triggered for Apple if the Automation Detectors allegedly operate within the playback environment but Apple allegedly acted outside it. *Contrast* FAC ¶ 61 (IP blocking applies to “the YouTube platform”), *with id.* ¶¶ 101–02 (alleging scraping “directly from [YouTube’s] servers”). If Apple confronted the Automation Detectors

at all, Plaintiffs allege that Apple accessed Plaintiffs’ works exactly as any other user would. For example, Plaintiffs allege that the purported IP blocking affects “*continued* access,” which presupposes that Apple would have had initial access *without* confronting it. *Id.* ¶ 61 (emphasis added). Plaintiffs further allege that because Apple rotated through IP addresses, YouTube constantly gave Apple access to Plaintiffs’ works without forcing Apple to even see CAPTCHA challenges—meaning the measure functioned as designed. *Id.* ¶¶ 68, 116. Plaintiffs give the game away when they allege that this was “the digital equivalent of returning to a checkpoint in a fresh disguise bearing new credentials after having been turned away.” *Id.* ¶¶ 110–11. Taking these allegations as true, Apple returned to the checkpoint, presented itself as any other user would, and was allowed access as anyone else would have been. Apple did not *appear* as an authorized user; it *was* an authorized user. That is not circumvention. *See Adobe*, 2015 WL 13022288, at *8; *World Cable*, 893 F. Supp. 2d at 464 (“[U]sing deception to gain access to copyrighted material is not the type of circumvention that Congress intended to combat in passing the DMCA.”); *I.M.S.*, 307 F. Supp. 2d at 532.¹¹ The DMCA does not impose liability for “circumventing” measures where access is obtained without any affirmative action taken against the alleged measure. *See* 4 Nimmer on Copyright § 12A.06[C][5] (“[H]acking around password protection violates the statute; using an authorized password does not do so, even if the defendant who uses that password is not the individual to whom plaintiff issued it—and, indeed, is someone whom plaintiff actually wished to exclude from its site.”); *see also* § 1201 Rulemaking Rep. 125 (“Nor do the two ways in which proponents state that they evade [Automation Detectors] likely qualify as ‘circumvention’ within the scope of” § 1201.).

¹¹ Based on the “plain language of the statute,” the “use of the normal process” to gain access to a work does “not avoid or bypass [a] conditional access system because [it] use[s] the intended mechanism . . . in precisely the manner in which [it was] designed to function.” *World Cable*, 893 F. Supp. 2d. at 465–66 (collecting cases). Although some courts may have reached an alternate conclusion, they are a distinct minority. *See Adobe*, 2015 WL 13022288, at *8 n.8 (rejecting minority view); *Burroughs*, 2011 WL 13217738, at *5 (same; analogizing that “[i]f the homeowner loses [a door] key, or even if it is stolen, one can hardly say that the person using it, while certainly not authorized to enter, somehow ‘avoided or bypassed’ the doorlock. They actually used the doorlock in a manner intended by the lock’s technology.”). Moreover, even some cases in which that view appears to have been adopted have distinguishable facts. For example, in *Google LLC v. SerpApi, LLC*, the district court appeared in dicta to adopt the view that “misrepresenting the device, software, or location from which the queries are sent” may qualify as circumvention. No. 25 Civ. 10826, Dkt. 42, at 16 (N.D. Cal. July 20, 2026). Yet, there, the defendant was alleged to have made its browsers “appear like authorized users” by providing them “the authorization obtained by a different browser after” it complied with the technological measure. *Id.* By contrast, here, Plaintiffs allege that either authorization was not needed to access their works, or YouTube authorized Apple’s requests. FAC ¶¶ 61, 68, 110–11, 116.

As to the Playback Connectors, Plaintiffs meet the same obstacles. For reasons discussed above, they do not allege that Apple was required to encounter these measures to access their works. *See supra* 16. Indeed, Plaintiffs repeatedly allege that the Playback Connectors operate *within* the playback environment, but Apple acted *outside* it. *Contrast* FAC ¶¶ 58, 65, 71, *with id.* ¶¶ 105, 115, 117. By Plaintiffs’ own allegations, then, these measures were irrelevant to Apple’s purported operations; Apple’s disregard for them therefore does not equate to circumvention. *See OpenAI*, 2025 WL 3635559, at *4. Plaintiffs’ allegations further run headlong into the problem that led the *Adobe* court to dismiss a § 1201(a) claim without leave to amend, citing futility: Plaintiffs allege that *if* sometimes Apple was confronted by the Playback Connectors, Apple complied with them. Thus, to “circumvent” the need for a session-bound, short-lived media URL, Apple could simply “obtain fresh authorization parameters and regenerat[ing] *valid links*.” FAC ¶ 115 (emphasis added). Apple allegedly got past the rolling cipher by similarly “generat[ing] *valid file requests* outside the authorized player,” *id.* ¶ 105 (emphasis added), and past the proof-of-origin tokens by “reus[ing] credentials that YouTube’s token system generates”; Plaintiffs thus concede that these credentials are thus not merely “valid-appearing” but rather issued by YouTube itself. *Id.* ¶¶ 73, 117. As with the alleged circumvention of the Automation Detectors, “[s]uch conduct . . . is not covered by the DMCA.” *See Adobe*, 2015 WL 13022288, at *8 (collecting cases holding use of valid keys by an unauthorized person is not “circumvention” under DMCA).

Plaintiffs conclusorily invoke a “descrambling tool,” but the FAC makes clear such a tool was irrelevant to Apple’s alleged circumvention. According to the FAC, the purpose of a descrambling tool would be to identify file URLs, FAC ¶ 106, but Apple allegedly already possessed an index file providing the same information. *Id.* ¶ 94. Plaintiffs do not explain why Apple would have used a descrambling tool to obtain information it already possessed. The allegation also is legally irrelevant: accessing static, publicly accessible locations is not circumvention, regardless of how Apple learned of those locations. *See Digit. Drilling Data Sys., LLC v. Petrolink Servs., Inc.*, 965 F.3d 365, 376 (5th Cir. 2020) (holding that a technology that “may have effectively restricted certain unauthorized uses of [a] software” was not an access control in part because the relevant “data was stored in an open database file”); *see also TD Ameritrade*, 2017 WL 4812035, at *4 (dismissing § 1201(a) claim alleging unauthorized access to unencrypted hard drives); *Couponcabin*, 2016 WL 3181826, at *6 (no § 1201(a) violation where “website

remains accessible”). At bottom, Plaintiffs cannot get past their concessions that YouTube’s design made their works accessible.

Plaintiffs thus do not allege that Apple took any affirmative action against the alleged technological measures. Instead, they allege that Apple acted toward the technological measures as any other user would. Although they allege that Apple did not seek a license to access their works in the manner as other users, *e.g.*, FAC ¶ 123, these allegations are undercut by Plaintiffs’ concession that YouTube’s Terms of Use required Plaintiffs to give all users such a license. *Id.* ¶ 77. At best, Plaintiffs allege that Apple lacked authorization to also make use of Plaintiffs’ works, but this is irrelevant because Plaintiffs do not plead any claim related to use of audiovisual works. *See supra* 11 n.5, 12. To sustain their claim, Plaintiffs therefore seek to define “circumventing” a technological measure so broadly that it encompasses doing nothing at all to it. Section 1201(a) requires more than that; it defines “circumvention” narrowly and contextually to require affirmative acts taken against an alleged technological measure. Plaintiffs do not allege any such affirmative acts, so the FAC must be dismissed.

V. CONCLUSION

The fatal flaw central to the FAC is that all of the works that Plaintiffs posted to YouTube were accessible to the public, notwithstanding any technological measures put in place by YouTube. Plaintiffs do not allege that their works were encased in a black box; rather, they allege that—at best—their works were put on public display inside a glass box that restricted certain uses *after* access, which Plaintiffs allege Apple nevertheless was able to accomplish. Taking these allegations as true, Plaintiffs complain of conduct that § 1201(a) does not regulate. Apple therefore respectfully requests that the Court dismiss the First Amended Complaint. Moreover, because Plaintiffs already amended their complaint once and still failed to state a claim, they should not be permitted to amend it again; any such amendment would be futile. *See In re NVIDIA Corp. Sec. Litig.*, No. 08 Civ. 4260, 2011 WL 4831192 (N.D. Cal. Oct. 12, 2011) (dismissing complaint without leave to amend after finding that “[d]espite prior opportunity to amend, plaintiffs fail[ed] to plead” necessary element), *aff’d*, 768 F.3d 1046 (9th Cir. 2014). Apple therefore respectfully requests that dismissal be with prejudice.

1 DATED: July 28, 2026

Respectfully submitted,

2
3 /s/ Dale M. Cendali

4 Dale M. Cendali (SBN 1969070)
5 Joshua L. Simmons (*pro hac vice*)
6 Josh Berlowitz (*pro hac vice*)
7 KIRKLAND & ELLIS LLP
8 601 Lexington Avenue
9 New York, NY 10022
10 Telephone: (212) 446-4800
11 dale.cendali@kirkland.com
12 joshua.simmons@kirkland.com
13 josh.berlowitz@kirkland.com

14 Andrew M. Gass (SBN 259694)
15 Joseph R. Wetzel (SBN 238008)
16 Melanie M. Blunschi (SBN 234264)
17 Nicole C. Valco (SBN 258506)
18 LATHAM & WATKINS LLP
19 505 Montgomery Street, Suite 2000
20 San Francisco, California 94111
21 Telephone: (415) 391-0600
22 andrew.gass@lw.com
23 joe.wetzel@lw.com
24 melanie.blunschi@lw.com
25 nicole.valco@lw.com

26 Elana Nightingale Dawson (*pro hac vice*)
27 LATHAM & WATKINS LLP
28 555 Eleventh Street, NW, Suite 1000
Washington, D.C. 20004
Telephone: (202) 637-2200
elana.nightingaledawson@lw.com

Attorneys for Defendant
Apple Inc.

CERTIFICATE OF SERVICE

On July 28, 2026, I electronically filed the foregoing with the Clerk of the Court by using the CM/ECF system, which will send a notice of electronic filing to all persons registered for ECF. All copies of documents required to be served by Fed. R. Civ. P. 5(a) and L.R. 5-1 have been so served.

/s/ Dale M. Cendali
Dale M. Cendali