

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
COMPLAINT OR, ALTERNATIVELY,
TO STRIKE**

Judge: Hon. Richard Seeborg

Complaint Filed: April 3, 2026

Hearing Date: August 6, 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 August 6, 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 Courtroom
 4 12, 19th Floor, 450 Golden Gate Avenue, San Francisco, California 94102, Defendant Apple Inc. will and
 5 hereby does move the Court for an order dismissing under Federal Rule of Civil Procedure 12(b)(6)
 6 Plaintiffs Ted Entertainment, Inc., Matt Fisher, and Golfholics, Inc.'s ("Plaintiffs") Consolidated Class
 7 Action Complaint (the "Complaint") with prejudice, or, in the alternative, striking under Rule 12(f)
 8 immaterial and impertinent relief as identified herein. This Motion is made pursuant to the Federal Rules
 9 and is based upon this Notice; the attached Memorandum of Points and Authorities; any reply papers filed
 10 by Apple; the pleadings filed with this Court; and such other evidence, oral or documentary, and argument
 11 as may be presented at or before the hearing.

12 As set forth in the Motion, the Complaint should be dismissed with prejudice because Plaintiffs
 13 fail to state a claim for circumvention of effective access controls pursuant to 17 U.S.C. § 1201(a)(1)(A),
 14 or, in the alternative, the Complaint's prayer for relief relating to infringement or other use post-
 15 circumvention should be struck as immaterial and impertinent to such a claim. Accordingly, Apple
 16 requests that the Court dismiss the Complaint with prejudice, or, in the alternative, strike relief relating to
 17 infringement rather than circumvention.

18 DATED: July 1, 2026

19 Respectfully submitted,

20 /s/ Dale M. Cendali

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

23 Attorney for Defendant
 24 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 Allegedly Made Audiovisual Works Available to the Public on YouTube	6
C.	YouTube Provides Public Access to Plaintiffs’ Works	7
D.	Apple Allegedly Accessed Plaintiffs’ Publicly Accessible Works.....	9
IV.	ARGUMENT	10
A.	The Complaint Should Be Dismissed for Failure to State a Claim	10
1.	The Alleged Technological Measures Are Not Access Controls	11
2.	The Alleged Technological Measures Do Not Operate in the Ordinary Course	14
3.	Ignoring Alleged Technological Measures Is Not “Circumvention”	18
B.	Plaintiffs’ Infringement-Based Relief Should Be Struck.....	22
V.	CONCLUSION	24

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).....	10, 21
<i>Airs Aromatics, LLC v. Victoria's Secret Stores Brand Mgmt., Inc.</i> , 744 F.3d 595 (9th Cir. 2014)	24
<i>Ambrozewicz v. 6Sense Insights, Inc.</i> , 804 F. Supp. 3d 1026 (N.D. Cal. 2025)	10, 22
<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).....	10, 12
<i>Baton v. Ledger SAS</i> , 740 F. Supp. 3d 847 (N.D. Cal. 2024)	22
<i>Caviness v. Horizon Cmty. Learning Ctr., Inc.</i> , 590 F.3d 806 (9th Cir. 2010)	10
<i>Columbia Pictures Indus., Inc. v. Fung</i> , 710 F.3d 1020 (9th Cir. 2013)	23
<i>Conservation Force v. Salazar</i> , 646 F.3d 1240 (9th Cir. 2011)	10
<i>Cordova v. Huneault</i> , 817 F. Supp. 3d 819 (N.D. Cal. 2026)	17
<i>Couponcabin LLC v. Savings.com, Inc.</i> , No. 14 Civ. 39, 2016 WL 3181826 (N.D. Ind. June 8, 2016).....	11, 14, 21
<i>Coupons, Inc. v. Stottlemire</i> , No. 07 Civ. 3457, 2008 WL 3245006 (N.D. Cal. July 2, 2008).....	10, 14
<i>Digit. Drilling Data Sys., LLC v. Petrolink Servs., Inc.</i> , 965 F.3d 365 (5th Cir. 2020)	21
<i>DISH Network LLC v. World Cable Inc.</i> , 893 F. Supp. 2d 452 (E.D.N.Y. 2012)	11, 18, 19

¹ All internal quotation marks and citations have been omitted, and all emphasis is in the original source, unless otherwise noted.

1	<i>Disney Enters., Inc. v. VidAngel, Inc.</i> ,	
2	869 F.3d 848 (9th Cir. 2017)	4, 13, 14
3	<i>Egilman v. Keller & Heckman, LLP</i> ,	
4	401 F. Supp. 2d 105 (D.D.C. 2005)	11
5	<i>Emmerich Newspapers, Inc. v. Particle Media, Inc.</i> ,	
6	No. 23 Civ. 26, 2025 WL 2146609 (S.D. Miss. July 29, 2025)	11
7	<i>Ground Zero Museum Workshop v. Wilson</i> ,	
8	813 F. Supp. 2d 678 (D. Md. 2011)	11
9	<i>Hattler v. Ashton</i> ,	
10	No. 16 Civ. 4099, 2017 WL 11634742 (C.D. Cal. Apr. 20, 2017)	10, 11, 17, 20
11	<i>Hecox v. Little</i> ,	
12	104 F.4th 1061 (9th Cir. 2024)	24
13	<i>hiQ Labs, Inc. v. LinkedIn Corp.</i> ,	
14	31 F.4th 1180 (9th Cir. 2022)	12, 15, 16, 18
15	<i>Lasica v. Am. Online, Inc.</i> ,	
16	No. 15 Civ. 4230, 2015 WL 12791495 (C.D. Cal. Sept. 3, 2015)	12
17	<i>Lexmark Int'l, Inc. v. Static Control Components, Inc.</i> ,	
18	387 F.3d 522 (6th Cir. 2004)	<i>passim</i>
19	<i>LivePerson, Inc. v. 24/7 Customer, Inc.</i> ,	
20	83 F. Supp. 3d 501 (S.D.N.Y. 2015)	11, 18
21	<i>MDY Indus., LLC v. Blizzard Ent., Inc.</i> ,	
22	629 F.3d 928 (9th Cir. 2010)	<i>passim</i>
23	<i>MGE UPS Sys., Inc. v. GE Consumer and Indus., Inc.</i> ,	
24	622 F.3d 361 (5th Cir. 2010)	22
25	<i>Navistar, Inc. v. New Baltimore Garage, Inc.</i> ,	
26	No. 11 Civ. 6269, 2012 WL 4338816 (N.D. Ill. Sept. 20, 2012)	11
27	<i>In re OpenAI, Inc. Copyright Infringement Litig.</i> ,	
28	No. 25 Civ. 4315, 2025 WL 3635559 (S.D.N.Y. Dec. 15, 2025)	11, 15, 19
	<i>Project Travel, LLC v. Terra Dotta, LLC</i> ,	
	No. 24 Civ. 2817, 2026 WL 890422 (M.D. Fla. Apr. 1, 2026)	11
	<i>Ramachandran v. City of Los Altos</i> ,	
	359 F. Supp. 3d 801 (N.D. Cal. 2019)	22
	<i>Sullivan v. Flora, Inc.</i> ,	
	936 F.3d 562 (7th Cir. 2019)	17

1	<i>TD Ameritrade, Inc. v. Matthews</i> ,	
2	No. 16 Civ. 136, 2017 WL 4812035 (D. Alaska Oct. 25, 2017)	10, 21
3	<i>U.S. v. Elcom Ltd.</i> ,	
4	203 F. Supp. 2d 1111 (N.D. Cal. 2002)	5
5	<i>Universal City Studios, Inc. v. Reimerdes</i> ,	
6	111 F. Supp. 2d 294 (S.D.N.Y. 2000)	15, 16, 19
7	<i>Universal City Studios v. Corley</i> ,	
8	273 F.3d 429 (2d Cir. 2001)	5, 22
9	<i>Van Buren v. U.S.</i> ,	
10	593 U.S. 374 (2021)	15
11	<i>Whittlestone, Inc. v. Handi-Craft Co.</i> ,	
12	618 F.3d 970 (9th Cir. 2010)	23
13	<i>Yates v. U.S.</i> ,	
14	574 U.S. 528 (2015)	18
15	Statutes	
16	17 U.S.C. § 106	12, 23
17	17 U.S.C. § 501	23
18	17 U.S.C. § 1201	<i>passim</i>
19	17 U.S.C. § 1203	23
20	Rules	
21	Fed. R. Civ. P. 12	3, 10, 22, 24
22	Other Authorities	
23	Exemption to Prohibition on Circumvention of Copyright Protection Systems for	
24	Access Control Technologies, 89 Fed. Reg. 85437, 85437 (Oct. 28, 2024)	16
25	H.R. Rep. 105-551	2, 4, 14
26	Melville B. Nimmer & David Nimmer, <i>Nimmer on Copyright</i>	6, 15, 16, 20
27	S. Rep. 105-190	4
28	U.S. Copyright Off., Section 1201 Rulemaking: Ninth Triennial Proceeding to	
	Determine Exemptions to the Prohibition of Circumvention (Oct. 2024),	
	https://www.copyright.gov/1201/2024/2024_Section_1201_Registers_	
	Recommendation.pdf	16, 20

1	U.S. COPYRIGHT OFF., THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998: U.S.	
2	COPYRIGHT OFF. SUMMARY (Dec. 1998)	5
3	U.S. COPYRIGHT OFF., SECTION 1201 OF TITLE 17: A REP. OF THE REG. OF	
4	COPYRIGHTS (June 2017)	5
5	<i>WIPO Copyright Treaties Implementation Act, and Online Copyright Liability</i>	
6	<i>Limitation Act: Hearing Before the H. Subcomm. on Courts and Intellectual</i>	
7	<i>Property of the H. Comm. on the Judiciary, 105th</i>	3
8	WIPO Copyright Treaty, TRT/WCT/001, art. 11	4
9	WIPO Performances and Phonograms Treaty, TRT/WPPT/001, art. 18	4

MEMORANDUM OF POINTS AND AUTHORITIES

I. PRELIMINARY STATEMENT

The fatal flaw to Plaintiffs’ Complaint is that it pleads a claim under § 1201(a) of the Digital Millennium Copyright Act (“DMCA”) but alleges conduct that falls outside of it. Congress long has differentiated between controlling *access* to a copyrighted work and preventing others from making *use* of it. Once a copyright owner *first publishes its work*, the right to control use is narrower than before. 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 the box from any angle. This black box is an “access control”: it is designed to protect against accessing the work inside at all. Or the painting might be loaned to a museum; the museum in turn puts it on display inside a *transparent* glass box for protection. The glass box is a “use control”: it limits the uses that viewers may make of the work, but it does not prevent them from seeing it. Museum visitors can make some uses of the painting (like photographing themselves with it) but not others (like running it through a photocopier).

The DMCA translated this framework into the digital environment. Although DMCA cases—including this one—often involve technological jargon, the difference between access and use controls remains critical. One DMCA provision, 17 U.S.C. § 1201(a), regulates black boxes: technological measures that control *access* to a work. Another provision, § 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.

Plaintiffs’ Complaint fails because it 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 password. No payment. No lock. No key. Allegedly, YouTube employs technological measures to prevent unauthorized *downloading*. But because YouTube provides public access to the videos, the alleged technological measures do not control *access to the works*, as § 1201(a) requires.

In view of Plaintiffs’ own allegations, their Complaint fails to state a claim for three independent reasons. *First*, Plaintiffs’ claim fails because they do not allege that Apple circumvented a technological measure that controls *access*. Instead, the Complaint alleges that YouTube’s technological measures

control *use*. 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 is rendered superfluous.” *MDY Indus., LLC v. Blizzard Ent., Inc.*, 629 F.3d 928, 946 (9th Cir. 2010). Moreover, the Complaint’s alleged technological measures all presuppose access: it repeatedly and tellingly refers to the measures at issue as designed to prevent “scraping, unauthorized downloading, bulk extraction, or other forms of data mining,” “downloading, copying or distribution.” *E.g.*, Dkt. 1 (“Compl.”) ¶¶ 50, 62. These are all forms of *use*, not access. Because the technological measures purport to control use, Plaintiffs allege that their works are locked behind only glass boxes: you can look, but you cannot copy. This claim for circumventing glass boxes is not cognizable under § 1201(a).

Second, the alleged technological measures are not covered by § 1201(a) for the additional reason that the public allegedly can access Plaintiffs’ works without encountering the measures. Section 1201(a)(3)(B) provides that a technological measure “effectively controls access” to a work only when it, “in the ordinary course of its operation, requires” the application of information or a process to access the work. But *by Plaintiffs’ own allegations*, YouTube users may never encounter the measures when accessing Plaintiffs’ works because they trigger in limited situations and even then only sometimes. The statute’s plain language, however, demands that a measure “*requires*” action in the ordinary course of operation. The alleged technological measures therefore fall outside § 1201(a)’s scope.

Third, according to the Complaint, Apple may never have triggered these technological measures as it allegedly was able to access the works without doing anything to overcome them; that is not “circumvention.” Under the DMCA, “circumvention” requires an act analogous to descrambling or decrypting, or “breaking into a locked room in order to obtain a copy of a book.” *See* H.R. Rep. (I) 105-551 at 17. The Complaint contains no such allegations. Plaintiffs conclusorily recite the statutory definition of “circumvention,” then allege that Apple simply disregarded YouTube’s purported measures. The DMCA and the case law that has interpreted it require more than that. Apple must have done *something* to overcome the technological measures to gain access to the works; circumventing a glass box by looking into it is not the same as breaking into a black box. And as discussed below, a box that is glass on five sides does not become a black box because its bottom is opaque. That Apple allegedly accessed works Plaintiffs purposefully made publicly available does not give rise to a § 1201(a) claim.

In addition to the Complaint requiring dismissal *in toto*, certain requested relief should be struck because it is irrelevant to Plaintiffs’ anti-circumvention claim. Plaintiffs inflated their Complaint by filling it with “immaterial” and “impertinent” allegations about use (including infringement) *after* access. *See* Fed. R. Civ. P. 12(f). These irrelevant allegations permeate Plaintiffs’ Complaint. Plaintiffs then doubled down, requesting relief from *infringement*, not circumvention. Because the Ninth Circuit has held that circumvention and infringement claims are “distinct” causes of action, these allegations and prayer for relief have no bearing on the case at hand. *See MDY*, 629 F.3d at 950–52. Accordingly, Apple respectfully requests that the Complaint be dismissed with prejudice under Rule 12(b)(6) or, in the alternative, that requested relief from infringement be struck under Rule 12(f).

II. STATEMENT OF ISSUES TO BE DECIDED

- Whether Plaintiffs’ Complaint should be dismissed because it fails to state a claim under 17 U.S.C. § 1201(a), including because (1) the alleged technological measures here are not access controls; (2) the alleged technological measures do not operate in the ordinary course; and (3) ignoring technological measures is not “circumvention” within the meaning of § 1201(a)?
- Whether a prayer for relief related to infringement should be struck from the Complaint, which alleges a violation of only § 1201(a)?

III. BACKGROUND

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

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

It has long been accepted in U.S. law that a copyright owner has the right to control access to his work, and may choose not to make it available to others or to do so only on set terms. 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.

WIPO Copyright Treaties Implementation Act, and Online Copyright Liability Limitation Act: Hearing Before the H. Subcomm. on Courts and Intellectual Property of the H. Comm. on the Judiciary, 105th Cong. 49 (1997) (statement of Marybeth Peters, Register of Copyrights, Copyright Office of the United States) (“Peters Testimony”). Before Congress passed the DMCA, the Copyright Act did not protect

1 against unauthorized access: “the conduct of circumvention was never before made unlawful.” S. Rep.
2 105-190 at 12. In the 1990s, the United States ratified two multilateral treaties that required signatories
3 to “provide adequate legal protection and effective legal remedies against the circumvention of effective
4 technological measures that are used by authors in connection with the exercise of their rights.” WIPO
5 Copyright Treaty, TRT/WCT/001, art. 11; *see also* WIPO Performances and Phonograms Treaty,
6 TRT/WPPT/001, art. 18.

7 To implement this protection, Congress determined that it was “necessary” to create a new right
8 against digital circumvention, distinct from an author’s rights against infringement. S. Rep. 105-190 at
9 12. In doing so, Congress recognized that U.S. law already balanced significant protections for authors
10 of creative works with the public interest. For example, it already prohibited certain types of unauthorized
11 use of works. *Id.* And telecommunications laws and the Computer Fraud and Abuse Act already covered
12 certain types of unauthorized access to works. *See* H.R. Rep. 105-551 (I) at 18 (citing 47 U.S.C. §§ 553,
13 605; 17 U.S.C. § 1002); S. Rep. 105-190 at 19 (citing 18 U.S.C. § 1030). To balance these protections
14 and non-copyright owners’ interest in maintaining access to published works, Congress “endeavored to
15 specify, with as much clarity as possible, how the right against anti-circumvention would be qualified.”
16 *See* H.R. Rep. (II) 105-551 at 26.

17 Against this backdrop, the DMCA has two anti-circumvention provisions, only one of which is at
18 issue in this case. Section 1201(a) applies to circumvention of technological measures designed to be
19 “access controls,” and § 1201(b) applies to trafficking in devices that circumvent technological measures
20 designed to be “use controls.” *Disney Enters., Inc. v. VidAngel, Inc.*, 869 F.3d 848, 863–64 (9th Cir.
21 2017). These must be understood as different so “neither section is rendered superfluous.” *MDY*, 629
22 F.3d at 946. More specifically, as a prohibition on circumvention of access controls, § 1201(a)(1) has
23 been “analogized to the equivalent of a law against breaking and entering.” Peters Testimony at 49. “For
24 example, if unauthorized access to a copyrighted work is effectively prevented through use of a password,
25 it would be a violation of this section to defeat or bypass the password and to make the means to do so.”
26 S. Rep. 105-190 at 11. Section 1201(a)(1), however, “does not apply to the subsequent actions of a person
27 once he or she has obtained authorized access to a copy of a work protected under Title 17, even if such
28 actions involve circumvention of additional forms of technological protection measures.” H.R. Rep. (I)

1 105-551 at 18. Section 1201(a) also prohibits trafficking in devices that enable circumvention of access
 2 controls, *see* § 1201(a)(2), but there are no allegations in this case about anyone distributing such a device.

3 Section 1201(b), by contrast, “deals with measures that prevent acts of infringement, rather than
 4 access. Such measures might include a technology that blocks users from downloading copies.” Peters
 5 Testimony at 48; *see also Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 545 (6th
 6 Cir. 2004) (Section 1201(b) “prohibits devices aimed at circumventing technological measures that allow
 7 some forms of ‘access’ but restrict other uses of the copyrighted work, such as streaming media, which
 8 permits users to view or watch a copyrighted work but prevents them from downloading a permanent copy
 9 of the work.”). And in contrast to § 1201(a), § 1201(b) contains only a trafficking prohibition;
 10 “circumventing use restrictions is not unlawful.” *U.S. v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1121 (N.D.
 11 Cal. 2002). This was by design: as the Copyright Office concluded in its initial analysis of the DMCA,
 12 Congress intentionally prohibited the act of circumventing access controls, but not the act of
 13 circumventing use controls, to maintain the balance between the rights of authors of creative works and
 14 the public interest. *See* U.S. COPYRIGHT OFF., THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998: U.S.
 15 COPYRIGHT OFF. SUMMARY 3–4 (Dec. 1998). Because both § 1201(a) and § 1201(b) focus narrowly on
 16 ***circumvention*** of specific technological measures (or trafficking in devices that enable circumvention),
 17 ultimate use of the work is not an element of a claim under either provision: the DMCA “does not concern
 18 itself with the ***use*** of [copyrighted] materials after circumvention has occurred” at all. *Universal City*
 19 *Studios v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001). As the Ninth Circuit held in *MDY*, claims dealing
 20 with potentially unlawful uses of a work—i.e., infringement claims—therefore are “distinct” from § 1201
 21 claims. *See MDY*, 629 F.3d at 950–52.

22 The technological measures at issue in these two provisions can be compared to an opaque black
 23 box and a transparent glass box. A § 1201(a) access control, like a black box, locks a work away from
 24 view altogether. Without opening the black box, the work remains entirely out of reach: a user must
 25 overcome the black box before the work can be read, viewed, or otherwise used in any way. A § 1201(b)
 26 use control, like a glass box, leaves a work in plain sight but prevents making certain uses of it. A user
 27 can read a novel inside a glass box, but cannot make copies of it. *See* U.S. COPYRIGHT OFF., SECTION
 28 1201 OF TITLE 17: A REP. OF THE REG. OF COPYRIGHTS 6 (June 2017) (§ 1201(b) measures “include, for

1 example, technology preventing the copying of an e-book after it has been downloaded to a user's
 2 device.”). Quoting the Senate’s DMCA committee report, the Ninth Circuit has held that “*the [two*
 3 *provisions] are not interchangeable*”:

4 If [a technological measure] does nothing to prevent access to the plain text of the work,
 5 but is designed to prevent that work from being copied, then a potential cause of action
 6 against the manufacturer of a device designed to circumvent the measure lies under
 7 § 1201(b)(1), but not under § 1201(a)(2). Conversely, if an effective technological
 8 protection measure limits access to the plain text of a work only to those with authorized
 9 access, but provides no additional protection against copying, displaying, performing or
 10 distributing the work, then a potential cause of action against the manufacturer of a device
 11 designed to circumvent the measure lies under § 1201(a)(2), but not under § 1201(b).

12 *MDY*, 629 F.3d at 946–47 (quoting S. Rep. 105-190 at 12) (emphasis added). Or, as the leading copyright
 13 treatise writes, § 1201(a) prohibits breaking into a digital “house” to see a work, whereas § 1201(b)
 14 focuses “not on breaking in but on violating the ‘house rules.’” 4 Nimmer on Copyright § 12A.03[C].

15 **B. Plaintiffs Allegedly Made Audiovisual Works Available to the Public on YouTube**

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

21 Plaintiffs allege that when they uploaded their videos to YouTube, they accepted YouTube’s
 22 Terms of Service. Through these Terms of Service, “content creators such as Plaintiffs who upload
 23 content onto YouTube grant license[s] to YouTube for certain uses as well as to other users of YouTube
 24 *to access content* through YouTube’s services.” *Id.* ¶ 63 (emphasis added). The Terms of Service
 25 distinguish this right of access from a right of use: according to the Complaint, YouTube’s “license makes
 26 clear that it ‘does not grant any rights or permissions for a user *to make use* of [the] Content independent
 27 of the Service.’” *Id.* (quoting “Terms of Service,” YouTube, <https://www.youtube.com/t/terms>) (emphasis
 28 added). 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 except
 through expressly permitted features or licensed APIs.” *Id.* ¶ 62. Plaintiffs thus repeatedly allege that
 YouTube users have access to any work uploaded to YouTube. *Id.* ¶¶ 34 (“YouTube’s ‘users’—the

individuals who view the digital content available on YouTube—can watch and listen to videos for free.”),
 35 (“While *YouTube permits members of the public to view audiovisual works* through its platform, such
 permission is limited to access through YouTube’s authorized playback environment.” (emphasis added)),
 64 (all users have “the ability to view (*i.e.*, stream) through YouTube’s controlled environment”), 79
 (“YouTube allows users to stream content.”).

C. YouTube Provides Public Access to Plaintiffs’ Works

When a creator uploads a video to YouTube, YouTube allegedly hosts the file for the video on its
 servers. *See id.* ¶ 11. This file is “located” on YouTube’s servers yet accessible over the Internet by
 anyone with knowledge of its location; it is maintained at a stable, unchanging URL. *See id.* ¶ 49.
 Plaintiffs do not allege that the files are encrypted, scrambled, or otherwise protected at these digital
 locations. The video contained in the file, meanwhile, can be streamed on YouTube’s website at a
 different, stable, unchanging URL. *Id.* ¶ 34. Importantly, although Plaintiffs repeatedly distinguish
 between access to “videos” and access to “files,” they also allege that each video and file represents a
 single work: as alleged, the videos and the files “collectively comprise the copyrighted work and are not
 distinct from it.” *Id.* ¶¶ 33, 46 (alleging the “audiovisual works themselves” are “not . . . ‘files’ distinct
 from those works”). Thus, each of Plaintiffs’ alleged videos and its respective file are the same work, and
 accessing either one constitutes access to the work, which is the underlying creative expression regardless
 of the medium in which it is embodied.

Because Plaintiffs concede that they have made their *works* publicly accessible, the gravamen of
 their Complaint is that YouTube nevertheless protects the *files* for Plaintiffs’ works against “scraping or
 bulk downloading.” *Id.* ¶ 66. Specifically, the Complaint describes five technological measures that fall
 into two categories. *First*, YouTube allegedly employs *Automation Detectors* that are designed to
 differentiate among categories of users of YouTube’s playback environment. The Automation Detectors
 aim to limit the ability of automated “bots” to “retriev[e] large numbers of videos at scale.” *Id.* ¶ 53.
 YouTube “monitors network behavior” to prevent abuse, and “[r]equests from an IP address that exceeds
 defined thresholds *may* be throttled, denied, or blocked.” *Id.* ¶ 52 (emphasis added). According to the
 Complaint, YouTube thus “restrict[s] automated access to YouTube’s underlying video files.” *Id.* ¶ 55.
 It also allegedly employs “Session-bound, short-lived URLs,” which “initiate[] new authorized sessions”

1 in YouTube’s playback environment by “retriev[ing]” the underlying file. *Id.* ¶¶ 56–57. The URLs thus
 2 allegedly “limit[] when and from where the file may be requested.” *Id.* ¶ 56. According to the Complaint,
 3 “automated scraping tools can maintain continuous access” by “programmatically renewing expired
 4 credentials and initiating new authorized sessions at machine speed.” *Id.* ¶ 57. Notably, however, the
 5 short-lived, generated URL is different from the file URL: YouTube “issu[es]” it “*after* a valid media
 6 URL is generated.” *Id.* ¶ 56 (emphasis added). Thus, the media URL is static and publicly available,
 7 notwithstanding any alleged design by YouTube to circuitously connect its playback environment to the
 8 media URL. Finally, Plaintiffs allege that “[w]hen traffic patterns indicate automated or suspicious
 9 activity, YouTube *may* require completion of a CAPTCHA challenge” that interrupts the ability of the
 10 playback environment to “obtain the data necessary to retrieve the audiovisual file.” *Id.* ¶ 58 (emphasis
 11 added).

12 ***Second***, YouTube allegedly employs ***File Location Maps***. According to the Complaint, although
 13 video files hosted by YouTube are readily accessible on the Internet at static locations, YouTube does not
 14 outright tell users their digital locations. *Id.* ¶¶ 8, 34–37. As alleged, “YouTube maintains two different
 15 URLs for any given video: the page URL,” which is where the user watches the video, and “the file URL,”
 16 where the video file itself lives. *Id.* ¶ 50. Allegedly, the file URL (and only the file ***URL***) “is encrypted
 17 using a complex and periodically changing algorithm—the rolling cipher—that is designed to impede
 18 external access to the underlying YouTube files.” *Id.* But although the file URL is encrypted, Plaintiffs
 19 do not allege that the file URL ever changes, nor that the file at that URL is itself encrypted. This alleged
 20 measure is thus akin to a treasure map: the underlying files remain available on the Internet, for free, to
 21 anyone who knows their location. YouTube also allegedly requires that “requests for video segments
 22 include cryptographic tokens demonstrating that the request originates from . . . the intended playback
 23 context” before YouTube will provide the treasure map to the underlying, unencrypted file. *Id.* ¶ 60. This
 24 second form of File Location Map, however, still provides only the information of ***how*** to find the readily
 25 accessible file, which represents the same work as the readily accessible video. Tellingly, Plaintiffs do
 26 not allege that this is the ***only*** way to obtain the unchanging file URL, or that the file at that location is
 27 otherwise scrambled or encrypted.

D. Apple Allegedly Accessed Plaintiffs' Publicly Accessible Works

Even though Plaintiffs intentionally made their videos readily accessible by the public, they allege that Apple “scrap[ed]” or “stream ripp[ed]” their videos by accessing the “video files directly from [YouTube’s] servers rather than viewing the content through the provider’s authorized playback environment.” *Id.* ¶ 87. The video in YouTube’s authorized playback environment and the file on YouTube’s server are, by Plaintiffs’ own allegations, the same work. *Id.* ¶¶ 33, 46. According to the Complaint, Apple accessed the files outside YouTube’s playback environment because it already knew their locations and did not need YouTube’s architecture to function as a treasure map. Plaintiffs allege that Apple possessed a dataset that itself “functions as a map” because it contains “location identifiers that point to millions of YouTube videos or clips.” *Id.* ¶¶ 76, 80, 84. Plaintiffs allege that their videos were logged in this index file, and that Apple thus accessed their videos by going to the readily accessible locations specified therein. *Id.* ¶¶ 19, 22, 24, 85.

According to Plaintiffs, Apple never encountered the alleged technological measures. They allege that Apple (1) “implemented an IP-rotation scheme,” *id.* ¶¶ 95–98; (2) “obtain[ed] fresh authorization parameters and regenerate[d] valid links,” *id.* ¶ 100; and (3) “distributed requests across numerous machines.” *Id.* ¶ 101. These acts all meant that the Automation Detectors never triggered for Apple. Plaintiffs also allege that Apple (4) used a tool to generate “valid file requests outside the authorized player environment and thereby obtain the underlying media files directly,” *id.* ¶ 91; and (5) “operate[d] outside” YouTube’s playback environment “to retrieve video data directly.” *Id.* ¶ 102. These acts allegedly meant that Apple knew the file locations without need for the File Location Maps. Plaintiffs allege that, having not encountered these technological measures, Apple downloaded their works. *E.g., id.* ¶¶ 6–7, 17–18, 89, 91–92, 94–98, 100, 102, 105, 110.

On April 3, 2026, Plaintiffs filed suit on behalf of themselves and “[a]ll persons and entities in the United States who are creators and/or rights-holders of YouTube-hosted videos that Apple accessed at the file level by scraping, downloading, or otherwise extracting underlying video files from YouTube through circumvention of YouTube’s” technological measures. *Id.* ¶ 114. Plaintiffs asserted a single cause of action for violation of § 1201(a)(1)(A) of the DMCA, claiming that Apple engaged in unauthorized circumvention to “facilitate[] [its] ongoing and mass-scale”—but not asserted—“copyright infringement.”

Id. ¶ 137. Due to supposed “acts of infringement,” *id.* ¶ 139, Plaintiffs requested relief including “equitable relief . . . as is necessary to prevent or restrain infringement of Plaintiffs’ and the Class Members’ copyright-protected content.” Dkt. 1, Prayer for Relief, at 26 ¶ d.

IV. ARGUMENT

A. The Complaint Should Be Dismissed for Failure to State a Claim

“A motion to dismiss a complaint 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 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,” however. *Caviness v. Horizon Cmty. Learning Ctr., Inc.*, 590 F.3d 806, 812 (9th Cir. 2010).

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

1 “Impermissible Blurring of § 1201(a) and § 1201(b)”². Here, the Complaint should be dismissed for
 2 three independent reasons.

3 1. The Alleged Technological Measures Are Not Access Controls

4 The Complaint first should be dismissed because it does not contain allegations of technological
 5 measures that control **access**, just measures that purport to control **use**. As discussed above, § 1201(a)
 6 covers “technological measure[s] that effectively controls access to a work,” whereas § 1201(b) covers
 7 “technological measure[s] that effectively protect[] a right of a copyright owner under this title in a work
 8 or a portion thereof.” Compare § 1201(a)(1)(A), with § 1201(b)(1)(A); see *supra* 3. These textual
 9 differences matter: as the Ninth Circuit has held, these differently worded provisions must be read to
 10 “ensure[] that neither section is rendered superfluous.” See *MDY*, 629 F.3d at 946.

11 The Ninth Circuit accordingly has rejected requiring a “nexus” to infringement for a § 1201(a)
 12 claim. *Id.* at 947. The Ninth Circuit, looking to the DMCA’s legislative history to confirm that the textual
 13 difference between § 1201(a) and § 1201(b) was intentional, held that “Congress created a new
 14 anticircumvention right in [§ 1201(a)] independent of traditional copyright infringement.” *Id.* at 946.
 15 Thus, “**where § 1201(a)(1) refers to technological measures that control ‘access’ to a protected work,**
 16 **that section should be interpreted narrowly to exclude technologies that permit access to copyrighted**
 17 **work, but restrict copying.**” *Hattler*, 2017 WL 11634742, at *8 (emphasis added). And where access is
 18 provided, even under certain conditions of use, violation of those conditions of use is not a circumvention
 19 of an access control because access already was provided. See *Project Travel*, 2026 WL 890422, at *6
 20 (“Importantly, [§ 1201(a)] is not concerned with people exceeding the alleged limits of their authority
 21 once given valid access.”). Section 1201(a) thus is a provision concerned with black boxes that prevent
 22 **all** uses of a work (infringing or not); it is § 1201(b) that regulates technological measures that control

23
 24 ² See also, e.g., *Project Travel, LLC v. Terra Dotta, LLC*, No. 24 Civ. 2817, 2026 WL 890422, at *6–7
 25 (M.D. Fla. Apr. 1, 2026); *In re OpenAI, Inc. Copyright Infringement Litig.*, No. 25 Civ. 4315, 2025
 26 WL 3635559, at *4–5 (S.D.N.Y. Dec. 15, 2025); *Emmerich Newspapers, Inc. v. Particle Media, Inc.*,
 27 No. 23 Civ. 26, 2025 WL 2146609, at *17–18 (S.D. Miss. July 29, 2025); *Couponcabin LLC v.*
 28 *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 Network 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); *Egilman v. Keller & Heckman, LLP*,
 401 F. Supp. 2d 105, 113 (D.D.C. 2005).

1 infringing uses (i.e., glass boxes). *See MDY*, 629 F.3d at 947 (noting “that bypassing a password and
 2 breaking into a locked room in order to read or view a copyrighted work would not infringe on any of the
 3 copyright owner’s exclusive rights under § 106,” yet may violate § 1201(a)).

4 According to the Complaint, the technological measures at issue here generally do not require
 5 anything to access Plaintiffs’ works—they are glass boxes that (aim to) prevent unauthorized **downloading**
 6 but do nothing to stop access in the first place. Although Plaintiffs asserted a cause of action for
 7 circumvention of access controls, *see* Compl. ¶ 132, their factual allegations describe purported use
 8 controls. For example, Plaintiffs allege that their intellectual property was “copied and used” due to
 9 purported circumvention—not that it was impossible to access the works at all absent engaging with or
 10 circumventing the alleged technological measures. *Id.* ¶ 13; *see also id.* ¶ 72 (“YouTube implemented [its
 11 purported measures] in its effort **to impede the downloading** of audiovisual content from its platform.”
 12 (emphasis added)). This makes sense, because Plaintiffs concede YouTube is designed to provide public
 13 access to works posted thereto. *Id.* ¶ 2. Plaintiffs further allege that YouTube’s Terms of Service, which
 14 “describe and reinforce YouTube’s” technological measures, “expressly prohibit scraping, unauthorized
 15 downloading, bulk extraction, or other forms of data mining of audiovisual content except through
 16 expressly permitted features or licensed APIs.” *Id.* ¶¶ 62, 129; *see also id.* ¶ 120(d) (allegedly common
 17 issue to proposed class is “[w]hether Defendant retrieved, scraped, downloaded or otherwise acquired”
 18 proposed class members’ videos). These Terms of Service, however, make clear that “content creators
 19 such as Plaintiffs who upload content onto YouTube grant license . . . to other users of YouTube to access
 20 content.” *Id.* ¶ 63.

21 All YouTube’s prohibited acts thus presuppose access: without prior access, there is no data to
 22 mine and no video to download or otherwise acquire. *Cf. hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180,
 23 1197–98 (9th Cir. 2022) (in parallel CFAA context, “scraping” a publicly accessible website is not
 24 “analogous to breaking and entering”); *see also id.* at 1186 (at issue were “technological systems to detect
 25 suspicious activity and restrict automated scraping”). Claiming violation of the Terms of Service for use
 26 after access, however, is not sufficient to state a § 1201(a) claim. *See Ass’n for Info. Media and Equip.*,
 27 2012 WL 7683452, at *9–10 (dismissing § 1201(a) claim where “Plaintiffs essentially allege improper
 28 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,” and the court held 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 Section 1201”). Notably absent from the list of what YouTube’s Terms of Service prevent is access; instead, Plaintiffs allege the exact opposite: that YouTube’s Terms of Service expressly *authorize access*. Compl. ¶ 63.

Plaintiffs cannot state a § 1201(a) claim for circumvention of technological measures that—by design—made Plaintiffs’ works readily accessible by the general public. *Id.* ¶ 2 (“YouTube allows the public to view audiovisual works”). And because the video and the file are the same work, *id.* ¶¶ 33, 46, that means Plaintiffs’ works are readily accessible notwithstanding the alleged technological measures, too.

In addition to Plaintiffs affirmatively alleging that their works are publicly accessible, they do not allege that the measures described in the Complaint would prevent such access:

- The Automation Detectors apply only to some users and seek only to limit those users’ ability to *download* files. As alleged, the Automation Detectors limit the ability of certain users in some circumstances to “retriev[e]” video *files*, which are downloadable forms of Plaintiffs’ videos. *E.g., id.* ¶ 36. They do nothing, however, to stop access to the works themselves, which remain on YouTube’s public website.
- The File Location Maps condition only provision of the file location; they do nothing to prevent accessing YouTube videos on YouTube, nor do they affect a user who already knows the file locations. As explained above, both of YouTube’s File Location Maps provide only the static file URL to users who do not otherwise know it; they have no effect on users who can and do go directly to the file URLs in the first place. *See supra* 7.

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. 105-551 (I) at 18 (emphasis added). By giving the public access to at least some form of their works via YouTube, Plaintiffs thus foreclosed their

§ 1201(a) claim.³ Both the files and the videos—the two forms of the same work at issue here—are accessible by any member of the public, for free, at static URLs, at any time.⁴ 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.⁵

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

2. The Alleged Technological Measures Do Not Operate in the Ordinary Course

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

³ Plaintiffs allege that “YouTube offers downloading options to subscribers who pay,” Compl. ¶ 69, but Plaintiffs do not otherwise allege any differences between paying and non-paying users. Plaintiffs thus concede that public access to their works is free.

⁴ Because both the video and the file are not “distinct” but rather the same work, they are not multiple “elements” of the work, as was the case in *MDY*. *Compare MDY*, 629 F.3d at 942–43 (comparing access to “literal elements,” “individual non-literal elements,” and “dynamic non-literal elements”), with *Lexmark*, 387 F.3d at 546 (discussing access to computer program’s “literal code”); *see also* Compl. ¶ 33 (“The segmented streams and underlying media representations obtained by Defendant collectively comprise the copyrighted work and are not distinct from it.”).

⁵ 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, which allegedly control only use, if they effectively control anything at all.

1 website remains accessible to users of servers and/or internet service providers that have not been blocked
2 by the Plaintiff’s technology”).

3 If a user need not encounter the technological measure to view the work, the measure does not
4 effectively control access. As Register Peters testified during the DMCA hearings, the “ordinary course
5 of its operation” requirement means that § 1201(a) “exclude[s] technologies that may have the incidental
6 or unintended effect of controlling access, or do so only when used in an unusual way.” Peters Testimony
7 at 47. Considering one such measure in *MDY*, the Ninth Circuit held that as “a player need not encounter
8 Warden to access [the works at issue,] Warden does not effectively control access.” *MDY*, 629 F.3d at
9 952. The Sixth Circuit reasoned similarly that the DMCA “requires the measure to control . . . access
10 ‘effectively,’ and it seems clear that this provision does not naturally extend to a technological measure
11 that restricts one form of access but leaves another route wide open.” *Lexmark*, 387 F.3d at 547. And the
12 *OpenAI* court held that “Robots.txt files instructing web crawlers to refrain from scraping certain content
13 do not ‘effectively control’ access to that content any more than a sign requesting that visitors ‘keep off
14 the grass’ effectively controls access to a lawn” because a user “may access the content without taking
15 any affirmative step other than impertinently disregarding the request.” 2025 WL 3635559, at *4. Thus,
16 for a technological measure to effectively control access to a work in the ordinary course of its operation,
17 it must be encountered by **all users**, and all users must **do something** to overcome the technological
18 measure and thereby access the work. In the analogous CFAA context, courts have referred to similar
19 access restrictions as involving a “gates-up-or-down approach.” Compare *Van Buren v. U.S.*, 593 U.S.
20 374, 390 (2021); *hiQ Labs*, 31 F.4th at 1198, with 4 Nimmer on Copyright § 12A.06[C][5].

21 A DVD example is instructive because courts have held that DVDs control access by requiring
22 decryption to view works contained on them. In *Universal City Studios, Inc. v. Reimerdes*, for example,
23 the court noted that “One cannot gain access to a CSS-protected work on a DVD without application of
24 the three keys that are required by the software. One cannot lawfully gain access to the keys except by
25 entering into a license . . . or by purchasing a DVD player or drive containing the keys pursuant to such a
26 license.” 111 F. Supp. 2d 294, 317–18 (S.D.N.Y. 2000). Relying on the DMCA’s legislative history, it
27 explained that CSS “effectively controls access” to works on DVDs because it “actually works” in the
28 ordinary course of operation to require application of information or a process before the contents of

1 DVDs become viewable. *Id.* at 318. It thus found CSS “effectively controls access” based on the
2 technology’s function, rather than its success rate. *Id.*; *see also Lexmark*, 387 F.3d at 547 (collecting cases
3 considering measures effective where they “blocked access”; finding “access-control measure [that] left
4 [a version of the work] freely readable” did not “effectively control[] access”).

5 Here, by contrast, the alleged technological measures, in the ordinary course of operation, do not
6 **require** anything to see Plaintiffs’ works. The Automation Detectors, as the name indicates, merely detect
7 automated users who use YouTube’s service in allegedly “abnormal” ways. Compl. ¶ 54. Then, and only
8 then, they “may” or “can” (but also may not) require some selected users to enter information to continue
9 seeing a work. *Id.* ¶¶ 54, 58. Alternatively, they may simply require a user to initiate a new request (which
10 will be granted) rather than relying on an old one. *Id.* ¶ 57. By Plaintiffs’ own allegations, the Automation
11 Detectors have no effect on users who are not selected by YouTube’s algorithms, which, in the ordinary
12 course of operation, is all human users and at least some automated users. The DMCA, however, “affords
13 no protection to technologies designed to discriminate between categories of users.” *See* 4 Nimmer on
14 Copyright § 12A.06[C][5]; *see also hiQ Labs*, 31 F.4th at 1201 (alleged technological measures did not
15 control authorized access for purposes of CFAA because they worked only sometimes for only some users
16 who used LinkedIn’s services in an unusual way). They therefore do not “effectively control access” to
17 anything; notwithstanding the Automation Detectors, users initiating requests for access via YouTube’s
18 playback environment are granted access. Unsurprisingly then, the Copyright Office already has
19 concluded that technological measures analogous to the alleged Automation Detectors “do not effectively
20 control access to a work as contemplated by Section 1201” because “[t]hey do not require ‘the application
21 of information, or a process or a treatment’—but instead require that users refrain from [certain] conduct.”
22 U.S. Copyright Off., Section 1201 Rulemaking: Ninth Triennial Proceeding to Determine Exemptions to
23 the Prohibition of Circumvention (“Section 1201 Rulemaking Rep.”) at 125 (Oct. 2024),
24 https://www.copyright.gov/1201/2024/2024_Section_1201_Registers_Recommendation.pdf; *see also*
25 Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control
26 Technologies, 89 Fed. Reg. 85437, 85437 (Oct. 28, 2024) (final rule adopting Copyright Office’s
27 recommendations).

1 The File Location Maps similarly do not require a user to do anything to access the **works**. When
 2 a user accesses YouTube’s public website, the user gains access to the work, which is the content itself,
 3 regardless of the tangible medium in which it is expressed, i.e., as the supposed video or the file. *See*
 4 *Sullivan v. Flora, Inc.*, 936 F.3d 562, 567–68 (7th Cir. 2019). And Plaintiffs concede that the video and
 5 the file are the same work, merely two sides of that same coin. Compl. ¶¶ 33, 46. The DMCA, however,
 6 protects access to the **work**. *See* 17 U.S.C. § 1201(a)(1)(A). In addition to the fact that a user can access
 7 the work as a video regardless of whether the user knows the file’s location, it is YouTube—not the user—
 8 that identifies the file **location**. *See* Compl. ¶ 50. And **even then**, YouTube does not descramble or
 9 decrypt the files themselves when accessing them. *E.g., id.* ¶ 91. Those files, like the videos that constitute
 10 the same work, remain publicly accessible on the Internet without descrambling or decryption, by
 11 Plaintiffs’ own allegations. *See id.* ¶ 2.⁶

12 The alleged technological measures do not disrupt access to Plaintiffs’ works in the ordinary
 13 course of any of the measures’ operation because streaming—which Plaintiffs indisputably authorized the
 14 public to do—**is** access. As the technological measures do not limit the ability of a user to stream
 15 Plaintiffs’ works, they do not control access. The Complaint thus fails to state a claim for relief. *See*
 16 *MDY*, 629 F.3d at 952; *see also Lexmark*, 387 F.3d at 546 (finding measures did not qualify for protection
 17 where “[a]nyone who buys a Lexmark printer may read the literal code of the Printer Engine Program
 18 directly from the printer memory, with or without the benefit of the authentication sequence, and the data
 19 from the program may be translated into readable source code after which copies may be freely
 20 distributed”); *Hattler*, 2017 WL 11634742, at *8 (dismissing § 1201(a)(1) claim, and denying leave to
 21 amend as futile, where it was “uncontested that the Works are accessible to the public”).

22
 23 ⁶ That Plaintiffs have pleaded themselves out of a claim distinguishes this case from others involving
 24 YouTube. In *Cordova v. Huneault*, for example, the court found that the defendants “ignore[d] the
 25 allegations of” that complaint. 817 F. Supp. 3d 819, 833 (N.D. Cal. 2026). Here, it is what Plaintiffs
 26 alleged, not what they failed to allege, that precludes their claim. Moreover, Judge DeMarchi held
 27 that “whether the videos may be viewed by the public is immaterial [because the Complaint] refers to
 28 technological measures intended to prevent unauthorized downloading.” *Id.* at 834. Yet, here, the
 technological measures prevent only unauthorized downloading, but that is not protected by § 1201(a),
 and Plaintiffs concede that the works are accessible without encountering them. *Supra* 9; *see also*,
e.g., Compl. ¶¶ 2, 33, 46. Indeed, Plaintiffs admit that access and downloading (i.e., copying or using)
 are “different value propositions” altogether. Compl. ¶ 65.

3. Ignoring Alleged Technological Measures Is Not “Circumvention”

In addition to the fact that the alleged technological measures are not covered by § 1201(a) for the two reasons discussed above, Apple did not “circumvent” 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 door. *See MDY*, 629 F.3d at 947; *see also hiQ Labs*, 31 F.4th at 1197–98 (applying similar understanding to CFAA analysis). 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)).

The more general examples of circumvention in § 1201(a) thus must be understood with reference to the two specific examples provided: descrambling and decrypting. Under the canon of *noscitur a sociis*, “a word is known by the company it keeps,” and thus a court should “avoid ascribing to one word a meaning so broad that it is inconsistent with its accompanying words, thus giving unintended breadth to the Acts of Congress.” *Yates v. U.S.*, 574 U.S. 528, 543 (2015). The other types of circumvention described, such as “avoid” or “bypass,” therefore must be understood to require some affirmative act akin to descrambling or decrypting; it is not enough for a § 1201(a) defendant simply to have ignored, or not encountered, the alleged technological measures altogether. *See DISH*, 893 F. Supp. 2d at 466 (“[T]he use of the words ‘avoid’ and ‘bypass’ in the statute, as well as the remainder of the words describing circumvent, imply that 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.”); *see also LivePerson*, 83 F. Supp. 3d at 509 (same).

1 Because “circumvention” requires an affirmative act analogous to descrambling or decrypting,
2 courts have refused to allow § 1201(a) claims where the defendant did nothing to disable the alleged
3 technological measure. In *DISH*, for example, the court held that although “lying to convince the Plaintiffs
4 to open the door and then stealing, copying, and selling the content of the books inside the room may
5 violate other laws, they do not violate the DMCA.” 893 F. Supp. 2d at 465. Thus, it is not sufficient for
6 a defendant to convince a plaintiff to disable the technological measure; the defendant itself must do so.
7 Similarly, in *OpenAI*, the court held that “[a]t most, [Plaintiff] alleges that [Defendant] **disregarded** the
8 instructions” provided to its web crawler. 2025 WL 3635559, at *5 (emphasis added). The court then
9 held that “[t]his is not ‘circumvention’ under the DMCA,” and accordingly dismissed Plaintiff’s § 1201(a)
10 claim. *Id.* Where a defendant is not alleged to have done anything besides ignore a technological measure,
11 a claim for circumvention will not lie. In other words, a defendant must unlock a black box, not simply
12 approach a mostly glass box from its side.

13 A DVD example is again instructive. DVDs encrypt content, such that possession of the disc is
14 insufficient to access content contained on it; a user also must possess a “key” to decrypt the content. *See*
15 *Reimerdes*, 111 F. Supp. 2d at 310 (“only players and drives containing the appropriate keys are able to
16 decrypt DVD files and thereby play movies stored on DVDs”). A DVD is like a black box: a user cannot
17 see the content inside without having a key to open it. By contrast, the content on YouTube is, by
18 Plaintiffs’ own allegations, readily accessible without decryption or any similar process. Compl. ¶ 2.
19 Plaintiffs do not, and cannot, allege that the files are encrypted either, because they are not. The alleged
20 technological measures here allow access at all times to some users who approach the works in the desired
21 direction; they are analogous to a glass box painted black on some sides, and left transparent on others—
22 if a user simply rotates the box, the work is accessible. Section 1201(a), however, does not cover alleged
23 technological measures that leave a work accessible. *See MDY*, 629 F.3d at 952–53 (“Just as one would
24 not say that a lock on the back door of a house ‘controls access’ to a house whose front door does not
25 contain a lock and just as one would not say that a lock on any door of a house ‘controls access’ to the
26 house after its purchaser receives the key to the lock, it does not make sense to say that this provision of
27 the DMCA applies to otherwise-readily-accessible copyrighted works.” (quoting *Lexmark*, 387 F.3d at
28 547)).

1 Plaintiffs’ § 1201(a) claim therefore also fails because they do not allege that Apple took any action
 2 regarding the alleged technological measures. Tellingly, Plaintiffs do not allege descrambling,
 3 decrypting, or any other affirmative form of circumvention. Instead, Plaintiffs try to shoehorn their claim
 4 into § 1201(a) by using the terms “*avoidance and bypassing*.” Compl. ¶ 134 (emphasis added). But
 5 because circumvention requires more than ignoring alleged technological measures, Plaintiffs’ conclusory
 6 invocation of these terms fails to state a claim. *See Hattler*, 2017 WL 11634742, at *3 (“A pleading that
 7 offers ‘labels and conclusions’ or ‘a formulaic recitation of the elements of a cause of action will not do.’”
 8 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009))).

9 As to the Automation Detectors, Plaintiffs allege that Apple accessed Plaintiffs’ works exactly as
 10 any other user would: by going to YouTube’s website. For example, Plaintiffs allege that the purported
 11 CAPTCHA challenges needed to be confronted “for continued access,” which presupposes initial access
 12 *without* confronting CAPTCHA. Compl. ¶ 101. If sometimes Apple was confronted by the Automation
 13 Detectors, it could ignore them by simply “obtain[ing] fresh authorization parameters and regenerat[ing]
 14 valid links.” *Id.* ¶ 100. And Apple allegedly “avoid[ed]” IP detection by simply using multiple IP
 15 addresses, all of which were granted access by YouTube. *Id.* ¶¶ 96, 98. For each of these purported
 16 technological measures, YouTube granted Apple access to Plaintiffs’ videos. The gates were down, and
 17 Apple strode through. But the DMCA does not impose liability for “circumventing” measures where
 18 access is obtained without any affirmative action. *See* 4 Nimmer on Copyright § 12A.06[C][5]
 19 (“[H]acking around password protection violates the statute; using an authorized password does not do
 20 so, even if the defendant who uses that password is not the individual to whom plaintiff issued it—and,
 21 indeed, is someone whom plaintiff actually wished to exclude from its site.”); *see also* Section 1201
 22 Rulemaking Rep. 125 (“Nor do the two ways in which proponents state that they evade [Automation
 23 Detectors] likely qualify as ‘circumvention’ within the scope of” § 1201.).

24 As to the File Location Maps, the Complaint’s allegations similarly fail because Plaintiffs do not,
 25 and cannot, allege that Apple was required to use these maps in the first place to access their works; Apple
 26 cannot have “circumvented” a measure it was not required to confront. As an initial matter, the File
 27 Location Maps affect only access to the works’ files. But Plaintiffs concede that the files are not “distinct”
 28 forms of the works from the videos, and Plaintiffs also concede they granted access to the videos. Compl.

¶¶ 2, 33, 46. Because Plaintiffs thus concede that they gave Apple access to their works in at least one form, Apple cannot have engaged in circumvention regardless of how it ultimately accessed the works. *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)). On top of that, the acts of “circumvention” that Plaintiffs allege amount only to disregarding the File Location Maps, not to taking any affirmative act to disable them that is analogous to breaking into a vault. For example, YouTube’s playback environment allegedly produces tokens demonstrating the origin of requests to call up files, but Apple’s “[a]utomated downloading tools operate *outside* that environment.” Compl. ¶ 102 (emphasis added). By Plaintiffs’ own allegations, then, these tokens were irrelevant to Apple’s purported operations. And although Plaintiffs conclusorily recite that Apple needed a “descrambling tool” to *find* the files, *id.* ¶ 92, the “descrambling tool” would have revealed only the files’ publicly accessible locations. Plaintiffs do not, and cannot, allege that the descrambling tool was needed to access the files at those locations because the files themselves were not scrambled or encrypted. That means that in addition to the works being readily accessible as videos on YouTube’s website, they also are readily accessible at their file locations by anyone with knowledge of the locations.

And that is exactly what Plaintiffs allege Apple did: it supposedly accessed “files directly from a website’s servers.” *See id.* ¶¶ 87–90; *see also id.* ¶¶ 84–85 (Apple allegedly possessed an independent “dataset consist[ing] of location identifiers”). But accessing unscrambled, unencrypted files at their intended, 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 Section 1201(a) violation where “website remains accessible”); *Adobe*, 2015 WL 13022288, at *8 (unauthorized use of “otherwise genuine and valid serial license keys” does not constitute circumvention).

Plaintiffs do not allege that Apple took any affirmative act *with respect to the alleged technological measures*; instead, they allege that Apple had access to Plaintiffs’ works from the outset

1 and could access other forms of the same works without ever confronting the purported technological
 2 measures at all. To sustain their claim, Plaintiffs seek to define “circumventing” a technological measure
 3 broadly to encompass doing nothing at all to it. Section 1201(a) requires more than that because it defines
 4 “circumvention” narrowly and contextually to require affirmative acts that disable an alleged
 5 technological measure. Because Plaintiffs do not allege any such affirmative acts, the Complaint must be
 6 dismissed.

7 **B. Plaintiffs’ Infringement-Based Relief Should Be Struck**

8 If the Court does not outright dismiss the Complaint due to the three fatal errors discussed above,
 9 relief related to use should be struck from the Complaint. Rule 12(f) permits a court to strike “any
 10 redundant, immaterial, impertinent, or scandalous matter” from a pleading. *See Ambrozewicz*, 804 F.
 11 Supp. 3d at 1030. The purpose of a Rule 12(f) motion to strike is “to avoid the expenditure of time and
 12 money that must arise from litigating spurious issues by dispensing with those issues prior to trial.” *Id.*
 13 “A matter is ‘immaterial’ if it has no essential or important relationship to the claim for relief or the
 14 defenses being pleaded.” *Ramachandran v. City of Los Altos*, 359 F. Supp. 3d 801, 808–09 (N.D. Cal.
 15 2019). “Statements that do not pertain to, and are not necessary to resolve, the issues in question are
 16 impertinent.” *Baton v. Ledger SAS*, 740 F. Supp. 3d 847, 872 (N.D. Cal. 2024). “Just as with a motion
 17 to dismiss, the Court should view the pleading sought to be struck in the light most favorable to the
 18 nonmoving party.” *Id.*

19 Section 1201 focuses on circumvention and accordingly is use-agnostic. As discussed above, the
 20 DMCA “does not concern itself with the *use* of [copyrighted] materials after circumvention has occurred.”
 21 *Corley*, 273 F.3d at 443; *see also MGE UPS Sys., Inc. v. GE Consumer and Indus., Inc.*, 622 F.3d 361,
 22 366 (5th Cir. 2010) (DMCA “does not apply to the use of copyrighted works *after*” circumvention). For
 23 this reason, the Ninth Circuit expressly rejected imposing an “infringement nexus” on § 1201(a) claims.
 24 Instead, it found that “there is significant textual evidence showing Congress’s intent to create a new
 25 anticircumvention right in § 1201(a) *distinct from infringement*.” *MDY*, 629 F.3d at 950–52 (emphasis
 26 added). Thus, § 1201(a) relates to circumvention of alleged access controls *regardless* of whether
 27 subsequent use is infringing or not, or even whether there is subsequent use at all. *Id.* at 950. The DMCA
 28

1 does not (and is not intended to) address claims related to use; those arise under the Copyright Act, if they
2 arise at all.

3 Here, Plaintiffs' Complaint is replete with allegations that relate solely to Apple's purported
4 intended or ultimate use of their works, none of which are material or pertinent to Plaintiffs' sole claim
5 for circumvention of *access* controls. From their first paragraph, Plaintiffs introduce the irrelevant
6 allegation that Apple engaged in circumvention "in order to" train an artificial intelligence model. Compl.
7 ¶ 1. Plaintiffs then repeatedly accuse Apple of "downloading" or "copying" their videos and thereby
8 "infringing" their alleged copyrights as part of "training" the alleged AI model. *E.g., id.* ¶¶ 1, 4, 6–7, 9,
9 11–13, 15–18, 23, 25, 66, 68–69, 71–78, 81, 83–92, 94–100, 102–103, 105, 110, 114, 121, 123, 126, 129,
10 133, 137, 139. Plaintiffs even seek to define their proposed class by reference to infringement. *Id.*
11 ¶¶ 120(b), 120(d). Yet, none of these allegations of use are relevant to whether Apple circumvented a
12 qualifying access control. *See Columbia Pictures Indus., Inc. v. Fung*, 710 F.3d 1020, 1034 (9th Cir.
13 2013) (unauthorized "downloading" implicates the right of reproduction under 17 U.S.C. § 106).

14 Plaintiffs' irrelevant allegations of use even extend to the prayer for relief, which requests an
15 injunction "to prevent or restrain infringement." Dkt. 1, Prayer for Relief, at 26 ¶ d. This prayer for relief
16 is immaterial because it has no essential relationship to the sole pleaded cause of action, which the Ninth
17 Circuit expressly has held is distinct from infringement. It also is impertinent because questions about
18 use (such as alleged infringement) are not necessary to resolve the issues in question, which all relate to
19 alleged circumvention. This follows from the plain text of the DMCA: a "violation" of the DMCA is
20 different from an "infringement" of copyright. *Compare* 17 U.S.C. § 1203, *with id.* § 501. Under
21 *Whittlestone, Inc. v. Handi-Craft Co.*, a court may not strike a demand for relief on the basis that it is
22 "precluded as a matter of law." 618 F.3d 970, 971 (9th Cir. 2010). Here, the DMCA authorizes damages
23 and injunctive relief. 17 U.S.C. § 1203. Yet, the injunction that Plaintiffs request covers conduct
24 "distinct" from that cause of action. *MDY*, 629 F.3d at 950–52. Whether *an* injunction may be available
25 on *a* DMCA claim is separate from whether *this* requested injunction against infringement is available on
26 *this* DMCA claim. It is not. *See Hecox v. Little*, 104 F.4th 1061, 1089 (9th Cir. 2024) (holding "injunctive
27 relief must be tailored to remedy the specific harm alleged"; vacating and remanding injunction). Pursuant
28

1 to Rule 12(f), the Court therefore should strike any requested relief related to scraping, copying,
2 downloading, infringing, or any other form of use that Plaintiffs allege occurred *after* access.

3 The relief Apple requests is narrow. Although none of the litany of immaterial and impertinent
4 allegations are proper, because they have no practical effect, Apple merely requests that the Court strike
5 Plaintiffs' prayer for relief regarding infringement.

6 **V. CONCLUSION**

7 For the foregoing reasons, Apple respectfully requests that the Court dismiss the Complaint. And,
8 because the Complaint itself shows why Plaintiffs have failed to state a claim, they should not be permitted
9 to amend it to remove the admissions as to YouTube's operation that they already have made. *See Airs*
10 *Aromatics, LLC v. Victoria's Secret Stores Brand Mgmt., Inc.*, 744 F.3d 595, 600 (9th Cir. 2014) ("A party
11 cannot amend pleadings to directly contradic[t] an earlier assertion made in the same proceeding.").
12 Plaintiffs alleged that YouTube's purported technological measures do nothing to control the ability of
13 the public to stream, watch, and listen to Plaintiffs' works. Taking these well-pleaded allegations as true,
14 YouTube's alleged technological measures do not control access. Because any amendment would be
15 futile, Apple respectfully requests that dismissal be with prejudice.

1 DATED: July 1, 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 1, 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