

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

UMG RECORDINGS, INC., et al.,

Plaintiffs,

v.

SUNO INC., et al.,

Defendants.

**Civil Action No.
24-11611-FDS**

**MEMORANDUM AND ORDER ON PLAINTIFFS' FIRST
MOTION TO AMEND THE COMPLAINT**

SAYLOR, J.

This is a copyright dispute concerning an AI music generator. Plaintiffs are a group of record companies or recorded-music businesses that own or exclusively control copyrights to sound recordings. Defendant Suno, Inc. is a generative AI company. It runs Suno AI, a service that generates music in response to text prompts.

Plaintiffs accuse Suno of copying their sound recordings to train its AI model in violation of their copyright rights. During discovery, plaintiffs learned that Suno obtained the recordings by downloading them from YouTube. It allegedly used a third-party software tool to circumvent technical measures put in place by YouTube to preclude downloading, copying, or distribution of its videos. They now seek to amend the complaint to assert a claim for violation of 17 U.S.C. § 1201(a)(1), which proscribes “circumvent[ing] a technological measure that effectively controls access to a [copyrighted] work.”

The ultimate determination of whether Suno circumvented a technological measure that effectively controls access to plaintiffs’ sound recordings will require a developed factual record

on how the technological measure and circumvention tools work. At this stage, however, the complaint alleges a plausible claim for violation of § 1201(a)(1), and the Court will grant plaintiffs’ motion for leave to amend.

I. Background

A. Procedural Background

The complaint alleges that Suno reproduced plaintiffs’ copyrighted sound recordings to train its AI model. (Dkt. No. 1). It asserts claims for direct copyright infringement.

After discovery commenced, plaintiffs served Suno with an interrogatory asking it to describe how it acquired its training data. (Dkt. No. 126-5, at 6). In May 2025, Suno responded that it downloaded audio files from YouTube. (Dkt. No. 128-2, at 19). It also explained that it used open-source software tools such as YT-DL and YT-DLP to download the files. (Dkt. No. 128-3, at 11).

Plaintiffs then moved for leave to amend the complaint. (Dkt. No. 134).¹ The proposed amended complaint seeks to add a claim against Suno for downloading copyrighted audio files from YouTube. (Dkt. No. 134-3 [“Prop. Am. Compl.”] ¶¶ 110-117). It contends that Suno circumvented a technological measure that controls access to copyrighted works in violation of 17 U.S.C. § 1201(a)(1) of the Digital Millenium Copyright Act.

Suno opposed the motion to amend. (Dkt. No. 131 [Opp’n]). It contends that YouTube’s technological measure inhibits copying of copyrighted works but does not control access to them. Section 1201 proscribes circumventing access controls but does not proscribe circumventing copy controls. It therefore asks the Court to deny the motion to amend the

¹ While that motion remained pending, plaintiffs filed a second motion to amend the complaint that seeks to assert additional copyrighted sound recordings that Suno allegedly infringed. (Dkt. No. 231). This memorandum and order will address only the first motion to amend.

complaint on the ground of futility.

B. Allegations of the Proposed Amended Complaint

The proposed amended complaint contends that YouTube employs a “rolling cipher” measure to prevent users from directly downloading media files. (Prop. Am. Compl. ¶ 53). YouTube maintains two URLs for any given video. (*Id.*). The page URL is visible to the user and displays the video player. (*Id.*). The file URL is not visible to the user and contains the audiovisual file that is played within the video player. (*Id.*). The file URL is “encrypted” using a periodically changing algorithm called a “rolling cipher.” (*Id.*). That cipher is designed to prevent or inhibit downloading, copying, or distribution of the videos. (*Id.*).

There are digital tools that enable users to circumvent the rolling cipher and directly download copies of the audiovisual file. (*Id.* ¶ 54). That process is known as “scraping” or “stream ripping.” (*Id.*). Suno utilized such tools known as YT-DL and YT-DLP to scrape copyrighted sound recordings from YouTube. (*Id.* ¶ 55). Suno then used those recordings in its training data for its AI model. (*Id.*).

II. Legal Standard

Under Rule 15(a), a party may amend a pleading without leave of court in certain relatively narrow circumstances. Fed. R. Civ. P. 15(a). “In all other cases, a party may amend its pleadings only with the opposing party’s written consent or the court’s leave. The court should freely give leave when justice so requires.” Fed. R. Civ. P. 15(a)(2). Nonetheless, amendments may be denied on the basis of “undue delay, bad faith or dilatory motive on the part of the movant, repeated failure to cure deficiencies by amendments previously allowed, undue prejudice to the opposing party by virtue of allowance of the amendment, [and] futility of amendment.” *Foman v. Davis*, 371 U.S. 178, 182 (1962). “‘Futility’ means that the complaint, as amended, would fail to state a claim upon which relief could be granted.” *Glassman v.*

Computervision Corp., 90 F.3d 617, 623 (1st Cir. 1996). “In reviewing for futility, the district court applies the same standard of legal sufficiency as applies to a Rule 12(b)(6) motion.” *Id.*

Under that standard, the complaint must state a claim that is plausible on its face. *See Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). In other words, the “[f]actual allegations must be enough to raise a right to relief above the speculative level, . . . on the assumption that all the allegations in the complaint are true (even if doubtful in fact).” *Id.* at 555 (citations omitted). “The plausibility standard is not akin to a ‘probability requirement,’ but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 556). When determining whether a complaint satisfies that standard, a court must “take the complaint’s well-pleaded facts as true, and . . . draw all reasonable inferences in the plaintiff’s favor.” *Lowe v. Mills*, 68 F.4th 706, 713 (1st Cir. 2023) (citation modified) (quoting *Frese v. Formella*, 53 F.4th 1, 5 (1st Cir. 2022)). Dismissal “is appropriate if the complaint fails to set forth ‘factual allegations, either direct or inferential, respecting each material element necessary to sustain recovery under some actionable legal theory.’” *Gagliardi v. Sullivan*, 513 F.3d 301, 305 (1st Cir. 2008) (quoting *Centro Médico del Turabo, Inc. v. Feliciano de Melecio*, 406 F.3d 1, 6 (1st Cir. 2005)).

III. Analysis

A. The Digital Millenium Copyright Act

In 1998, Congress passed the Digital Millenium Copyright Act (“DMCA”), 17 U.S.C. § 1201 *et. seq.*, to “mitigate the problems presented by copyright enforcement in the digital age.” *MDY Indus., LLC v. Blizzard Ent., Inc.*, 629 F.3d 928, 942 (9th Cir. 2010). The Act seeks to balance the public’s right to access a work and make fair use of it with a copyright holder’s interest in restricting access and protecting against infringing uses. *See id.* at 945-46.

To that effect, the DMCA distinguishes between technological measures that control

access to a copyrighted work (access controls) and technological measures that impede copying or another infringing use of a copyrighted work (copy or use controls). *See Disney Enters., Inc. v. VidAngel, Inc.*, 869 F.3d 848, 864 (9th Cir. 2017); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 441 (2d Cir. 2001); U.S. Copyright Off., *Section 1201 of Title 17: A Rep. of the Reg. of Copyright* 6-7 (2017).

Section 1201(a) governs access controls. It prohibits circumventing a technological measure that “effectively controls access” to a copyrighted work. 17 U.S.C. § 1201(a)(1)(A). It also prohibits trafficking in technologies that are primarily designed to circumvent such access controls. *Id.* § 1201(a)(2).

Section 1201(b) governs copy controls. It prohibits trafficking in technologies that are primarily designed to circumvent the “right of a copyright owner” under title 17, *id.* § 1201(b)(1), such as the exclusive right to reproduce or copy its work, *id.* § 106(1). It does not prohibit the act of circumventing a copy control. *See id.* § 1201(b).

B. The Anticircumvention Provision

Section 1201(a)(1), which prohibits circumventing an access control, is at issue here. It provides that “[n]o person shall circumvent a technological measure that effectively controls access to a work protected under this title.” 17 U.S.C. § 1201(a)(1)(A). Under that provision, “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.” *Id.* § 1201(a)(3)(A). Furthermore, “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.” *Id.* § 1201(a)(3)(B).

Neither the Supreme Court nor the First Circuit has yet construed that provision.

Nonetheless, the Court is not writing on a blank slate. Courts outside this circuit have applied the provision to a variety of technologies over the past decades. Those precedents suggest at least three relevant principles for this case.

First, to qualify as an “access control,” the measure does not have to prevent all access. A measure “effectively controls access” if it ordinarily requires an authorized “application of information, or a process or a treatment” to gain access to the work. 17 U.S.C. § 1201(a)(3)(B). That definition presupposes that some users will, in the ordinary course, access the work. It follows that a user’s ability to access the work through the authorized means is not evidence that the measure fails to “effectively control access.”

A line of cases involving DVDs illustrates that principle. *See Disney Enters.*, 869 F.3d 848 (9th Cir. 2017); *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 442 (2d Cir. 2001); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085 (N.D. Cal. 2004); *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000). In *Disney Enterprises, Inc. v. VidAngel, Inc.*, plaintiffs, a group of movie studios, encrypted their copyrighted content on DVDs and Blu-ray discs and distributed the decryption keys to licensed player manufacturers. 869 F.3d at 853. In the ordinary course, a viewer had to use a DVD or Blu-ray player from a licensed manufacturer to decrypt a disc’s contents and watch the film. *Id.* Even then, the licensed players did not enable copying of the disc’s contents. *Id.*

Defendant used a third-party software program to decrypt and copy the discs, and plaintiffs sued for violation of § 1201(a)(1)(A). *Id.* Defendant asserted that the disc encryption was not an “access control” because it could have decrypted the discs through a licensed player. *Id.* at 863. The Ninth Circuit rejected that argument. *Id.* It reasoned that defendant’s authority to decrypt the content through the authorized means did not give it the authority to circumvent

that process and decrypt it another way. *Id.* at 864-65. In other words, the fact that there was an authorized way to access the content did not mean that the content was not protected by an access control. *Id.* at 865 (“Nothing in the legislative history suggests that [defendant] did not circumvent an access control simply because there are authorized ways to access [plaintiffs’] works.”).

Second, a measure does not “effectively control” access to a copyrighted work if there is a way to readily access the work without going through the authorized process. Section 1201(a) “does not naturally extend to a technological measure that restricts one form of access but leaves another route wide open.” *Lexmark Int’l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 547 (6th Cir. 2004), *abrogated on other grounds by eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388 (2006); *see also* 17 U.S.C. § 1201(a)(3)(B) (stating that a technological measure “effectively controls access” if it “*requires* the application of information, or a process or a treatment . . . to gain access to the work” (emphasis added)). As the Sixth Circuit explained:

Just as one would not say that a lock on the back door of a house “controls access” to a house whose front door does not contain a lock and just as one would not say that a lock on any door of a house “controls access” to the house after its purchaser receives the key to the lock, it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works.

Lexmark, 387 F.3d at 547.

A line of cases beginning with *Lexmark International, Inc. v. Static Control Components, Inc.* illustrates that principle. In *Lexmark*, plaintiff’s printers ran an authentication sequence between the printer and toner cartridge to ensure that only its own cartridges could be used. *Id.* at 530. Defendant sold microchips that generated the authentication sequence so that other manufacturer’s cartridges could be used with plaintiff’s printers. *Id.* Plaintiff asserted that the authentication sequence controlled access to its copyrighted printer software program. *Id.* at 546. The Sixth Circuit disagreed; it concluded that anyone who purchased plaintiff’s printer could

read the program directly from the printer's memory without encountering the authentication sequence. *Id.* The authentication sequence was not an access control because it did not stand between the user and the copyrighted work.

The Ninth and Fifth Circuits have also applied the reasoning of *Lexmark*. In *MDY Industries, LLC v. Blizzard Entertainment, Inc.*, a technological measure controlled access to World of Warcraft game elements while connected to a World of Warcraft server. 629 F.3d at 952. A purchase of a World of Warcraft game nevertheless enabled a user to access the game's literal code and individual non-literal elements such as graphics and sounds without signing on to the server. *Id.* The Ninth Circuit found that the technological measure was not an access control because while one form of access was blocked another was left open. *Id.* at 953.

Similarly, in *Digital Data Systems, L.L.C. v. Petrolink Services, Inc.*, plaintiff's software aggregated real-time drilling data and then wrote it into a database using an open-source database application. 965 F.3d 365, 370-71 (5th Cir. 2020). Users could query the database through the software's interface process that only ran when a USB dongle was plugged into the laptop. *Id.* at 370. Nonetheless, defendant was able to access the database directly through the open-source application. *Id.* at 371. The Fifth Circuit found that the USB dongle and interface process did not "effectively control" access to the database, a copyrighted work, because the database was accessible through third-party programs without ever encountering the protective measures. *Id.* at 376-77.

Third, a user does not circumvent an access control measure by using the authorized process, even if the user is not authorized to use that process. Section 1201(a)(3)(A) defines circumvention as avoiding, bypassing, removing, deactivating, or impairing the technological measure itself. The focus of the statute is thus exclusively on circumventing or disabling actions

directed to the technological measure. *See Egilman v. Keller & Heckman, LLP*, 401 F. Supp. 2d 105, 113 (D.D.C. 2005). Whether or not the user has permission to use the authorized process is not the subject of § 1201(a)(1). *See id.* (“What is missing from this statutory definition is any reference to ‘use’ of a technological measure without the authority of the copyright owner, and the court declines to manufacture such language now.”); *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004) (“[A] cause of action under the DMCA does not accrue upon unauthorized and injurious access *alone*; rather, the DMCA ‘targets the *circumvention* of digital walls guarding copyrighted material.’” (emphasis in original) (quoting *Corley*, 273 F.3d at 443)).

In *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, defendant used a password issued to a third party to access plaintiff’s website. 307 F. Supp. 2d at 531. The court found that accessing a copyrighted work by an unauthorized use of an otherwise authorized password did not qualify as circumvention. *Id.* at 532-33. It reasoned that entering the password did not avoid or bypass the technological measure in the measure’s gatekeeping capacity. *Id.* at 532. Rather, “what defendant avoided and bypassed was *permission* to engage and move through the technological measure.” *Id.* Section 1201(a) “d[id] not target [that] sort of activity.” *Id.* at 533.

That principle is consistent with the cases cited above concerning DVDs. In *VidAngel*, defendant asserted that it did not circumvent an access control measure because it “was given the key” to the disc’s contents. *VidAngel*, 869 F.3d at 864. The Ninth Circuit disagreed. It explained that defendant “was never given the ‘keys’ to the discs’ contents—only authorized players get those keys.” *Id.* Instead of using the keys in the licensed players, it used a third party software to decrypt the discs. Defendant circumvented the technical measure because it did not use the authorized means. *Id.* at 865.

With those principles in mind, the Court will now turn to the present issue.

C. Application

To state a claim under § 1201(a)(1), a complaint must plausibly allege that the defendant (1) circumvented a technological measure (2) that effectively controls access (3) to a copyrighted work. 17 U.S.C. § 1201(a)(1); *see CDK Glob., LLC v. Tekion Corp.*, 2025 WL 1939951, at *8 (N.D. Cal. July 15, 2025).

The proposed amended complaint does so here. It alleges that YouTube’s rolling cipher encrypts the file URL that contains the copyrighted sound recordings. Suno used software tools such as YT-DL and YT-DLP to circumvent the rolling cipher and access the audio files. That plausibly states a claim under § 1201(a)(1).

Defendant’s principal response is that the rolling cipher is not an “access control” under § 1201(a). YouTube allows users to stream plaintiffs’ copyrighted sound recordings for free. According to Suno, there are no technological measures gatekeeping that content and no application of information or other authorized process is required to gain access to it. It contends that “YouTube is the paradigmatic online platform whose content is accessible *without* circumventing any” technological measure. (Opp’n 13). Citing *Lexmark*, it asserts that the rolling cipher cannot be an access control because the sound recordings are accessible without encountering any technological measure. Rather, it is a copy control, whose circumvention is not proscribed by the DMCA.

That contention cannot be resolved on the pleadings. To start, the fact that YouTube users are able to access the copyrighted works for free does not, on its own, establish that the rolling cipher fails to effectively control access. Under the statute, the relevant question is whether a technological measure ordinarily requires an authorized process to gain access. *See* 17 U.S.C. § 1201(a)(3)(B). In other words, what matters is the process used to stream the videos.

Here, the proposed amended complaint alleges that the encrypted file URL contains the protected audiovisual file. (Prop. Am. Compl. ¶ 53). That audiovisual file is played within the video player on the publicly visible page URL. (*Id.*). The proposed amended complaint does not explain how that process works. However, it is a reasonable inference that the video player on the page URL must decrypt or descramble the file URL in order to locate and play the underlying audiovisual file. In any event, defendant's contentions as to the technological measures required to view a video on YouTube in the ordinary course require further factual development and cannot be resolved on the pleadings.

Defendant seeks to distinguish the DVD cases by arguing that *VidAngel*'s reasoning relied on the fact that the technology applied to DVDs actually prohibited access. (Sur-Reply 8, Dkt. No. 157). But that is not an accurate reading of those cases. The Ninth Circuit focused on the fact that defendant used an unauthorized process to gain access to the disc's contents, not how easy or difficult it was to use the authorized process. On Suno's reasoning, the disc encryption would cease to be an access control if the movie studios gave out licensed DVD players for free with every disc. The technological measure in *VidAngel* did not prohibit access—it just set up a single authorized means to obtain access (using a licensed player). Likewise, on these allegations, YouTube has a single authorized means to obtain access (using the video player on the page URL).

In addition, the *Lexmark* line of cases does not apply here. *Lexmark* applies only when there is some other means of accessing the copyrighted work that does not encounter the technological measure. Here, there is no suggestion that there is any way to readily access the copyrighted work other than through the YouTube video player. Thus, to the extent that YouTube player on the page URL must go through the rolling cipher to access the underlying

audiovisual file, then the *Lexmark* reasoning does not apply.

Finally, at this stage, it is not clear how the YT-DL and YT-DLP tools work. They may access the copyrighted content through authorized means—for example, by using an issued key to decipher the rolling cipher—or it may bypass the measure altogether, and thus circumvent it within the meaning of the statute. It may also fall in a gray area in between. That, too, requires further factual development.

At this stage, it is enough to say that the proposed amended complaint plausibly pleads a claim for violation of § 1201(a), and is therefore not futile. There appears to be complicated questions about how the technology works that need a developed factual record to be answered, but those issues must be resolved at a later day.

IV. Conclusion

For the foregoing reasons, plaintiffs’ motion for leave to amend the complaint is GRANTED. For purposes of answering or otherwise responding, the amended complaint is deemed to be effective as of the date of this memorandum and order. Plaintiffs shall file the amended complaint as a separate docket entry within seven days of this order.

So Ordered.

Dated: August 18, 2026

/s/ F. Dennis Saylor IV
F. Dennis Saylor IV
United States District Judge