



**TABLE OF CONTENTS**

	<b><u>Page</u></b>
INTRODUCTION .....	1
ARGUMENT .....	2
I. PLAINTIFF’S SECTION 1201 ARGUMENTS IGNORE THE CONTROLLING LEGAL STANDARDS AND OTHERWISE ADDRESS IRRELEVANT POINTS.....	2
A. Plaintiff’s Own Allegations Establish that YouTube’s Rolling Cipher Is an Effective Technological Protective Measure from the Perspective of the Ordinary Consumer.....	2
B. Plaintiff’s Own Allegations Establish that Yout Is Used to Derive the Signature Value and thus to Circumvent the Rolling Cipher TPM .....	5
C. Plaintiff’s Other Arguments Are Irrelevant and Meritless .....	7
II. PLAINTIFF’S SECTION 512(F) CLAIM MISCHARACTERIZES RIAA’S NOTICES AND FAILS TO ALLEGE A KNOWING MISREPRESENTATION.....	8
III. PLAINTIFF’S STATE LAW CLAIMS SHOULD BE DISMISSED .....	10
IV. THE COURT SHOULD DENY PLAINTIFF’S REQUEST TO AMEND .....	10
CONCLUSION.....	10

**TABLE OF AUTHORITIES**

	<b><u>Page(s)</u></b>
<b>FEDERAL CASES</b>	
<i>321 Studios v. Metro Goldwyn Mayer Studios, Inc.</i> , 307 F. Supp. 2d 1085 (N.D. Cal. 2004) .....	6
<i>DISH Network L.L.C. v. World Cable Inc.</i> , 893 F. Supp. 2d 452 (E.D.N.Y. 2012) .....	7
<i>Healthcare Advocates, Inc. v. Harding, Earley, Follmer &amp; Frailey</i> , 497 F. Supp. 2d 627 (E.D. Pa. 2007) .....	7
<i>ISE Entertainment Corp. v. Longarzo</i> , 2018 U.S. Dist. LEXIS 40755 (C.D. Cal. Feb. 2, 2018).....	10
<i>N.Y. Times Co. v. Gonzales</i> , 459 F.3d 160 (2d Cir. 2006).....	9
<i>RealNetworks, Inc. v. DVD Copy Control Ass’n</i> , 641 F. Supp. 2d 913 (N.D. Cal. 2009) .....	1, 4, 6, 9
<i>Sony Comput. Entm’t Am., Inc. v. Divineo, Inc.</i> , 457 F. Supp. 2d 957 (N.D. Cal. 2006) .....	6
<i>Staton v. Holzbach</i> , 2021 WL 293566 (D. Conn. Jan. 27, 2021).....	10
<i>Universal City Studios, Inc. v. Corley</i> , 273 F.3d 429 (2d Cir. 2001).....	6, 7
<i>Universal City Studios, Inc. v. Reimerdes</i> , 111 F. Supp. 2d 294 (S.D.N.Y. 2000).....	3, 4, 5, 6
<i>Windstream Servs., LLC v. BMG Rights Mgmt. (US) LLC</i> , 2017 WL 1386357 (S.D.N.Y. Apr. 17, 2017).....	8
<b>FOREIGN DECISIONS</b>	
<i>In the Matter of Sony Music Entertainment Germany GmbH</i> , File No. 308 0 230/17 .....	4
<b>FEDERAL STATUTES</b>	
17 U.S.C. § 512.....	2, 9, 10
17 U.S.C. § 1201.....	1, passim

**TABLE OF AUTHORITIES**  
**(Continued)**

**Page**

**OTHER AUTHORITIES**

4 *Nimmer on Copyright* § 12A.03 (2020).....4

## INTRODUCTION

Plaintiff's opposition ignores the controlling legal standards; is based on a misleading description of the Yout service that is belied by the complaint's allegations; and fails to show that Plaintiff has stated any claim on which relief may be granted. The Yout service enables Plaintiff's users to do something that YouTube's rolling cipher technology otherwise prevents: turn authorized streams of sound recordings into unauthorized permanent downloads. That is circumvention of a technological protection measure ("TPM"), which section 1201 prohibits.

Plaintiff's arguments to the contrary are meritless:

- Plaintiff contends the rolling cipher is not an effective TPM, but Plaintiff does not engage with the DMCA's text and ignores the cases RIAA cited in its motion. A TPM is effective if it "requires the application of information, or a process or a treatment" to access the underlying copyrighted work. 17 U.S.C. § 1201(a)(3)(B). Plaintiff's allegations establish this technological process is required. (First Am. Compl., ECF No. 9 ("FAC") ¶ 41 (discussing "read[ing]," interpret[ing]" and "deriving" the program.) Whether a TPM is effective is gauged from the perspective of an "ordinary consumer." *RealNetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 2d 913, 932 (N.D. Cal. 2009)). Ordinary consumers cannot use their standard web browsers to turn authorized streams into unauthorized downloads. Indeed, if consumers could do that, they would not need the Yout service, and Plaintiff would have no business. Thus, the rolling cipher is an effective TPM. *See infra* at 2–4.
- Plaintiff argues that the Yout service does not circumvent because it merely *uses* the signature value. This is wordplay. The Yout service enables its users to use the rolling cipher TPM or the signature value in an unauthorized way. In the ordinary course, those users would not have access to the digital sound recording file. The users need the Yout

service to “read” and “interpret” code and “derive” the “signature value” (FAC ¶ 41)— i.e., bypass the rolling cipher’s protection of the sound recording file. That functionality is circumvention, as section 1201 and controlling cases make clear. *See infra* at 4–7.

- Plaintiff’s section 512(f) claim fundamentally misreads the statute, which penalizes only misrepresentations that “material or activity is *infringing*.” 17 U.S.C. § 512(f)(1) (emphasis added). RIAA’s notices to Google raised only *circumvention*. Plaintiff concedes that Section 512(f) does not create liability for notices based on circumvention claims, but insists that RIAA’s notices *implicitly* represented the Yout service was engaged in secondary copyright infringement. That argument is not supported by the statute or any case and, in any event, blatantly misreads RIAA’s notices (which were attached as exhibits to the complaint and can be considered on a motion to dismiss), which track the elements of a circumvention claim. *See infra* at 8–9.
- Plaintiff’s section 512(f) and state law claims independently fail because Plaintiff does not and cannot plead the notices were false. *See infra* at 9–10.

RIAA respectfully requests the Court dismiss Plaintiff’s claims with prejudice.

## ARGUMENT

### I. PLAINTIFF’S SECTION 1201 ARGUMENTS IGNORE THE CONTROLLING LEGAL STANDARDS AND OTHERWISE ADDRESS IRRELEVANT POINTS

Whether the Yout service circumvents turns on two questions: whether the rolling cipher is an effective TPM and whether the Yout service circumvents that TPM. While Plaintiff tries to confuse the issues, the controlling legal standards and the complaint’s own allegations make clear that the answer to both questions is yes.

#### A. Plaintiff’s Own Allegations Establish that YouTube’s Rolling Cipher Is an Effective Technological Protective Measure from the Perspective of the Ordinary Consumer

The opposition argues that because Plaintiff has purportedly figured out how to “derive[]

a signature value” from YouTube without using a “password, key, or other secret knowledge,” the rolling cipher TPM is necessarily ineffective. (Opposition at 4, 8–9, ECF No. 35 (“Opp’n”).) But Plaintiff fails to address any of the extensive authority cited in RIAA’s motion that squarely rejects Plaintiff’s arguments. (See Def. Mot. at 8–9, ECF No. 28-1 (“Def. Mot.”).) Plaintiff’s silence speaks volumes.

First, Plaintiff ignores the statutory text, under which the rolling cipher “effectively controls access to a work” if, “in the ordinary course of its operation,” the rolling cipher “*requires the application of information, or a process or a treatment*” to access the underlying copyrighted sound recording file. 17 U.S.C. § 1201(a)(3)(B) (emphasis added). The complaint’s allegations make clear that the rolling cipher meets this standard. Plaintiff admits that YouTube’s “signature mechanism” requires the application of technological processes to “read and interpret the JavaScript program” to “derive[] a signature value.” (FAC ¶ 41.) The rolling cipher thus requires a technological process to access the file and is therefore an effective TPM under the plain text of the statute. *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 317–18 (S.D.N.Y. 2000) (finding a TPM effectively controlled access to DVD movies where “[o]ne cannot gain access to a [TPM]-protected work . . . without application of the three keys that are required by the software”).

Second, Plaintiff’s claim that its ability to derive the signature value means the rolling cipher is ineffective (Opp’n at 4, 8–9) is directly contrary to the case law interpreting section 1201(a)(3)(B). The cases that RIAA cited (Def. Mot. at 8)—and that Plaintiff does not even discuss—make clear that effectiveness must be assessed from the “level of the ordinary consumer.” *RealNetworks*, 641 F. Supp. 2d at 932; see *Reimerdes*, 111 F. Supp. 2d at 318 (a TPM may “effectively control[] access’ . . . whether or not it is a strong means of protection”

(citation omitted)). As Professor Nimmer has explained, if a TPM’s effectiveness were judged from the level of the party that succeeded in bypassing the TPM—here a tech company—section 1201 would be “nonsensical.” 4 *Nimmer on Copyright* § 12A.03 (2020).

The very existence of the Yout service shows that the rolling cipher is effective from the level of ordinary consumers. If the rolling cipher were not effective, Plaintiff’s customers would have no need for the Yout service in the first place: they would simply obtain the signature value themselves and gain access to the digital sound recording file. Plaintiff’s service exists precisely because YouTube’s rolling cipher prevents them from turning legal streams on YouTube into illegal downloads.<sup>1</sup> The rolling cipher is an effective TPM.

Plaintiff tries to avoid this result with the completely circular argument that the rolling cipher is not an effective TPM because “any digital mechanism in place designed as anti-circumvention technology [would] stop[] Yout users from recording and saving that protected work.” (FAC ¶ 38.) Plaintiff, in other words, argues that the rolling cipher is not effective because the Yout service has figured out a way to bypass it (but not other TPM technology). That tautology is not the test, and courts have rejected exactly that type of self-serving reasoning. *See Reimerdes*, 111 F. Supp. 2d at 317–18 (noting that such a definition of an effective TPM “if adopted, would limit the application of the statute to access control measures that thwart

---

<sup>1</sup> Plaintiff’s complaint incorporates a letter from the Electronic Frontier Foundation (“EFF”) discussing YouTube’s rolling cipher. (FAC ¶ 43 n.3, incorporating original Compl. Ex. A.) The EFF letter, in turn, discusses a decision of the Hamburg Regional Court, which analyzed the rolling cipher in the context of a circumvention claim under Germany’s statute analogous to section 1201. Exhibit A to this reply is a true and correct copy of that December 18, 2017 decision of *In the Matter of Sony Music Entertainment Germany GmbH*, File No. 308 0 230/17, along with a certified translation to English. In that decision, the court concluded that the YouTube rolling cipher is an effective TPM because, “for the average user, it is typically not possible to download an audio track that is available as a stream and convert it into an MP3 file with the on-board instruments of the [user’s web] browser.” Ex. A at 7.



circumvention, but withhold protection for those measures that can be circumvented”).

**B. Plaintiff’s Own Allegations Establish that Yout Is Used to Derive the Signature Value and Thus to Circumvent the Rolling Cipher TPM**

Plaintiff next argues that the Yout service does not circumvent YouTube’s rolling cipher because the service “mere[ly] use[s]” the “signature value.” (Opp’n at 8.) Again, Plaintiff’s argument ignores and is contrary to the controlling legal authority.

“To circumvent” a TPM means, among other things, “to . . . *bypass* . . . a technological measure, without the authority of the copyright owner.” 17 U.S.C. § 1201(a)(3)(A). Even accepting Plaintiff’s factual allegations as true, that is exactly what the Yout service does: it makes an end-run, by design, around the restrictions the rolling cipher erects to safeguard access to the digital sound recording file. When using an ordinary web browser as intended, the user can only receive a *stream* of the sound recording through the YouTube video player; the user is not granted access to the location of the digital file and cannot download it.<sup>2</sup> To get around this protection, the Yout service “interprets the JavaScript program sent by YouTube” and “derives a signature value” to access the protected file and so the user can copy the audio stream as an MP3 file. (FAC ¶¶ 23, 24, 41.) The Yout service is not “using” the signature value in the way a user’s browser ordinarily does when it streams. The Yout service provides its users the means to get around the rolling cipher’s protections so they can get access to the copyrighted file—access that is not authorized by the copyright owners or YouTube.<sup>3</sup> That is circumvention.

---

<sup>2</sup> As the Hamburg Regional Court explained, “the precise storage location of the video is not displayed in the user’s browser when he accesses the services of the YouTube platform and watches a video,” and thus technology is required for the user to get around the rolling cipher’s protections of the information that identifies the file’s location. Ex. A at 2.

<sup>3</sup> Plaintiff’s vague claim that some “content creators encourage their audience and fans to use Yout to record and play back their original content” is irrelevant. (Opp’n at 3.) Even if some copyright owners did not object to the use of the Yout service to bypass the rolling cipher to gain

Yout contends that its service does not violate section 1201 because it uses YouTube's signature value, which Yout alleges can be "freely accessed by anyone who seeks it." (Opp'n at 8–9.) But courts have found circumvention of section 1201 where the offending party uses an authorized key to get around, i.e., to "bypass," a TPM to gain unauthorized access to copyrighted works. For example, RealNetworks was liable for distributing a device that used the same keys that authorized DVD players use to play back DVDs so that RealNetworks's customers could gain *unauthorized* access to the movie file on the DVD. 641 F. Supp. 2d at 935. Likewise, the defendants in *Corley/Reimerdes* were liable for trafficking in the DeCSS technology, which again used the authorized DVD keys to gain *unauthorized* access to the movie files on DVDs, thereby bypassing the CSS scramble on DVDs so that the user could make a copy of the copyrighted content from the disk. *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 460 (2d Cir. 2001), *aff'g Reimerdes*, 111 F. Supp. 2d 346; *see also 321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004) (unauthorized actor's trafficking in technology that "uses the authorized key to unlock the encryption" is "avoid[ing] and bypass[ing]" the TPMs). In all these cases, when the keys were used in the authorized manner, the DVD player only played back the movie. The circumvention consisted of the offending party's use of the same keys, but for the unauthorized access to a digital copy of the copyrighted work that the user could then copy. The Yout service does the same thing.

The cases Plaintiff cites do not change this result. In *DISH Network L.L.C. v. World*

---

access to their copyrighted works on YouTube, Plaintiff would still be liable under section 1201 when its service is used to access the content of RIAA's members, who have given no such authority. *See Sony Comput. Entm't Am., Inc. v. Divineo, Inc.*, 457 F. Supp. 2d 957, 965 (N.D. Cal. 2006) (rejecting similar argument).

*Cable Inc.*, defendant’s agents used DISH’s authorized cable boxes to descramble encrypted signals of DISH’s satellite programming; defendant then rebroadcast the programming without authorization. 893 F. Supp. 2d 452, 456 (E.D.N.Y. 2012). The court held the use of the boxes was not circumvention because the cable boxes continued to work according to their “normal process” and defendant did not interfere (or even interact) with the receipt and decryption of the copyrighted content. *Id.* at 465. Much of the *DISH* court’s reasoning is inconsistent with *Corley* and should not be adopted here. But the Court does not have to reach that issue because the *DISH* court’s emphasis on defendant’s use of the “normal process” makes the case inapposite. The Yout service does not use the normal process (a web browser that permits only streaming); rather, it uses an unauthorized process that permits its users to access and download a local copy.

*Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey* is likewise inapposite because it involved a temporary system malfunction resulting in the TPM on a database service’s servers failing to provide any restriction on accessing copyrighted content on those servers. 497 F. Supp. 2d 627 (E.D. Pa. 2007). The court held that the defendant did not circumvent the TPM because the defendant did not need to do anything to get around the TPM. *Id.* at 644. That case does not change the result here, where it is undisputed the Yout service gets around the rolling cipher TPM when that TPM is working. (*See* FAC ¶ 41.)

In short, Plaintiff cannot state a declaratory judgment claim under section 1201 through creative wording. The cases that interpret and apply section 1201 make clear that the Yout service circumvents the rolling cipher, which is an effective TPM.

### **C. Plaintiff’s Other Arguments Are Irrelevant and Meritless**

The opposition is laced with a number of irrelevant arguments that distract from the question whether the Yout service circumvents a TPM. First, Plaintiff asserts that the “without the author[ization] of the copyright owner” element of the circumvention definition, 17 U.S.C.

§ 1201(a)(3), is not satisfied because RIAA’s notices do not identify the copyrighted works at issue. (Opp’n at 10.) This argument is a red herring. RIAA used a process established by Google to notify Google of Yout’s circumvention of YouTube’s rolling cipher. Google did not require the identification of particular copyrighted works that the rolling cipher protects. Regardless, Plaintiff’s complaint and opposition admit that RIAA’s members—on whose behalf the notices were sent—are copyright owners. They are the major music companies. (See FAC ¶ 29; Opp’n at 11.) Plaintiff does not and cannot allege that it has permission from RIAA’s member companies to access or enable copies of their sound recordings.

Second, the opposition includes a digression about an alleged “circuit split” over whether there must be “a nexus between the purported circumvention and actual copyright infringement.” (Opp’n at 11–12.) As Plaintiff admits, however, “we need not address the split” because the rolling cipher protects copyrighted sound recordings, which Yout users can copy and thereby infringe. (*Id.* at 11.) RIAA agrees that there is no need to address this argument.

Finally, the Court can and should decline to exercise jurisdiction under the Declaratory Judgment Act (“DJA”). Plaintiff points to RIAA’s statement in the parties’ Rule 26(f) report concerning the possibility of counterclaims against Plaintiff as a justification for exercising jurisdiction over Plaintiff’s claims now. (Opp’n at 13.) But Plaintiff cannot manufacture declaratory judgment jurisdiction by filing suit and then claiming that the defendant’s response represents a “threat of litigation” against Plaintiff. *Cf. Windstream Servs., LLC v. BMG Rights Mgmt. (US) LLC*, 2017 WL 1386357, at \*9–10 (S.D.N.Y. Apr. 17, 2017). That is “procedural fencing,” which Plaintiff’s own cited authority makes clear is a basis for the court’s discretion to decline DJA jurisdiction. *See N.Y. Times Co. v. Gonzales*, 459 F.3d 160, 167 (2d Cir. 2006).

## **II. PLAINTIFF’S SECTION 512(f) CLAIM MISCHARACTERIZES RIAA’S NOTICES AND FAILS TO ALLEGE A KNOWING MISREPRESENTATION**

Plaintiff’s opposition reflects a fundamental misunderstanding about section 512(f) and the notices that RIAA sent to Google. By its plain text, section 512(f) penalizes only misrepresentations about alleged copyright *infringement*. Section 512(f) does not proscribe misrepresentations about alleged *circumvention* under section 1201. The statute and the case law are clear on this distinction. (Def. Mot. at 14–15.) In this case, RIAA’s notices to Google (which are the basis of Plaintiff’s claims) raised only claims of circumvention. Plaintiff fails to cite to any authority holding a circumvention notice can give rise to a section 512(f) claim, and RIAA has located none. Plaintiff’s section 512(f) claim fails as a matter of law.

Plaintiff tries to resurrect its section 512(f) claim by arguing that RIAA’s circumvention notices to Google “impute[d] allegations of copyright infringement.” (Opp’n at 1.) But section 512(f) does not apply to implicit or imputed representations of copyright infringement. It applies to notices whose contents are specified in section 512(c)(3)(A), and those contents must include (among other things) an express assertion that material or activity is “infringing,” as well as an identification of the infringed work or a representative list of such works. 17 U.S.C.

§ 512(c)(3)(A)(ii)–(v). RIAA’s notices did not include this information because they were not notices of infringement.<sup>4</sup> (Compl. Exs. A–C, ECF No. 1.)

Plaintiff’s section 512(f) claim separately fails because Plaintiff has not plausibly alleged that RIAA made “knowing” misrepresentations in its notices to Google. (*See* Def. Mot. at 15–

---

<sup>4</sup> Plaintiff points to the fact that the notices stated that the rolling cipher TPM “protects our members’ works on YouTube from unauthorized copying/downloading.” (Opp’n at 11 (quoting FAC ¶ 30).) That reference simply refers to an element of section 1201(b), which prohibits trafficking in technology designed to circumvent TPMs that protect the rights of copyright owners. 17 U.S.C. § 1201(b)(1)(A)–(C) (trafficking offenses). A party may traffic in a single technology in violation of both section 1201(a) and section 1201(b). *See generally RealNetworks*, 641 F. Supp. 2d at 935 (defendant liable under both 1201(a) and 1201(b)). That is what Plaintiff here does with the Yout service. The fact that RIAA’s notices referred to both types of prohibited conduct did not transform them into notices “under” section 512.

16.) Plaintiff asserts that *ISE Entertainment Corp. v. Longarzo*, 2018 U.S. Dist. LEXIS 40755 (C.D. Cal. Feb. 2, 2018), sets forth the level of detail required to plead subjective belief under section 512(f). That case is easily distinguished. Unlike in *ISE Entertainment Corp.*, Plaintiff fails to allege that RIAA was confronted or otherwise made aware that the Yout service did not circumvent the rolling cipher. *See id.* at \*19 (section 512(f) claim pled where defendant refused to withdraw takedown notice after the plaintiff repeatedly asserted copyrights in the works).

### **III. PLAINTIFF'S STATE LAW CLAIMS SHOULD BE DISMISSED**

Plaintiff's claims for defamation per se and business disparagement should be dismissed because Plaintiff has failed to plausibly plead that RIAA's notices are false. As discussed above, the plausible reading of the FAC is that the Yout service *does* circumvent the rolling cipher. And to the extent the state law claims are the only remaining claims, the Court should decline to exercise supplemental jurisdiction. *See Staton v. Holzbach*, 2021 WL 293566, at \*6 (D. Conn. Jan. 27, 2021) (dismissing state law defamation claims after dismissal of federal law claims).

### **IV. THE COURT SHOULD DENY PLAINTIFF'S REQUEST TO AMEND**

The Court can decide this motion as a matter of law based on Plaintiff's current, albeit oversimplified, allegations. Further amendment would be futile because any additional facts would only further support RIAA's legal arguments.

### **CONCLUSION**

RIAA respectfully requests that the Court dismiss Plaintiff's FAC with prejudice.

DATED: March 18, 2021

Respectfully submitted,

/s/ Rose Leda Ehler

GLENN D. POMERANTZ (*appearing pro hac vice*)

ROSE LEDA EHLER (*appearing pro hac vice*)

SHANNON AMINIRAD (*appearing pro hac vice*)

MUNGER, TOLLES & OLSON LLP

350 South Grand Avenue

Fiftieth Floor

Los Angeles, CA 90071-3426

T: (213) 683-9100

F: (213) 687-3702

glenn.pomerantz@mto.com

rose.ehler@mto.com

shannon.aminirad@mto.com

JAMES O. CRAVEN (ct18790)

DAVID NORMAN-SCHIFF (ct30082)

WIGGIN AND DANA LLP

One Century Tower

265 Church Street

P.O. Box 1832

New Haven, CT 06508-1832

T: (203) 498-4400

F: (203) 782-2889

jcraven@wiggins.com

Attorneys for Defendant Recording Industry  
Association of America, Inc.