

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

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

Plaintiffs,

v.

SNAP, INC.,

Defendants.

Case No. 2:26-cv-00754-AB-MBK

**ORDER DENYING DEFENDANT'S
MOTION TO DISMISS [DKT. NO.
42]**

Before the Court is Defendant Snap Inc.'s ("Defendant" or "Snap Inc.") Motion to Dismiss the Consolidated Class Action Complaint ("CAC," Dkt. No. 36). "Mot.," Dkt. No. 42. Plaintiffs Ted Entertainment, Inc., Matt Fisher, Golfholics, Inc., and Nicole Chmura (collectively "Plaintiffs") filed a timely Opposition ("Opp'n," 50) and Defendant filed a Reply ("Reply," Dkt. No. 55). The Court held a hearing on the matter on June 26, 2026. For the following reasons, the Motion is **DENIED**.

I. BACKGROUND

Plaintiffs are content creators who upload and share videos on YouTube for

1 public viewing. CAC ¶¶ 17-24. Plaintiffs exclusively upload their original videos to
2 YouTube for public viewing in a manner consistent with YouTube’s Terms of Service.
3 *Id.* ¶¶ 18, 21, 23 & 25. Under YouTube’s Terms of Service, Plaintiffs and other content
4 creators grant YouTube and other users of YouTube to access content through
5 YouTube’s services. *Id.* ¶ 67. The license however “does not grant any rights or
6 permissions for a user to make use of [the] Content independent of the [YouTube]
7 Service.” *Id.*

8 Plaintiffs allege the following:

9
10 **A. YouTube and the Technological Protection Measures (“TPMs”)**

11
12 YouTube is a video-sharing platform that permits individuals to upload
13 audiovisual content for public access. *Id.* ¶¶ 32, 34. The “work” at issue includes its
14 digital embodiment through “encoded media streams and associated data structures.”
15 *Id.* ¶ 33. YouTube permits users to watch and listen to videos for free through its
16 advertisement-supported service, with access limited to its authorized playback
17 environment. *Id.* ¶¶ 34, 37. Rather than providing videos in their native or fixed file
18 form or allowing file-level access, *id.* ¶¶ 38–39, YouTube delivers each video in
19 segments through temporary links and reassembles those segments for playback
20 through its authorized streaming mechanism. *Id.* ¶ 42.

21
22 To ensure that users access the uploaded content only through the authorized
23 streaming mechanism, YouTube uses five TPMs to control access to content and
24 monitor its delivery system: (1) the rolling cipher; (2) IP-based blocking and rate
25
26
27
28

1 limiting; (3) short-lived session-bound streaming URLs; (4) CAPTCHA human-
2 verification challenges; and (5) proof-of-origin tokens. *Id.* ¶ 45. Each of these
3 mechanisms independently protects and controls access to the uploaded works.
4

5 **a. The Rolling Cipher**

6 The rolling cipher is an encryption that protects access to the audiovisual file. *Id.*
7 ¶ 50. Each YouTube video URL includes two URLs: the page URL, which is visible to
8 the user, and the file URL, which is not visible to the user. *Id.* ¶ 51. The file URL is the
9 video file itself played within the page and it is encrypted using a complex and
10 periodically changing algorithm, or the rolling cipher, designed to “impede external
11 access to the underlying YouTube files.” *Id.*
12

13 YouTube uses a proprietary logic embedded in the official YouTube player to
14 decrypt authentication requests and deliver the content. *Id.* ¶¶ 50, 51. Thus, the rolling
15 cipher serves as a “digital lock,” controlling access to the audiovisual content and
16 protecting against unauthorized downloads. *Id.* ¶ 51. YouTube’s streaming architecture
17 serves as the key, permitting users to view content through YouTube’s authorized
18 playback environment. *Id.* ¶ 51.
19

20 **b. IP Blocking and Rate Limiting**

21 YouTube restricts access to suspicious users through IP-based blocking and rate
22 limiting. YouTube monitors network behavior and restricts access when it detects
23 excessive or abusive behavior. *Id.* ¶ 53. Once certain thresholds are exceeded, YouTube
24 blocks the IP address from accessing the platform entirely. *Id.*
25
26
27
28

1 **c. Session-Bound, Short-Lived URLs**

2 YouTube limits access to works by using session-bound, short-lived URLs.
3
4 When YouTube creates a file URL for uploaded content, the URL itself protects the
5 work because it is “temporary, cryptographically signed, and tied to a particular
6 playback session and client context.” *Id.* ¶ 56. In other words, these file URLs are
7 “session-bound” because they provide a user with temporary access, limited to a
8 particular use session. Session-bound URLs expire automatically, such that an attempt
9 to access the content using an expired link will be unsuccessful. *Id.* ¶ 57. Re-accessing
10 content requires obtaining fresh authorization parameters and regenerating new valid
11 URLs. *Id.*

12 **d. CAPTCHA Challenges**

13 YouTube uses CAPTCHA challenges to monitor access and ensure that it is
14 limited to human users, rather than automated bots. When traffic activity and patterns
15 indicate suspicious or automated activity, YouTube requires completion of a
16 CAPTCHA challenge, a test required to separate human users from bots. *Id.* ¶ 58.
17 Plaintiffs allege that these CAPTCHA challenges serve a gatekeeping function by
18 preventing certain users from accessing the platform. *Id.*

19 **e. Proof of Origin Tokens**

20 Finally, YouTube uses “proof of origin” tokens to ensure that requests for videos
21 are valid. YouTube requires all requests for video segments include cryptographic
22 “proof-of origin” tokens that validate a request as originating from an authorized
23

1 YouTube playback environment. *Id.* ¶ 62. Requests that do not possess a valid token or
2 that possess an expired token are refused. *Id.* Proof of origin tokens are generated
3 exclusively within YouTube’s authorized player environment, so software operating
4 outside that environment cannot obtain valid tokens through ordinary means. *Id.*

6 **B. Defendant’s Alleged Scraping of YouTube Videos**

7
8 Defendant Snap Inc. is a Delaware corporation that allegedly circumvented the
9 TPMs to access and scrape millions of videos from YouTube to feed, train, improve,
10 and commercialize Defendant’s large-scale commercial generative text-to-video
11 artificial intelligence (“AI”) models (collectively “Snap AI Video”). *Id.* ¶¶ 1, 77.
12 Defendant had significant incentives to acquire data to train its Snap AI Video at scale.
13 *Id.* ¶ 78. Rather than seek permission for use of the content or negotiate lawful licenses,
14 Defendant broke through YouTube’s access protections to obtain the underlying files.
15 *Id.* ¶ 9, 78.

16
17 Defendant used the publicly available HD-VILA-100M dataset, which was
18 compiled by Microsoft Research Asia from millions of YouTube videos. *Id.* ¶ 80. HD-
19 VILA-100M consists not of the actual video files but of data points to identify different
20 YouTube videos, such as URLs, video identifiers, and timestamps. *Id.* ¶ 81. In short,
21 HD-VILA-100M is an index file. The dataset is composed of roughly 100 million clips
22 derived from 3,098,462 YouTube videos. *Id.* ¶ 84. HD-VILA-100M was published was
23 for use in a non-commercial research setting, stating that users “may not use the Data
24 or any Results in any commercial offering, including as part of a product or service (or
25
26
27
28

1 to improve any product or service) you use or provide to others.” *Id.* ¶ 85.

2 Using HD-VILA-100M, Defendant’s researchers developed the Panda-70M
3 dataset. They created Panda-70M by curating 3.8 million high-resolution videos from
4 HD-VILA-100M and splitting them into 70.8 million video clips. *Id.* ¶ 89. Like HD-
5 VILA-100M, Panda-70M is an index file that does not contain the actual audiovisual
6 files, but instead contains location identifiers. *Id.* ¶ 91. Indexes to Plaintiffs’ videos were
7 found in either the HD-VILA-100M dataset or Panda-70M dataset. *Id.* ¶¶ 17, 20, 22,
8 24.

9 Plaintiffs allege that Defendant used the Panda-70M dataset to unlawfully scrape
10 videos from YouTube. By scraping the content, Defendant used an automated process
11 to access and download the audio and video files directly from the website’s servers
12 rather than viewing the content through the authorized playback environment. *Id.* ¶ 95.
13 Defendant used scraping tools and/or workflows to bypass or evade YouTube’s TPMs
14 and then reproduced the videos to train Defendant’s AI. *Id.* ¶¶ 48-49; 99 - 113.

15 In using these tools, Plaintiffs allege that Defendant was able to bulk extract,
16 access, and download YouTube videos at scale through automation, a process known
17 as “scraping” or “stream ripping.” *Id.* ¶ 95.

18 Plaintiffs brought this putative class action against Defendant alleging violations
19 of the Digital Millennium Copyright Act (“DMCA”) anti-circumvention provision, or
20 17 U.S.C. § 1201(a). *Id.* ¶¶ 145-161. Plaintiffs seek statutory damages, equitable relief,
21 and any other just relief. *Id.* at 37-38. Defendant moves the dismiss the action under
22
23
24
25
26
27
28

1 Federal Rule of Civil Procedure 12(b)(6).

2 II. LEGAL STANDARD

3
4 Federal Rule of Civil Procedure (“Rule”) 8 requires a plaintiff to present a “short
5 and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R.
6 Civ. P. 8(a)(2). Under Rule 12(b)(6), a defendant may move to dismiss a complaint for
7 “failure to state a claim upon which relief can be granted.” Fed. R. Civ. P. 12(b)(6). To
8 defeat a Rule 12(b)(6) motion to dismiss, the complaint must provide enough detail to
9 “give the defendant fair notice of what the . . . claim is and the grounds upon which it
10 rests.” *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). The complaint must also
11 be “plausible on its face,” allowing the court to “draw the reasonable inference that the
12 defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678
13 (2009). “The plausibility standard is not akin to a ‘probability requirement,’ but it asks
14 for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* Labels,
15 conclusions, and “a formulaic recitation of the elements of a cause of action will not
16 do.” *Twombly*, 550 U.S. at 555.

17
18 A complaint may be dismissed under Rule 12(b)(6) for the lack of a cognizable
19 legal theory or the absence of sufficient facts alleged under a cognizable legal theory.
20
21 *Balistreri v. Pacifica Police Dep’t*, 901 F.2d 696, 699 (9th Cir. 1988). When ruling on
22 a Rule 12(b)(6) motion, “a judge must accept as true all of the factual allegations
23 contained in the complaint.” *Erickson v. Pardus*, 551 U.S. 89, 94 (2007). But a court is
24 “not bound to accept as true a legal conclusion couched as a factual allegation.” *Iqbal*,

1 556 U.S. at 678 (2009) (internal quotation marks omitted).

2 A court generally may not consider materials other than facts alleged in the
3 complaint and documents that are made a part of the complaint. *Anderson v. Angelone*,
4 86 F.3d 932, 934 (9th Cir. 1996). However, a court may consider materials if (1) the
5 authenticity of the materials is not disputed and (2) the plaintiff has alleged the existence
6 of the materials in the complaint or the complaint “necessarily relies” on the materials.
7
8 *Lee v. City of Los Angeles*, 250 F.3d 668, 688 (9th Cir. 2001) (citation omitted). The
9 court may also take judicial notice of matters of public record outside of the pleadings
10 and consider them for purposes of the motion to dismiss. *Mir v. Little Co. of Mary*
11 *Hosp.*, 844 F.2d 646, 649 (9th Cir. 1988); *Lee*, 250 F.3d at 689-90.

14 III. DISCUSSION

15 A. The DMCA Anti-Circumvention Provision

16 Congress enacted the DMCA in 1998 to “conform United States copyright law
17 to its obligations under two World Intellectual Property Organization (“WIPO”)
18 treaties, which require contracting parties to provide effective legal remedies against
19 the circumvention of protective technological measures used by copyright owners.”
20 *MDY Industries, LLC v. Blizzard Ent., Inc.*, 629 F.3d 928, 942 (2010). Congress also
21 recognized “the ease with which digital works can be copied and distributed worldwide
22 virtually instantaneously” so without protections, “copyright owners will hesitate to
23 make their works readily available on the Internet.” Sen. Rep. No. 105-190 at 8. Thus,
24 protective legislation would “create[] the legal platform for launching the global digital
25
26
27
28

1 on-line marketplace for copyrighted works” and “facilitate making available . . . via the
2 Internet the movies, music, software, and literary works that are the fruit of American
3 creative genius.” *Id.*

4
5 Section 1201(a)(1)(A) provides that, “[n]o person shall circumvent a
6 technological measure that effectively controls access to a work protected under this
7 title.” 17 U.S.C. § 1201(a)(1)(A). A technological measure effectively controls access
8 to a work if, “in the ordinary course of its operation, requires the application of
9 information, or a process or a treatment, with the authority of the copyright owner, to
10 gain access to the work.” 17 U.S.C. § 1201(a)(3)(B). To circumvent a technological
11 measure means “to descramble a scrambled work, to decrypt an encrypted work, or
12 otherwise to avoid, bypass, remove, deactivate, or impair a technological measure,
13 without the authority of the copyright owner.” 17 U.S.C. § 1201(a)(3)(A).
14
15
16

17 **B. Present Action**

18
19 Plaintiffs asserts a single cause of action against Defendant: breach of the anti-
20 circumvention provisions of 17 U.S.C. § 1201(a). Defendant argues that Plaintiffs have
21 failed a state a claim. The Court reviews each of Defendant’s arguments in turn.
22

23 **a. Public Access of YouTube Videos**

24 Defendant first contends that Plaintiffs have not alleged a violation of the DMCA
25 because “their works are freely accessible.” Mot. at 19-22. Defendant argues that
26 Plaintiffs have conceded that users may “watch and listen to YouTube content for free”
27 and do not allege that “users encounter any technological measure before they are able
28

1 to perceive the works – no paywall, password, authentication, nor any other barrier.”
2 *Id.* at 20. However, this argument is unsupported by the factual allegations in the CAC
3 and the legal precedent of this circuit.
4

5 As an initial matter, Plaintiffs *do* allege that a user encounters the TPMs to access
6 the content. According to the CAC, a user will not be able to access content *except*
7 through YouTube’s authorized streaming architecture. Each of the alleged TPMs serve
8 the control access to the work by ensuring access only through the permitted channel:
9 the YouTube streaming architecture. *See* CAC ¶¶ 2, 38.
10
11

12 The rolling cipher and proof of origin tokens, as alleged, each require a user to
13 satisfy certain conditions in advance of viewing the content, or providing the proprietary
14 decryption key and providing correct proof-of-origin tokens. CAC ¶¶ 50-52, 62-65.
15 Plaintiffs further allege that access is restricted through the temporary, session-bound
16 media URLs which permit access only for a limited period and particular session. *Id.*
17 ¶¶ 56-57. Moreover, Plaintiffs allege that YouTube retroactively monitors access by
18 using IP-based blocking, rate monitoring, and CAPTCHA challenges to detect and
19 restrict suspicious or prohibited activity. *Id.* ¶¶ 53-55, 58-61. Whether, as a factual
20 matter, these technological measures actually function as TPMs is an inappropriate
21 inquiry at this stage. Plaintiffs have plausibly alleged that these measures do control
22 access under the meaning of the DMCA.
23
24
25
26

27 The Court is not persuaded by Defendant’s contention that a technological
28 measure does not control access merely because the user does not affirmatively interact

1 with a visible barrier. Mot. at 20. Nothing in § 1201(a) requires an access control to take
2 the form of a paywall, password prompt, or other measure requiring affirmative user
3 input. Rather, the statutory inquiry is whether the technological measure, “in the
4 ordinary course of its operation,” requires the application of authorized “information,
5 or a process or a treatment” to gain access to the work. 17 U.S.C. § 1201(a)(3)(B).
6

7
8 As alleged, YouTube’s system performs background authentication and
9 authorization processes before granting access to a video, and continued access remains
10 subject to additional technological restrictions. The fact that these access restrictions
11 may be less onerous than other potential protective measures, or readily permit access
12 to users who satisfy relatively minimal requirements, does not mean that no barriers to
13 access exist. As alleged, the barriers exist and require users to satisfy certain conditions
14 before obtaining access. Those barriers may be modest, perhaps by design given
15 YouTube’s business model, but they are barriers nonetheless. At the pleadings stage,
16 Plaintiffs’ allegations are sufficient.
17
18
19

20 This position is consistent with the Ninth Circuit’s previous holding in *Disney*
21 *Enterprises, Inc. v. VidAngel Inc.*, upholding a preliminary injunction based in part on
22 violations of the DMCA anti-circumvention provision. Disney distributed and licensed
23 its work through specified distribution channels, including the sale of physical DVDs
24 or Blu-Ray discs. *Disney Ent., Inc. v. VidAngel, Inc.*, 869 F.3d 848, 853 (9th Cir. 2017).
25 These discs included encryption-based technological protection measures that allowed
26 licensed players to decrypt content for lawful playback. *Id.* VidAngel purchased several
27
28

1 of these DVDs and Blu-Ray discs and used a software to decrypt them, obtaining a
2 digital copy of the content. *Id.* Once decrypted, VidAngel created and sold versions of
3 the copyrighted material with certain “objectionable content” removed. *Id.* at 853-54.
4

5 The Ninth Circuit concluded that, by bypassing the encryption on the DVD and
6 Blu-Ray discs without authorization, VidAngel had circumvented an access control in
7 violation of the DMCA. *Id.* at 865. Significantly, the Ninth Circuit rejected the
8 proposition that a work ceases to be protected by an access control merely because
9 consumers have authorized means of accessing it, observing “[n]othing in the legislative
10 history suggests that VidAngel did not circumvent an access control simply because
11 there are authorized ways to access the [] works.” *Id.*
12
13

14 The same reasoning applies here. As alleged, YouTube’s TPMs condition access
15 to the videos on use of YouTube’s authorized streaming architecture and satisfaction of
16 the technological requirements embedded within that process. The fact that members of
17 the public may ordinarily access the videos without payment does not establish that the
18 works are technologically unrestricted. Just as the authorized players in VidAngel
19 provided consumers with an authorized means of accessing encrypted DVDs and Blu-
20 ray discs, YouTube’s streaming architecture provides an authorized means of accessing
21 video content. *See also Sony Music Ent. v. Uncharted Labs, Inc.*, 2026 WL 1019199, at
22 * 3 (S.D.N.Y. Apr. 15, 2026) (declining to dismiss a complaint based on allegations
23 that YouTube’s rolling cipher served as a TPM under the DMCA anti-circumvention
24 provision); *Yout LLC v. Recording Industry Ass’n of Am., Inc.*, 633 F. Supp. 3d 650,
25
26
27
28

1 666-72 (D. Conn. 2022) (concluding that Plaintiff failed to plausibly allege that
2 YouTube did not use technological protections measures that control access to the
3 copyrighted works within the meaning of the DMCA).
4

5 In short, the Court concludes that the Plaintiffs works are not freely accessible,
6 still requiring certain technological requirements be met prior to access.
7

8 **b. TPMs as Access Controls**

9 Defendant next argues that Plaintiffs asserted TPMs are only “copy controls,” not
10 “access controls” under the meaning of DMCA. Defendant argues that each of the five
11 TPMs alleged only limit downloading content, not accessing it. Mot. at 22-28.
12 However, Defendant’s arguments are inconsistent with Plaintiff’s allegations or present
13 factual disputes that are inappropriate for resolution at this stage.
14
15

16 **i. The Rolling Cipher**

17 Defendant argues the rolling cipher is not an access control since (1) it functions
18 as a lock with a key attached at all times; (2) does not restrict the file URL because a
19 sophisticated user may still obtain the file; and (3) is only a copy control, not an access
20 control. Mot. 23-25.
21

22 The first argument is unpersuasive. Contrary to Defendant’s assertion, Plaintiff
23 has not alleged that the rolling cipher is a lock with the key perpetually attached. Rather,
24 Plaintiffs allege that the rolling cipher requires the key, or the proprietary YouTube
25 decryption, to provide the video. CAC ¶ 50. Defendant’s second argument presents a
26 pure factual dispute about the mechanics of the rolling cipher and YouTube’s webpage
27
28

1 that is inappropriate for resolution at this stage.

2 Finally, the argument that the rolling cipher is only alleged as a copy control is
3 unavailing. As a matter of law, it is irrelevant that the rolling cipher may also restrict
4 download access since the statute does “not provide that a TPM cannot serve as both an
5 access control and a use control.” *Disney Ent., Inc.*, 869 F.3d at 864. Moreover,
6 Plaintiffs do allege that the rolling cipher restricts viewing and streaming since
7 streaming is restricted to the YouTube streaming architecture, which provides the
8 relevant encryption key. CAC ¶¶ 50-52; *see also Cordova v. Huneault*, 817 F. Supp. 3d
9 819, 834 (N.D. Cal. 2026) (finding that plaintiff had adequately pled that YouTube’s
10 rolling cipher effectively controlled access under § 1201(a)). To the degree that
11 Defendant’s dispute Plaintiffs’ characterization of the rolling cipher, they present a
12 question of fact inappropriate for resolution at the pleadings stage.

13 Thus, the Court concludes that the rolling cipher, as alleged, constitutes an access
14 control.

15 **ii. IP Blocking and Rate Limiting**

16 Defendant first argues that the IP blocking and rate limiting cannot be a copy
17 control because it targets copying, or downloads, of the video. However, as previously
18 discussed, Plaintiffs have alleged that IP blocking and rate limiting control access to the
19 platform as a whole because YouTube authenticates a requestor’s IP address before
20 allowing the user to proceed to the site. CAC ¶ 103.

21 Next, Defendant argues that these procedures are a “monitoring and blocking

1 system” that cannot effectively control access to a work under the meaning of the
2 DMCA because there is no application of a process to “*gain access* to the work.” Mot.
3 at 25-26. However, the fact that a measure may revoke access after access has initially
4 been granted does not preclude that measure from qualifying as an access control under
5 the meaning of the DMCA. The Ninth Circuit has rejected that proposition, noting that
6 an access control includes measures that “revoke access if a secondary check determines
7 that access was unauthorized.” *MDY Industries, LLC*, 629 F.3d at 943. As alleged, the
8 IP blocking and rate monitoring systems serve as this “secondary check,” by monitoring
9 for suspicious activity and revoking access when the resulting data indicates that access
10 was improper.
11
12
13

14 **iii. Session-Bound Short Lived URLs**

15 Defendant argues that there are no factual allegations that Defendant or any user
16 could not use these URLs to view a work without restriction before its expiration. Mot.
17 at 26. The argument here is not appropriate for the pleadings stage. Plaintiffs have
18 plausibly alleged that Defendant must have “programmatically renew[ed] access
19 credentials outside ordinary playback sessions” in order to engage in bulk extraction of
20 YouTube videos. CAC ¶¶ 93, 109. At this stage, these allegations are sufficient.
21
22
23

24 **iv. CAPTCHA Challenges**

25 Defendant first argues that CAPTCHA challenges cannot be a TPM under the
26 DMCA because they do not “initially block a user’s attempt to view a video and only
27 appear in limited circumstances[.]” Mot. at 27. However, as noted in the discussion on
28

1 IP blocking and rate limiting, the Ninth Circuit has held that technological programs
2 that control access *after* its initial grant may still qualify as an access control. *MDY*
3 *Industries, LLC*, 629 F.3d at 943.

4
5 Defendant next argues that Plaintiffs have failed to plead that Defendant was
6 prevented from accessing a particular video due to the CAPTCHA challenges. This
7 position, however, misstates Plaintiffs' position. Plaintiffs do not assert that Defendant
8 met and completed CAPTCHA challenges. Rather, that Defendant engaged in behavior
9 that would ordinarily have triggered CAPTCHA challenges but Defendant used
10 processes like IP rotation to avoid the mechanism entirely. CAC ¶ 59. These allegations
11 are sufficient to survive a motion to dismiss.
12
13

14 **v. Proof of Origin Tokens**
15

16 Finally, with respect to the proof of origin tokens, Defendant advances arguments
17 similar to those it raised regarding the rolling cipher. Defendant argues that the proof of
18 origin tokens are, at best, a lock with the key attached. Mot. at 27-28. However, these
19 arguments are unpersuasive for the same reasons the Court articulated in its analysis of
20 the rolling cipher. The proof of origin tokens, as alleged by Plaintiffs, limit access to
21 videos by ensuring access requests originate from the intended playback context. CAC
22 ¶ 62. Again, to the extent Defendant disputes the operations of the proof of origin
23 tokens, such arguments are inappropriate at the pleadings stage.
24
25

26 Accordingly, the Court concludes that Plaintiffs have sufficiently alleged that
27 each of the TPMs serve as access controls, not copy controls.
28

1 **C. Sufficiency of Allegations Around Timing**

2 Finally, Defendant argues that Plaintiffs have not sufficiently alleged information
3
4 on the technological measures in place at the time of the alleged circumvention.
5 Defendant claims that “Plaintiffs have described a variety of technological measures”
6 but “Plaintiffs have not alleged any information about when YouTube implemented
7 those measures – let alone whether they were in place at the time Snap accessed the
8 videos.” Mot. at 28-29.
9

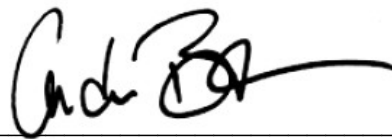
10 Reading the CAC in the light most favorable to the non-moving party, this
11 argument is not convincing. Plaintiffs have alleged that the five TPMs existed at the
12 time Defendant scraped the YouTube videos. CAC ¶¶ 45-49. This is sufficient to
13 support the timing element and place Defendant on notice.
14
15

16 **IV. CONCLUSION**

17 For the foregoing reasons, the Court **DENIES** Defendant’s Motion to Dismiss.

18 **IT IS SO ORDERED.**

19
20 Dated: August 19, 2026



21 HONORABLE ANDRÉ BIROTTE JR.
22 UNITED STATES DISTRICT COURT JUDGE
23
24
25
26
27
28