

1 Rom Bar-Nissim (SBN 293356)  
Rom@HeahBarNissim.com  
2 HEAH BAR-NISSIM LLP  
1801 Century Park East, Suite 2400  
3 Los Angeles, CA 90067  
Telephone: (310) 432-2836  
4

*Attorney for Plaintiffs and the Proposed Class*  
5 [additional counsel on signature page]  
6

7 **UNITED STATES DISTRICT COURT**  
8 **NORTHERN DISTRICT OF CALIFORNIA**

9 TED ENTERTAINMENT, INC., MATT  
10 FISHER, and GOLFHOLICS, INC., each  
individually and on behalf of all others  
11 similarly situated,

12 Plaintiffs,

13 v.

14 APPLE, INC.,  
15 Defendant  
16

Case No.: 3:26-cv-2936

**CONSOLIDATED CLASS ACTION**  
**COMPLAINT**

**DEMAND FOR JURY TRIAL**

1 Plaintiffs Ted Entertainment, Inc. (“TEI”), Matt Fisher, and Golfholics, Inc. (collectively,  
2 where appropriate “Plaintiffs”), each individually and on behalf of all others similarly situated (the  
3 “Class,” as defined below), by and through their undersigned counsel, file this Complaint against  
4 Apple, Inc. (“Defendant”), for violations of the Digital Millennium Copyright Act (“DMCA”), 17  
5 U.S.C. § 1201. The allegations contained herein, which are based on Plaintiffs’ knowledge of facts  
6 pertaining to themselves and their own actions and counsels’ investigations, and upon information  
7 and belief as to all other matters, are as follows:

### 8 **NATURE OF THE ACTION**

9 1. This is a nationwide class action for violations of the DMCA’s anti-circumvention  
10 provisions, 17 U.S.C. § 1201(a), arising from Defendant unlawfully circumventing technological  
11 protection measures to access and scrape millions of copyrighted videos from the online video  
12 viewing platform, YouTube, in order to feed, train, improve, and commercialize Defendant’s large-  
13 scale generative text-to-video artificial intelligence (“AI”) model (hereinafter referred to as “Apple  
14 AI Video”).

15 2. YouTube allows the public to view audiovisual works only through controlled  
16 streaming, keeping its underlying video files locked away behind careful access restrictions.

17 3. YouTube does not provide public access to the underlying audiovisual works  
18 themselves, but instead delivers those works through a controlled streaming architecture that  
19 includes technological protection measures (“TPMs”) which require the application of authorized  
20 processes, including tokenized requests, segmented delivery protocols, and player-based  
21 reconstruction.

22 4. Defendant published a peer-reviewed academic paper authored by its own  
23 researchers publicly disclosing that it trained Apple AI Video on Panda-70M—a dataset derived  
24 entirely from millions of YouTube videos that were themselves extracted from YouTube through  
25 circumvention of YouTube’s TPMs.

26 5. Defendant deployed tools designed to evade and circumvent YouTube’s TPMs by  
27 deploying automated systems that replicated and manipulated authorized request flows while  
28 evading enforcement mechanisms, thereby gaining access to the underlying works in a form not

1 available to the public and outside the conditions authorized by the copyright owner.

2 6. On information and belief, Defendant used automated video-downloading programs  
3 combined with virtual machines that rotated IP addresses to avoid detection and blocking, enabling  
4 the mass unauthorized access and extraction of videos at the scale necessary to train Apple AI  
5 Video. Defendant then used Plaintiffs' and Class Members' intellectual property for their own  
6 commercial gain in developing and commercializing Apple AI Video. In doing so, Defendant has  
7 violated the law (and YouTube's Terms of Service), which were intended to protect Plaintiffs and  
8 others similarly situated.

9 7. By accessing, scraping, and downloading those files, Defendant deliberately  
10 circumvented YouTube's access controls to obtain the training data necessary to build and  
11 commercialize Apple AI Video.

12 8. This case does not concern ordinary viewing or downstream copying of publicly  
13 available content. It concerns Defendant's deliberate circumvention of YouTube's controlled  
14 streaming architecture to access copyrighted works in a form and manner not made available to the  
15 public. YouTube does not provide open access to audiovisual works themselves, but instead  
16 conditions access on the application of specific technical processes that Defendant intentionally  
17 bypassed.

18 9. Plaintiffs and the Class Members whom Plaintiffs seek to represent are content  
19 creators who upload their audiovisual content to YouTube. On information and belief, the  
20 audiovisual content of Class Members was among the video content utilized by Defendant to train  
21 Apple AI Video and related generative AI models.

22 10. In uploading content to YouTube, content creators are authorizing and instructing  
23 YouTube to provide protection to the video content through YouTube's anti-circumvention  
24 software. In fact, YouTube's anti-circumvention software are a driving factor behind many content  
25 creators' decision to upload their video content to YouTube.

26 11. Rather than seek permission or pay a fair price for the audiovisual content hosted on  
27 YouTube, Defendant harvested content creators' protected and copyrighted videos for commercial  
28 use and at scale without consent or compensation to the content creators.

1           12. Defendant’s actions were not only unlawful, but an unconscionable attack on the  
2 community of content creators whose content is used to fuel the multi-trillion-dollar generative AI  
3 industry without any compensation.

4           13. Content creators such as Plaintiffs and the Class Members will never be able to claw  
5 back the intellectual property unlawfully copied and used by Defendant to train its generative AI  
6 models. Once AI ingests content, that content is stored in its neural network and not capable of  
7 deletion or retraction. Defendant’s actions constitute abuse and exploitation of content creators’  
8 work for Defendant’s profit.

9           14. Most YouTube videos are not registered with the U.S. Copyright Office. That lack  
10 of registration, however, does not render them valueless or leave them unprotected. Content  
11 creators invest time, skill, and resources into producing their works, and they rely on YouTube’s  
12 TPMs to safeguard their files from unauthorized access. Because copyright registration is not a  
13 prerequisite for protection against unlawful circumvention of access controls, this claim is  
14 especially critical where Defendant’s misconduct lies in breaking through access barriers that  
15 prevent anyone from obtaining the underlying files in the first place.

16           15. It is also critical to protect a flourishing internet ecosystem. In a world where  
17 Defendant and others can circumvent technological protections to exploit copyrighted works  
18 without authorization with impunity, creators will be less likely to make their creations available  
19 on YouTube and other similar platforms, for fear of losing all control of them. The world will be  
20 poorer for it.

21           16. An essential component of Defendant’s business model—powering AI features and  
22 services with large-scale training data—includes the mass acquisition and ingestion of creators’  
23 videos scraped from YouTube.

24           17. Defendant has profited substantially from its infringement of Plaintiffs’ and Class  
25 Members’ video content through Defendant’s training of its generative AI products. Defendant’s  
26 massive financial success would not have been possible without the video content created by  
27 Plaintiffs and Class Members, which was intended for streaming on YouTube.

28           18. Plaintiffs bring this class action on behalf of themselves and on behalf of a

1 nationwide class of YouTube creators whose works were scraped, ingested, and trained on without  
2 authorization, seeking statutory damages, injunctive relief, restitution, and all other remedies  
3 allowed by law pursuant to the DMCA § 1201(a) seeking an injunction and damages commensurate  
4 with the scope of Defendant’s massive and ongoing infringement.

5 **THE PARTIES**

6 19. Plaintiff Ted Entertainment, Inc. (“TEI”), is an independent California based media  
7 company and content creator with over 5,800 original videos on YouTube, with a combined total  
8 of over 4 billion views. TEI has amassed a substantial following on YouTube with over 2.6 million  
9 subscribers to its channels. TEI owns and operates the channels “h3h3 Productions” and “H3  
10 Podcast Highlights.” H3H3 Productions appears with 155 videos in Panda-70M. H3 Podcast  
11 Highlights appears with 283 videos in Panda-70M. Plaintiff invested significant resources – time  
12 and money – into producing and publishing this video content and bringing awareness to its content.

13 20. Plaintiff TEI is the creator of the videos identified in Exhibit A, all of which were  
14 uploaded exclusively to YouTube by Plaintiff. Plaintiff derives value from the works identified in  
15 Exhibit A through viewership, advertising, sponsorships, licensing, and related monetization.

16 21. Plaintiff TEI and its owners – Ethan and Hila Klein – are longtime champions of the  
17 rights of YouTube creators. The Kleins helped define what constitutes fair use reaction videos and  
18 the good faith belief standard for DMCA counternotifications. TEI has championed online free  
19 speech and is currently helping define what reaction content does not constitute fair use to ensure  
20 YouTube content creators can enjoy the fruits of their labor.

21 22. Plaintiff Matt Fisher is an individual and resident of the State of California. He is a  
22 golf content creator who posts his original videos on YouTube, many of which are instructional.  
23 His channel is “MrShortGame Golf” on the YouTube platform. He has over 500,000 subscribers  
24 and hundreds of millions of views. Plaintiff has invested substantial time and money into bringing  
25 awareness around his content. MrShort Game appears with 8 videos in Panda-70M.

26 23. Plaintiff Matt Fisher is the creator of the videos identified in Exhibit B, all of which  
27 were uploaded exclusively to YouTube by Plaintiff and all of which were included in datasets used  
28 by Defendant to train its generative AI models. Plaintiff derives value from the works identified in

1 Exhibit B through viewership, advertising, sponsorships, licensing, and related monetization.

2 24. Plaintiff Golfholics is a corporate entity organized pursuant to the laws of the State  
3 of California. It is a golf content channel that posted its original videos on YouTube. The channel  
4 is “Golfholics” on the YouTube platform. It has over 130,000 subscribers and millions of views.  
5 Plaintiff invested substantial time and money into bringing awareness around its content. Golfholics  
6 appears with 62 videos in Panda-70M..

7 25. Plaintiff Golfholics is the creator of the videos identified in Exhibit C, all of which  
8 were uploaded exclusively to YouTube by Plaintiff and all of which were included in datasets used  
9 by Defendant to train its generative AI models. Plaintiff derives value from the works identified in  
10 Exhibit C through viewership, advertising, sponsorships, licensing, and related monetization.

11 26. Defendant Apple Inc., is a Delaware corporation with its principal place of business  
12 at One Apple Park Way, Cupertino, CA 95014.

13 **JURISDICTION AND VENUE**

14 27. This Court has subject matter jurisdiction under 28 U.S.C. § 1332(d) (the Class  
15 Action Fairness Act) because the amount in controversy exceeds \$5,000,000, exclusive of interest  
16 and costs, and a member of the Class is a citizen of a different state than Apple. This Court also has  
17 subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under 17 U.S.C. §  
18 1201, et seq..

19 28. The Court has supplemental jurisdiction over related state-law claims, if any, under  
20 28 U.S.C. § 1367.

21 29. Personal jurisdiction is proper because Defendant’s principal place of business is in  
22 Cupertino, California, transacts business nationwide, purposefully avails itself of this forum, and a  
23 substantial part of the events or omissions giving rise to these claims occurred or were directed  
24 here.

25 30. Venue lies in this judicial district pursuant to 28 U.S.C. § 1391(b)(1) and/or 1400(a)  
26 because Defendant resides in, is found in, or may be sued in this District, and a substantial part of  
27 the events giving rise to the claims occurred here.

28 31. Plaintiffs reserve the right to refine jurisdiction and venue allegations after discovery

1 and as additional facts become available.

2 **FACTUAL BACKGROUND**

3 **A. YouTube Employs TPMs that Function as Access Controls Over Video Files.**

4 32. As noted above, Plaintiffs and the Class Members are content creators of audiovisual  
5 content. Plaintiffs and the Class Members create original video content that has been uploaded onto  
6 YouTube’s video sharing platform.

7 33. The audiovisual work at issue is embodied in digital form through encoded media  
8 streams and associated data structures that together constitute the work itself. The segmented  
9 streams and underlying media representations obtained by Defendant collectively comprise the  
10 copyrighted work and are not distinct from it.

11 34. YouTube’s “users”—the individuals who view the digital content available on  
12 YouTube—can watch and listen to videos for free on YouTube’s advertising-supported service,  
13 but YouTube prevents access to the digital files underlying the content viewed by the user through  
14 YouTube’s authorized playback mechanism.

15 35. While YouTube permits members of the public to view audiovisual works through  
16 its platform, such permission is limited to access through YouTube’s authorized playback  
17 environment and subject to the technological conditions imposed by its delivery systems.

18 36. For example, YouTube does not authorize access to audiovisual works through  
19 automated extraction, direct retrieval of media streams, or reconstruction of works outside its  
20 controlled environment.

21 37. YouTube does not provide users with direct access to audiovisual works in their  
22 native or fixed form. YouTube only delivers audiovisual works through a controlled streaming  
23 architecture that transmits segmented, time-limited portions of a work for ephemeral playback  
24 within YouTube’s proprietary player environment.

25 38. To protect against file level access, YouTube deploys multiple TPMs designed to  
26 control, restrict, and monitor access to the underlying video files and to deter extraction outside  
27 YouTube’s controlled playback environment.

28 39. YouTube’s TPMs effectively control access to audiovisual works by requiring the

1 application of information and processes with YouTube’s authorization before a user may obtain  
2 the work in usable form.

3 40. These TPMs control how videos are delivered and accessed. For example, YouTube  
4 uses temporary, expiring links to send pieces of a video; breaks videos into small segments that  
5 must be put together in a specific way; checks and controls each request to make sure it follows the  
6 proper sequence; and requires the video to be assembled and played through YouTube’s own player  
7 rather than accessed directly.

8 41. In simple terms, YouTube doesn’t just hand over a video file to every user seeking  
9 to view content. It sends the video in pieces, through temporary links, and only lets those pieces be  
10 put together and played using its own system, while checking each step along the way.

11 42. These measures function as access controls because they condition access to the  
12 audiovisual work on the application of authorized processes and prevent users from obtaining the  
13 work outside YouTube’s controlled delivery system.

14 43. Access to a work on YouTube therefore requires the application of a sequence of  
15 authorized processes, including the issuance and validation of session-specific tokens, execution of  
16 player-side instructions, and reconstruction of segmented media streams into a continuous  
17 audiovisual experience. The audiovisual work itself—i.e., the complete, machine-readable  
18 embodiment of the work capable of being copied, processed, or analyzed—cannot be accessed by  
19 the public absent compliance with these technological processes.

20 44. The TPMs specifically alleged here include, among others: (1) an obfuscated  
21 signature system commonly referred to as a “rolling cipher,” (2) IP-based blocking and rate limiting  
22 that restrict high-volume automated access, (3) short-lived, session-bound streaming URLs, (4)  
23 CAPTCHA human-verification challenges triggered by automated activity, and (5) proof-of-origin  
24 tokens that verify requests originating from authorized client environments.

25 45. Each TPM is an access control which independently functions as a gatekeeping  
26 mechanism that must be satisfied before the audiovisual file can be retrieved, and circumvention  
27 of any one of them enables access to the file in a manner not authorized by YouTube or the owners  
28 of the content.

1           46. Defendant accessed and obtained the audiovisual works themselves—not merely  
2 “files” distinct from those works—by reconstructing and assembling the protected media streams  
3 outside YouTube’s authorized environment.

4           47. Defendant exceeded any authorized access by obtaining audiovisual works through  
5 methods that bypassed the technological conditions under which access is granted. Defendant’s  
6 conduct therefore constituted access “without the authority of the copyright owner” within the  
7 meaning of 17 U.S.C. § 1201(a).

8           48. On information and belief, Defendant employed automated systems and tools  
9 designed to bypass YouTube’s TPMs by replicating and manipulating authorized request flows  
10 while avoiding enforcement mechanisms. These actions allowed Defendant to avoid, bypass, and  
11 impair technological measures that otherwise restrict access to audiovisual works, thereby  
12 constituting circumvention under 17 U.S.C. § 1201(a)(3)(A).

13 ***TPM (1) - Rolling cipher***

14           49. YouTube controls access to the underlying media file by withholding a usable file  
15 location unless the requesting client can transform an obfuscated signature parameter using  
16 proprietary logic embedded in the official YouTube player. The playback data delivered to users  
17 contains a scrambled signature that must be processed to produce a valid media request URL.  
18 Without performing this authorized transformation, the server will not deliver the audiovisual file.  
19 Thus, the rolling cipher controls access by requiring application of a specific computational process  
20 before the file can be obtained at all.

21           50. YouTube’s rolling cipher encryption measure acts as a digital lock, controlling  
22 access to content by protecting against unauthorized downloading of underlying media files.  
23 YouTube maintains two different URLs for any given video: the page URL, visible to the user, is  
24 for the webpage where the video playback occurs, and the file URL, not visible to the user, is for  
25 the video file itself that is played within the page. The file URL is encrypted using a complex and  
26 periodically changing algorithm – the rolling cipher – that is designed to impede external access to  
27 the underlying YouTube files. YouTube’s player software uses a decryption routine to authenticate  
28 requests and deliver content only through approved interfaces. This TPM inhibits access to the

1 underlying audiovisual files for the purposes of any downloading, copying or distribution of the  
2 audiovisual content. In other words, the rolling cipher controls access to copies of audiovisual  
3 content uploaded to the platform and impedes an ordinary user from creating a permanent,  
4 unrestricted download of audiovisual content made available on YouTube only for streaming and  
5 restricted downloading.

6 51. The rolling cipher is a TPM measure within the meaning of 17 U.S.C. §1201(a)  
7 because it “effectively controls access” to copyrighted works by preventing users access to the files  
8 of video streams without first executing YouTube’s proprietary decryption code.

9 ***TPM (2) - IP blocking and rate limiting***

10 52. YouTube monitors network behavior and restricts access when excessive or abusive  
11 request patterns are detected. Requests from an IP address that exceeds defined thresholds may be  
12 throttled, denied, or blocked entirely, preventing further retrieval of audiovisual data from that  
13 source. This mechanism controls access by limiting how frequently and at what scale a particular  
14 requester may obtain the file and by cutting off access altogether when abuse is detected.

15 53. YouTube’s infrastructure monitors the number and frequency of video requests  
16 originating from individual IP addresses. This system serves an important function. Even if a user  
17 were able to generate a valid media request for an individual video, YouTube’s infrastructure is  
18 designed to prevent automated systems from retrieving large numbers of videos at scale.

19 54. Once YouTube detects abnormal volume of access to files, the system can block the  
20 offending IP address from accessing YouTube’s servers. This prevents automated scraping systems  
21 from accessing large volumes of copyrighted audiovisual content.

22 55. This IP-based monitoring and blocking system therefore also functions as a TPM  
23 measure within the meaning of 17 U.S.C. §1201(a) because it “effectively controls access” to  
24 copyrighted works by restricting automated access to YouTube’s underlying video files.

25 ***TPM (3) - Session-bound, short-lived URLs***

26 56. Even after a valid media URL is generated, YouTube restricts access by issuing  
27 URLs that are temporary, cryptographically signed, and tied to a particular playback session and  
28 client context. These URLs include authorization parameters such as expiration timestamps and

1 client identifiers. Once the authorization window expires or the session ends, the server will refuse  
2 to deliver the audiovisual file in response to that URL. Accordingly, possession of a previously  
3 valid link does not provide continuing access to the file, and new authorization must be obtained to  
4 retrieve it. This mechanism therefore controls access by limiting when and from where the file may  
5 be requested.

6 57. Because session-bound URLs expire automatically, any automated system  
7 attempting to access videos outside ordinary playback cannot rely on a static link and must instead  
8 repeatedly obtain fresh authorization parameters and regenerate valid media URLs. By  
9 programmatically renewing expired credentials and initiating new authorized sessions at machine  
10 speed, automated scraping tools can maintain continuous access to audiovisual files that would  
11 otherwise become unavailable once the original authorization lapses. This conduct circumvents the  
12 temporal and session-based restrictions imposed by YouTube and allows persistent retrieval of files  
13 in a manner not available to ordinary users. Circumventing this measure constitutes circumvention  
14 of a technological measure that effectively controls access to a copyrighted work in violation of 17  
15 U.S.C. § 1201(a).

16 ***TPM (4) - CAPTCHA challenges***

17 58. When traffic patterns indicate automated or suspicious activity, YouTube may  
18 require completion of a CAPTCHA challenge before allowing further requests to proceed. Until  
19 the challenge is successfully completed, the requesting client cannot obtain the data necessary to  
20 retrieve the audiovisual file. CAPTCHAs therefore function as an access control by conditioning  
21 continued access to content on proof that the requester is a human user rather than an automated  
22 system.

23 59. Large-scale scraping operations necessarily generate request patterns that would  
24 ordinarily trigger such human-verification challenges. To continue accessing without interruption,  
25 automated systems must be configured either to evade detection, distribute requests across multiple  
26 machines, or otherwise prevent CAPTCHA enforcement from halting access. By avoiding or  
27 neutralizing these verification gates, such systems obtain audiovisual data without demonstrating  
28 the human interaction that YouTube requires for continued access. Defeating or bypassing this

1 human-verification mechanism constitutes circumvention of a technological measure that  
2 effectively controls access to copyrighted works in violation of 17 U.S.C. § 1201(a).

3 ***TPM (5) - Proof-of-origin tokens***

4 60. YouTube further restricts access by requiring that requests for video segments  
5 include cryptographic tokens demonstrating that the request originates from an authorized client  
6 environment operating within the intended playback context. These tokens are generated during  
7 playback and validated by YouTube's servers before data is delivered. Requests lacking valid  
8 tokens, or presenting forged or replayed tokens, are denied or degraded. This mechanism controls  
9 access by preventing unauthorized software from directly requesting the audiovisual file unless it  
10 can present credentials proving it is an approved client.

11 61. Automated tools operate outside YouTube's authorized player environment and  
12 therefore must extract, replicate, or reuse the necessary request parameters in order to obtain access  
13 to video data. By presenting such credentials outside their intended context, these tools can retrieve  
14 audiovisual files without operating as approved clients. This conduct bypasses the origin-  
15 verification function of the token system and enables direct access to media files that would  
16 otherwise be delivered only to authorized playback software. Such bypassing constitutes  
17 circumvention of a technological measure that effectively controls access to copyrighted works in  
18 violation of 17 U.S.C. § 1201(a).

19 **B. YouTube's Terms of Service Reinforce their Technological Protection**  
20 **Measures**

21 62. YouTube's Terms of Service describe and reinforce YouTube's TPMs. YouTube's  
22 Terms of Service expressly prohibit scraping, unauthorized downloading, bulk extraction, or other  
23 forms of data mining of audiovisual content except through expressly permitted features or licensed  
24 APIs. These contractual restrictions operate together with YouTube's TPMs to prevent unlicensed  
25 access to creators' videos.

26 63. According to YouTube's Terms of Service, content creators such as Plaintiffs who  
27 upload content onto YouTube grant license to YouTube for certain uses as well as to other users of  
28 YouTube to access content through YouTube's services; however, the license makes clear that it

1 “does not grant any rights or permissions for a user to make use of [the] Content independent of  
2 the Service.”<sup>1</sup>

3 64. This language confirms that end users are not given access to the file itself, only the  
4 ability to view (*i.e.*, stream) through YouTube’s controlled environment. YouTube’s Terms of  
5 Service reflect YouTube’s intent to use the TPMs described above to restrict access to the digital  
6 files underlying the videos that YouTube’s users are allowed to stream through YouTube’s  
7 platform.

8 65. Streaming through YouTube and downloading permanent copies provide the user  
9 with different value propositions—watching and listening for free but seeing ads, versus possessing  
10 a permanent digital copy.

11 66. Accordingly, scraping or bulk downloading is not merely copying material already  
12 provided; it is an act of unauthorized access to data files that YouTube affirmatively withholds  
13 from public download.

14 67. In fact, during a Bloomberg interview about OpenAI (another generative text-to-  
15 video artificial intelligence competitor) scraping YouTube’s CEO, Neal Mohan, confirmed that  
16 unauthorized scraping constitutes a violation of creators’ rights and YouTube’s Terms of Service  
17 stating, “From a creator’s perspective, when a creator uploads their hard work to our platform, they  
18 have certain expectations. One of those expectations is that the terms of service is going to be  
19 abided by,” Mohan said, “It does not allow for things like transcripts or video bits to be downloaded,  
20 and that is a clear violation of our terms of service. Those are the rules of the road in terms of  
21 content on our platform.”<sup>2</sup>

22 68. The scraping and acquisition processes used by Defendant to circumvent YouTube’s  
23 TPMs were inconsistent with, and in violation of, YouTube’s Terms of Service, which forbid  
24 scraping and mass downloading of videos.<sup>3</sup>

25 <sup>1</sup> “Terms of Service,” YouTube, <https://www.youtube.com/t/terms> (last viewed March 11, 2026).

26 <sup>2</sup> Davey Alba & Emily Chang, *YouTube Says OpenAI Training Sora With Its Videos Would Break*  
27 *Rules*, Bloomberg (Apr. 4, 2024), [https://www.bloomberg.com/news/articles/2024-04-04/youtube-  
28 says-openai-training-sora-with-its-videos-would-break-the-rules](https://www.bloomberg.com/news/articles/2024-04-04/youtube-says-openai-training-sora-with-its-videos-would-break-the-rules) (video available at  
[https://www.youtube.com/watch?v=FBZ\\_BeChRg](https://www.youtube.com/watch?v=FBZ_BeChRg)).

<sup>3</sup> *Supra*, note 1 (prohibiting “access, reproduce, download, distribute, transmit, broadcast, display,  
sell, license, alter, modify or otherwise use any part of the Service or any Content except: (a) as  
(continued).

1           69. Although YouTube offers downloading options to subscribers who pay for  
2 YouTube’s “Premium” plan, YouTube still employs TPMs to restrict access. Specifically,  
3 YouTube prohibits all downloading audiovisual content except to the YouTube app. Further, the  
4 “download” option only makes audiovisual content available for offline streaming—it does not  
5 provide the Premium subscriber with access to the audiovisual files. Accordingly, the audiovisual  
6 files cannot be transferred to any other device, but remain only for streaming on the app. Finally,  
7 the files are available only for offline streaming for a limited amount of time, at which point they  
8 will become available only for online streaming once again. For users who do not have a “Premium”  
9 plan, the “download” option on YouTube’s player page is non-functional.

10           70. YouTube’s Terms of Service and policies reinforce the variety of TPMs YouTube  
11 implements to restrict access to Plaintiffs’ and Class Members’ underlying audiovisual files.

12           **C. Defendant Improperly Circumvented YouTube’s Technological Protection**  
13           **Measures to Obtain Millions of YouTube Videos to Train Its Foundational AI**  
14           **Model.**

15           71. As noted above, Defendant requires significant amounts of data to feed, train,  
16 improve, and commercialize Apple AI Video.

17           72. Without authorization, Defendant accessed Plaintiffs’ and Class Members’  
18 audiovisual content from YouTube for use in its training data for Apple AI Video. To do so,  
19 Defendant unlawfully circumvented YouTube’s TPMs that YouTube implemented in its effort to  
20 impede the downloading of audiovisual content from its platform.

21           73. Apple AI Video is not a research tool. It is Defendant's plan to commercialize a  
22 text-to-video generative AI model. Defendant is a for-profit company.

23           74. Because Apple AI Video models are a core feature of Defendant's future plans,  
24 Defendant had an overwhelming incentive to acquire training data on an unprecedented scale.  
25 Rather than negotiate for lawful licenses, Defendant broke through YouTube's access protections  
26 to access the underlying files needed to utilize the massive datasets necessary to fuel Apple AI  
27 Video and, by extension, Defendant's broader product lines.

28           \_\_\_\_\_ expressly authorized by the Service; or (b) with prior written permission from YouTube and, if applicable, the respective rights holders;”).

1           75. Defendant has sought to develop Apple AI Video so it is capable of, among other  
2 things, turning language prompts into audiovisual content. In other words, Defendant has sought  
3 to, and has had success with, creating an AI product that accepts language instruction and produces  
4 a video based on that instruction.

5           76. The dataset central to Defendant's unlawful acquisition of training data for Apple  
6 AI Video is Panda-70M, a derivative dataset of HD-VILA-100M, compiled by Snap, Inc.

7           77. Defendant's own researchers publicly admitted to training Apple AI Video on  
8 Panda-70M in a paper titled *STIV: Scalable Text and Image Conditioned Video Generation*, co-  
9 authored by fourteen named Apple employees.<sup>4</sup> In the paper's Section 3.1, under the heading  
10 "Data," the authors state: "our data sources include Panda-70M." Panda-70M is a dataset compiled  
11 from 3,098,462 YouTube videos — and consists of approximately 70.8 million video clips  
12 extracted from those YouTube sources, none of which were obtained with the authorization of  
13 YouTube or the copyright holders whose works they contain. By publishing this admission in a  
14 citable academic paper under Apple institutional affiliation, Defendant's own researchers confirmed  
15 in writing that Apple AI Video was trained on a dataset derived from YouTube content accessed  
16 through circumvention of YouTube's TPMs.

17           78. The dataset consist entirely of pointers to YouTube content. Panda-70M does not  
18 contains the underlying audiovisual files. To use either dataset for AI training, a company must  
19 access, retrieve, and download every referenced video directly from YouTube—an act that requires  
20 circumventing YouTube's TPMs at scale.

21           79. YouTube allows users to stream content but prohibits, through contractual terms and  
22 TPMs, accessing the underlying video file of the content it streams. Defendant obtained  
23 unauthorized access to audiovisual content by unlawfully accessing and stream ripping, converting  
24 streaming content into permanent, locally stored files, and by circumventing the TPMs specifically  
25 designed to prevent such access.

26           80. The Panda-70M dataset functions as a map or index file identifying specific  
27 YouTube videos and clips by URL, video identifier, and timestamp. A single YouTube video may

28 <sup>4</sup> Zongyu Lin et al., *STIV: Scalable Text and Image Conditioned Video Generation*,  
arXiv:2412.07730 (Dec. 10, 2024), <https://arxiv.org/pdf/2412.07730>.

1 be divided into numerous clips, each treated as a separate training sample. Extracting any clip  
2 requires independently accessing the source video on YouTube and isolating the designated  
3 segment, a process that constitutes a separate act of circumvention for each clip retrieved.

4 81. Defendant obtained unauthorized access to audiovisual content to train its AI models  
5 by unlawfully “stream ripping” them—*i.e.*, converting the audiovisual streaming content into  
6 permanent, locally-stored files—from YouTube and circumventing TPMs specifically designed to  
7 prevent access for such use.

8 82. Panda-70M was compiled by Snap Inc and released in 2024.<sup>5</sup> In a remarkable act of  
9 institutional irony, Snap, Inc. then published Panda-70M as an open-access blueprint (a detailed,  
10 step-by-step methodology for stream ripping millions of YouTube videos) while purporting to  
11 launder its own unlawful conduct by restricting downstream users to “non-commercial, research  
12 purposes only” and disclaiming that “[n]o commercial license, whether implied or otherwise, is  
13 granted in or to this dataset and code, unless you have entered into a separate agreement with Snap  
14 Inc. for such rights.”<sup>6</sup>

15 83. In other words, having itself circumvented YouTube's TPMs and copied millions of  
16 protected works without authorization or compensation, Snap handed the world a roadmap for  
17 doing the same; then absolved itself of responsibility by declaring the theft permissible so long as  
18 others kept it academic. Snap had no rights to grant or withhold. The underlying videos belong to  
19 the YouTube creators whose content Snap had already unlawfully circumvented and copied.

20 84. The Panda 70M dataset consists of location identifiers that point to millions of  
21 YouTube videos or clips. None of them contains the underlying audiovisual files. To use them in  
22 training, a company must access, retrieve and download every referenced video directly from  
23 YouTube. Defendant used this dataset to initiate millions of individual downloads of protected  
24 YouTube content, all without authorization or compensation, all in violation of YouTube’s TPMs,  
25 and all for the commercial purpose of building its foundational video model.

26 85. Plaintiffs do not yet know the full extent of all datasets Defendant used to train

27 <sup>5</sup> Tsai-Shien Chen et al., *Panda-70M: Captioning 70M Videos with Multiple Cross-Modality*  
28 *Teachers*, arXiv:2402.19479 (Feb. 29, 2024), <https://arxiv.org/abs/2402.19479>.

<sup>6</sup> Panda-70M Project Page, Snap Research, <https://snap-research.github.io/Panda-70M/>

1 Apple AI Video and any derivative or successor models. The identity, contents, sources, and  
2 provenance of all training datasets are exclusively within Defendant's possession, custody, and  
3 control. On information and belief, Defendant used additional datasets beyond those publicly  
4 disclosed that incorporated YouTube-sourced content obtained through the same circumvention  
5 processes alleged herein. The full scope of Defendant's unlawful data acquisition, including any  
6 datasets, scraping pipelines, or third-party data purchases that incorporated YouTube-sourced  
7 content, will be the subject of discovery.

8 **D. Defendant's Automated Scraping Required Circumvention of YouTube's**  
9 **Technological Protection Measures.**

10 86. Bulk extraction of YouTube videos at the scale alleged here cannot occur without  
11 circumventing YouTube's layered TPMs, each of which independently controls access to the  
12 underlying audiovisual files. Illicit tools and services are specifically designed to defeat these  
13 protections, enabling automated systems to retrieve permanent copies of content that YouTube  
14 makes available only for streaming. This process is commonly known as "scraping" or "stream  
15 ripping." Under DMCA § 1201(a), circumvention of any single technological measure that  
16 effectively controls access to a copyrighted work is sufficient to establish liability. YouTube's  
17 protections are layered and overlapping, and the circumvention of one does not negate the  
18 effectiveness or legal significance of the others.

19 87. "Scraping" or "stream ripping" content involves the automated accessing and  
20 downloading of audio and video files directly from a website's servers rather than viewing the  
21 content through the provider's authorized playback environment.

22 88. Upon information and belief, in order to acquire "high-quality text-to-video  
23 generation," Defendant, directly and through agents, contractors, and affiliates, intentionally  
24 accessed large volumes of YouTube videos by scraping and/or using tools and workflows that  
25 bypass or evade YouTube's TPMs and usage restrictions, and then reproduced those videos to  
26 assemble training corpora for Defendant's AI models and services.

27 89. When Defendant scraped audio and video files from YouTube, Defendant did not  
28 simply access and download those files onto the YouTube app for offline streaming, as envisioned

1 by YouTube's Premium plan. Instead, Defendant improperly accessed the underlying audio and  
2 video files and downloaded those files into Defendant's own system, where Defendant had access  
3 over the files and where Defendant could store them indefinitely. These actions circumvented  
4 YouTube's TPMs, violated YouTube's Terms of Service, and are inconsistent with the access  
5 provided by YouTube's Premium plan.

6 90. Defendant also obtained its own separate audiovisual datasets directly through its  
7 own independent scraping of YouTube's video sharing platform.

8 91. To retrieve audiovisual files at scale, Defendant was required to defeat TPM (1), the  
9 rolling cipher that protects the true media file URL. On information and belief, Defendant used one  
10 or more descrambling tools designed to defeat YouTube's proprietary signature-transformation  
11 logic, allowing automated systems to generate valid file requests outside the authorized player  
12 environment and thereby obtain the underlying media files directly. Such tools include, for  
13 example, the open-source program yt-dlp, which is specifically engineered to descramble, replicate,  
14 or extract YouTube's proprietary signature-transformation logic and circumvent the access controls  
15 YouTube uses to prevent unauthorized downloading.

16 92. A descrambling tool such as yt-dlp works by replicating or extracting the signature-  
17 transformation process that YouTube uses to protect its media URLs, allowing a user to bypass the  
18 authorized streaming environment entirely and retrieve the underlying video and audio files directly  
19 from YouTube's servers. Tools of this kind can be used to automatically merge separate audio and  
20 video streams and to download entire playlists at scale. On information and belief, Defendant used  
21 yt-dlp or a substantially similar descrambling tool for precisely this purpose.

22 93. To deploy a descrambling tool such as yt-dlp, a user must first obtain and configure  
23 the program, along with ancillary software necessary to merge video and audio streams into  
24 complete audiovisual files. Once configured, the tool can be directed at individual videos or entire  
25 playlists by supplying the URL for each target video. The result is a complete audiovisual file  
26 retrieved outside of and in circumvention of YouTube's authorized playback environment.

27 94. In simpler terms, a descrambling tool such as yt-dlp acts as a bootleg key for the  
28 lock imposed by YouTube's rolling cipher. On information and belief, Defendant used yt-dlp or a

1 substantially similar tool to improperly access and download audiovisual files from YouTube and  
2 merge them into complete audiovisual packages for ingestion into their generative AI training  
3 pipeline.

4 95. Defendant also defeated TPM (2), YouTube's IP-based monitoring and blocking  
5 system, which restricts high-volume accessing and downloading from a single source. On  
6 information and belief, Defendant implemented an IP-rotation scheme so that when YouTube  
7 detected automated activity and blocked one address, accessing and downloading could  
8 immediately resume from another. This allowed continuous access to audiovisual files despite  
9 YouTube's efforts to detect and terminate abusive activity.

10 96. YouTube uses automated programs to monitor activity from IP addresses, detect  
11 high-volume accessing and downloading behavior, and block those IP addresses from further  
12 access to audiovisual content on the platform. An IP-rotation scheme is specifically designed to  
13 defeat this monitoring system by cycling through different IP addresses to avoid detection and  
14 blocking.

15 97. Executing an IP-rotation scheme at the scale necessary to download the volume of  
16 files indexed in any one of the datasets and required to train Apple AI Video necessarily required  
17 the use of virtual machines or substantially similar infrastructure. A single physical machine with  
18 a fixed IP address would have been detected and blocked almost immediately given the volume of  
19 requests involved. On information and belief, Defendant deployed virtual machines, cloud  
20 computing infrastructure, or substantially similar technology to rotate IP addresses at scale,  
21 ensuring that when YouTube detected and blocked one address, Defendant's downloading  
22 operation could immediately resume from another.

23 98. On information and belief, by repeatedly cycling through IP addresses in this  
24 manner, Defendant ensured that their automated downloading operation could continue  
25 uninterrupted even after YouTube detected and blocked individual addresses. The sheer volume of  
26 videos necessary to train Apple AI Video makes any alternative explanation implausible. The full  
27 details of the specific infrastructure Defendant used to execute this scheme will be the subject of  
28 discovery.

1           99.     Processes such as these allowed Defendant to bypass YouTube’s player page and  
2 avoid YouTube’s monitoring systems in order to access and scrape content from YouTube.

3           100.    Defendant’s conduct necessarily circumvented TPM (3), the use of session-bound,  
4 short-lived media URLs. Because these URLs expire and cannot be reused, automated tools must  
5 repeatedly obtain fresh authorization parameters and regenerate valid links in order to continue  
6 downloading. By programmatically renewing access credentials outside ordinary playback  
7 sessions, Defendant maintained uninterrupted access to files that would otherwise become  
8 unavailable once the original authorization lapsed.

9           101.    At scale, Defendant’s automated activity would also trigger TPM (4), CAPTCHA  
10 challenges intended to distinguish human users from automated systems. To continue retrieving  
11 videos without interruption, Defendant’s infrastructure distributed requests across numerous  
12 machines and operated in a manner designed to avoid or neutralize such verification barriers,  
13 thereby obtaining audiovisual data without the human interaction required for continued access.

14           102.    Defendant further circumvented TPM (5), YouTube’s proof-of-origin token system,  
15 which requires requests for video segments to present credentials demonstrating that they originate  
16 from an authorized playback environment. Automated downloading tools operate outside that  
17 environment and therefore must extract, replicate, or reuse the necessary request parameters in  
18 order to retrieve video data directly, allowing Defendant to access and obtain files that would  
19 otherwise be delivered only to approved clients.

20           103.    Defendant did not obtain the consent of YouTube, Plaintiffs or other Class Members  
21 to conduct its scraping activities.

22           104.    The automated system used by Defendant to access video content from YouTube  
23 was intentionally designed and utilized to circumvent YouTube’s TPMs.

24           105.    To be clear, Defendant’s generative AI models are not “watching” YouTube in order  
25 to be trained. Rather, data improperly accessed and downloaded from YouTube is being uploaded  
26 into Defendant’s generative AI models to develop and improve Defendant’s products.

27           106.    Defendant knew or should have known its conduct violated YouTube’s TPMs.  
28

1           107. Defendant’s actions constitute a violation of the DMCA’s anti-circumvention  
2 provisions, which state, among other things, that “[n]o person shall circumvent a technological  
3 measure that effectively controls access to a work protected under this title.” 17 U.S.C. §  
4 1201(a)(1)(a).

5           E.       **Defendant’s Actions Caused Harm to Plaintiffs and Class Members**

6           108. At no time did Defendant seek or obtain Plaintiffs’ or Class Members’ authorization  
7 to access and use the videos Defendant used to train its generative AI models.

8           109. At no time did Defendant seek or obtain Plaintiffs’ or Class Members’ authorization,  
9 nor did Defendant compensate Plaintiffs or the Class Members for the access, copying, ingestion,  
10 and use of their YouTube videos in AI training and related workflows.

11           110. Plaintiffs and Class Members used YouTube as their platform of choice to upload  
12 their video content in substantial part due to YouTube’s protective measures, including TPMs and  
13 Terms of Service, that prohibit the type of scraping, unauthorized accessing and downloading, bulk  
14 extraction, and other forms of data mining of audiovisual content utilized by Defendant to obtain  
15 Plaintiffs’ video content.

16           111. The harm Defendant is causing goes beyond the immediate economic consequences  
17 of unauthorized and uncompensated extraction and use of Plaintiffs’ and Class Members’ works. It  
18 degrades the rights of creators to control their works, determine whether future uses of their work  
19 align with their values, and decide the products or services with which they wish to be associated.

20           112. Defendant’s conduct also caused concrete harm to the licensing market for  
21 Plaintiffs’ and Class Members’ content. The market for licensing video content to AI training  
22 pipelines is an emerging and recognized market. By obtaining Plaintiffs’ content through  
23 circumvention rather than licensing, Defendant deprived Plaintiffs of licensing fees they could have  
24 negotiated and suppressed the development of that market by establishing a pattern of unauthorized  
25 extraction as an alternative to licensing.

26           113. As a direct and proximate result of Defendants' circumvention, Plaintiff has suffered  
27 actual damages, including loss of control over his copyrighted works, impairment of market value,  
28 and costs incurred to identify, remove, and prevent further distribution of the infringing content.

1 This harm to the value and market for Plaintiffs' works constitutes a concrete, non-speculative  
2 injury sufficient to establish Article III standing independent of any statutory damages.

### 3 CLASS ACTION ALLEGATIONS

4 114. **Class Definition:** Plaintiffs bring this action on behalf of themselves and other  
5 similarly situated individuals defined as follows:

6 All persons and entities in the United States who are creators and/or rights-holders  
7 of YouTube-hosted videos that Apple accessed at the file level by scraping,  
8 downloading, or otherwise extracting underlying video files from YouTube through  
circumvention of YouTube's TPMs (the "Class").

9 115. The "Class Period" is the period beginning on the date established by the Court's  
10 determination of any applicable statute of limitations, after consideration of any tolling,  
11 concealment, and accrual issues, and ending on the date of entry of judgement or preliminary  
12 approval of a settlement.

13 116. Excluded from the Class are Defendant; any affiliate, parent, or subsidiary of  
14 Defendant; any entity in which Defendant has a controlling interest; any officer director, or  
15 employee of Defendant; any successor or assign of Defendant; anyone employed by counsel in this  
16 action; any judge to whom this case is assigned, his or her spouse and immediate family members;  
17 and members of the judge's staff.

18 117. Plaintiff reserves the right to modify the class definitions or add sub-classes as  
19 needed prior to filing a motion for class certification.

20 118. The proposed Class meets the criteria for certification under Rule 23 of the Federal  
21 Rules of Civil Procedure.

22 119. Numerosity. The Members of the Class are so numerous that joinder of all of them  
23 is impracticable. The exact number of Class Members is unknown to Plaintiffs now, but Plaintiffs  
24 estimates that there are thousands of Class Members.

25 120. Commonality. Questions of law and fact common to the Class Members  
26 predominate over questions that may affect only individual Class Members because Defendant has  
27 acted on grounds generally applicable to the Class. Such generally applicable conduct is inherent  
28 in Defendant's wrongful conduct. The following questions of law and fact are common to the

1 Class:

- 2 a. Whether YouTube employs TPMs “that effectively control access” to  
3 copyrighted audiovisual works within the meaning of 17 U.S.C. § 1201(a);
- 4 b. Whether Defendant’s defeated, avoided, bypassed, removed, deactivated,  
5 impaired, or otherwise circumvented YouTube’s TPMs, including through  
6 automated tools used to download or otherwise obtain unauthorized access to  
7 the Plaintiffs’ and Class Members’ copyrighted content on YouTube;
- 8 c. Whether Apple’s circumvention and/or trafficking conduct was willful,  
9 knowing, and undertaken for commercial advantage or private financial gain;
- 10 d. Whether Defendant retrieved, scraped, downloaded, or otherwise acquired the  
11 underlying YouTube videos referenced in Panda-70M and any other datasets  
12 used by Apple at massive scale to build training material for its AI systems;
- 13 e. Whether Plaintiffs and Class Members suffered damages from Defendant’s  
14 misconduct.

15 121. Typicality. Plaintiffs’ claims are typical of those of other Class Members because  
16 Plaintiffs’ video content, like that of every other Class Member, was made available on YouTube  
17 and improperly altered and used by Defendant to train Defendant’s generative AI models for  
18 commercial purposes. Plaintiffs’ claims are typical of those of the other Class Members because,  
19 among other things, all Class Members were injured through the common misconduct of  
20 Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and  
21 all other Class Members, and no defenses are unique to Plaintiffs. Plaintiffs’ claims and those of  
22 Class Members arise from the same operative facts and are based on the same legal theories.

23 122. Adequacy of Representation. Plaintiffs will fairly and adequately represent and  
24 protect the interests of the Members of the Class. Plaintiff’s interests coincide with, and not  
25 antagonistic to, those of the Class Members. Plaintiff is represented by attorneys with experience  
26 in the prosecution of class action litigation. Plaintiff’s attorneys are committed to vigorously  
27 prosecuting this action on behalf of the Class Members.

28 123. Predominance. Defendant has engaged in a common course of conduct toward

1 Plaintiffs and Class Members, in that Plaintiffs' and Class Members' video content was unlawfully  
2 downloaded, altered and used by Defendant in the same way. The fact that Apple AI Video was a  
3 foundational model underscores that Defendant's conduct was uniform across the Class: every  
4 video unlawfully accessed from YouTube was ingested into the same core model that underpins  
5 Defendant's product ecosystem. This commonality further demonstrates the predominance of  
6 shared legal and factual issues among Class Members. The common issues arising from  
7 Defendant's conduct affecting Class Members set out above predominate over any individualized  
8 issues. Adjudication of these common issues in a single action has important and desirable  
9 advantages of judicial economy.

10 124. Superiority. A Class action is superior to other available methods for the fair and  
11 efficient adjudication of the controversy. Class treatment of common questions of law and fact is  
12 superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class  
13 Members would likely find that the cost of litigating their individual claims is prohibitively high  
14 and would therefore have no effective remedy. The prosecution of separate actions by individual  
15 Class Members would create a risk of inconsistent or varying adjudications with respect to  
16 individual Class Members, which would establish incompatible standards of conduct for  
17 Defendant. In contrast, the conduct of this action as a class action presents far fewer management  
18 difficulties, conserves judicial resources and the parties' resources, and protects the rights of each  
19 Class member.

20 125. Defendant has acted on grounds that apply generally to the Class as a whole, so that  
21 class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-  
22 wide basis.

23 126. Ascertainability. Finally, all members of the proposed Class are readily  
24 ascertainable. Defendant used datasets that contain the full lists of URLs and video identifiers for  
25 every YouTube video incorporated into the training pipeline. Those identifiers allow the parties to  
26 determine exactly which videos were used and to match each video to its creator through  
27 YouTube's public channel and authorship information. Because the datasets provide a complete  
28 map of the videos Defendant downloaded, the identities of the affected creators are identifiable

1 through straightforward reference to the URLs and corresponding channel data.

2 **CLAIM FOR RELIEF**

3 **Violation of the DMCA (Anti-Circumvention) 17 U.S.C. § 1201(a)**

4 127. Plaintiffs repeat, reallege, and incorporates the allegations contained in the previous  
5 paragraphs as if fully set forth herein.

6 128. Plaintiffs are owners of valid copyrights in audiovisual works distributed through  
7 the YouTube platform. Plaintiffs and Class Members own all rights, title, and interest in and to the  
8 claims asserted in this action, including all claims for violation of 17 U.S.C. § 1201.

9 129. YouTube employs TPMs that effectively control access to Plaintiffs' and Class  
10 Members' copyrighted works within the meaning of 17 U.S.C. § 1201(a)(3)(B). YouTube's TPMs  
11 prohibit scraping, unauthorized downloading, bulk extraction, or other forms of data mining of  
12 audiovisual content.

13 130. These TPMs require the application of information, processes, and authorized  
14 interactions in order to access the audiovisual works in usable form. These measures function to  
15 prevent access to Plaintiffs' works outside YouTube's authorized delivery environment. These  
16 restrictions prevent unlicensed access to the underlying video files, not simply reproduction of  
17 content.

18 131. When each of Plaintiffs' and Class Members works were published to YouTube,  
19 YouTube automatically applied TPMs that control access to and prevent unauthorized access to  
20 these audiovisual files.

21 132. Defendant knowingly and intentionally circumvented YouTube's TPMs by  
22 deploying automated systems designed to avoid, bypass, and impair those TPMs.

23 133. Defendant used automated tools for the sole purpose of circumventing YouTube's  
24 technological barriers that effectively control access to extracted files never made available to the  
25 public. Specifically, Defendant employed measures to access, extract, copy, and download  
26 Plaintiffs' and Class Members' content from YouTube without authorization. In doing so,  
27 Defendant improperly obtained millions of videos from YouTube's platform.

28 134. Defendant's conduct constitutes circumvention because it involved the avoidance

1 and bypassing of technological measures that control access to copyrighted works, without the  
2 authority of Plaintiffs or the Class Members (i.e., the copyright owners).

3 135. This distinction is critical: viewing a YouTube video through YouTube's authorized  
4 and playback mechanisms does not provide access to the underlying file. Defendant's  
5 circumvention tools broke through that access barrier, triggering liability under §1201.

6 136. As a direct and proximate result of Defendant's violations, Plaintiffs have been  
7 injured and are entitled to all remedies available under 17 U.S.C. § 1203, including statutory  
8 damages, injunctive relief, and attorneys' fees.

9 137. Plaintiffs and Class Members have been harmed by Defendant's conduct because  
10 Defendant has taken their content without authorization or compensation. Defendant's  
11 circumvention of YouTube's technological measures has facilitated Defendant's ongoing and  
12 mass-scale copyright infringement through its unauthorized and uncompensated use of the content  
13 in its training data. Defendant accessed, downloaded, stored and utilized those videos to assemble  
14 training corpora for Defendant's AI models and services.

15 138. Each act of circumvention constitutes a separate violation of §1201. Plaintiffs and  
16 the Class Members are entitled to statutory damages, injunctive relief, impoundment, and attorneys'  
17 fees and costs under 17 U.S.C. §1203.

18 139. Each of Defendant's acts of infringement is a willful violation as Defendant  
19 specifically utilized automated tools designed to evade YouTube's TPMs.

20 **PRAYER FOR RELIEF**

21 WHEREFORE, Plaintiffs respectfully request a judgment in their favor and against  
22 Defendant as follows:

- 23 a. Certification of this action as a class action and appointment of Plaintiffs and  
24 Plaintiffs' counsel to represent the Class;
- 25 b. Declare that Defendant has willfully circumvented the copyright protection  
26 systems of YouTube intended to protect Plaintiffs' and the Class Members's  
27 audiovisual content.
- 28 c. For statutory damages (up to the maximum allowed by law per violation),

1 injunctive relief, and attorneys' fees and costs under 17 U.S.C. §1203;

- 2 d. For such equitable relief under Title 17, Title 28, and/or the Court's inherent  
3 authority as is necessary to prevent or restrain infringement of Plaintiffs' and the  
4 Class Members' copyright-protected content, including a preliminary and  
5 permanent injunction requiring that Defendant and its officers, agents, servants,  
6 employees, attorneys, directors, successors, assigns, licensees, and all others in  
7 active concert or participation with any of them, cease infringing, or causing,  
8 aiding, enabling, facilitating, encouraging, promoting, inducing, or materially  
9 contributing to or participating in the infringement of any of Plaintiff's or the  
10 Class Members' exclusive rights under federal law, including without limitation  
11 in the content identified in Exhibits A, B, and C;
- 12 e. For an award of pre-judgment and post-judgment interest, to the fullest extent  
13 available, on any monetary award made part of the judgment against Defendant;  
14 and
- 15 f. For such other and further relief as the Court may deem just and proper.

16 **JURY DEMAND**

17 140. Plaintiffs demand a trial by jury on all claims for which trial by jury is proper.  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Dated: April 3, 2026

Respectfully submitted,

/s/ Rom Bar-Nissim  
Rom Bar-Nissim (SBN 293356)  
**HEAH BAR-NISSIM LLP**  
1801 Century Park East, Suite 2400  
Los Angeles, CA 90067  
Tel: (310) 432-2836  
Rom@HeahBarNissim.com

Jarrett Lee Ellzey (*pro hac vice*)  
Tom Kherkher (*pro hac vice*)  
Leigh S. Montgomery (*pro hac vice*)  
**ELLZEY KHERKHER SANFORD  
MONTGOMERY LLP**  
4200 Montrose Street, Suite 200  
Houston, TX 77006  
Jellzey@EKSM.com  
TKherkher@EKSM.com  
LMontgomery@EKSM.com

---

*Attorneys for Plaintiffs and the Proposed  
Class*