AIPLA QUARTERLY JOURNAL

Volume 53, Number 4 Page 529 Fall 2025

DMC-AI:
AN ANTIVENOM

*Wade Witcher**

 I would like to thank Professor John Dzienkowski of The University of Texas School of Law and Professor Matthew Murrell of the University of New Mexico School of Law for their invaluable guidance and mentorship in preparing this Article. All viewpoints in this Article are entirely my own and do not reflect the viewpoints of any past, current, or future employer.

LIST OF FIGURES

I. INTRODUCTION: COPYRIGHT AT THE KNIFE'S EDGE OF AI

Venom: a toxic substance produced by some animals (e.g., snakes, scorpions, or bees) that is injected into prey or an adversary chiefly by biting or stinging and has an injurious or lethal effect.[1]

Artificial Intelligence (AI) has not killed copyright. Yet. However, there is concern that it may eviscerate copyright protection in the United States.[2]

Antivenom: an antitoxin to a venom.[3]

As scholars have warned, copyright may be snake-bit by AI.[4] However, as this Article will demonstrate, the cure is the poison. AI represents a mortal threat and a hopeful savior for copyright protection in the digital age. Like snake venom,

---

1 *Venom*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/venom [https://perma.cc/M8PU-GTN7].

2 *See, e.g.*, Louis Menand, *Is A.I. the Death of I.P.?*, NEW YORKER (Jan. 15, 2024), https://www.newyorker.com/magazine/2024/01/22/who-owns-this-sentence-a-history-of-copyrights-and-wrongs-david-bellos-alexandre-montagu-book-review [https://perma.cc/R998-32UM] ("Whatever happens, the existential threats of AI will not be addressed by copyright law."); David Shapiro, *AI: Copyright is Dying a Slow Death*, MEDIUM (Sep. 21, 2023), https://medium.com/@dave-shap/ai-copyright-is-dying-a-slow-death-934d9f9c3449 [https://perma.cc/96LE-6JLG] ("AI generated works are not applicable to copyright protection requirements.").

3 *Antivenom*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/antivenom [https://perma.cc/HP6F-GB9B]; *Antivenin*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/antivenin [https://perma.cc/B7ET-63NQ]; *Antitoxin*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/antitoxin [https://perma.cc/J8ZE-RP53] (defining antivenom as "an antibody that is capable of neutralizing the specific toxin (such as a specific causative agent of disease) that stimulated its production in the body and is produced in animals for medical purposes by injection of a toxin or toxoid with the resulting serum being used to counteract the toxin in other individuals").

4 Benjamin L. W. Sobel, *Artificial Intelligence's Fair Use Crisis*, 41 COLUM. J.L. & ARTS 45, 97 (2017) ("Machine learning technology empowers these companies to extract value from authors' protected expression without authorization, and to use that value for commercial purposes that may someday jeopardize the livelihoods of human creators. Construing fair use to protect this activity will place the doctrine at odds with the public interest and potentially exacerbate the social inequalities that Al threatens. At the same time, finding that expressive machine learning is not fair use would frustrate the progress of the promising technology.").

which can kill but also becomes essential in developing lifesaving antivenom, AI simultaneously endangers intellectual property rights while offering powerful mechanisms to protect them.

Snake venom's deadly properties were once attributed to supernatural forces until scientists discovered its biological mechanisms. Until the seventeenth century, the prevailing rationale for this morbidity was the "bad spirits" within snakes.[5] Francesco Redi found that the poison was not mystical or supernatural but a property of the liquid released from the viper's fangs.[6] Two centuries later, Henry Sewall discovered that non-lethal doses of rattlesnake venom repeatedly introduced to pigeons built up the birds' immunity to the poison.[7] Dr. Albert Calmette built on this work by developing a serum in rabbits to combat cobra venom.[8] This research laid the foundation for the antivenom production process we know today, where horses are inoculated with a non-lethal, non-damaging amount of snake venom to develop antivenom.[9] The horse's immune system then binds to the venom to create antibodies, which are removed from the horse and purified to produce an intravenous antidote for human use.[10]

Society does not have centuries to combat AI's venom in the copyright system. Unlike snakes, AI's potency grows year-to-year. However, we must learn from the development of snake antivenom that our perils are not paranormal but scientific.[11] Modern AI is a powerful tool, but it is not SkyNet.[12] The same features

---

5 Gerhard G. Habermehl, *Francesco Redi—Life and Work*, 32 TOXICON 411, 415–16 (1994) ("It is hardly believable for us today, but conceivable if one considers the way of thinking in those times, that the Archbishop of Madrid exorcized the venom from all snakes of Spain.").

6 *See id.* at 416.

7 *See* Henry Sewall, *Experiments on the Preventive Inoculation of Rattlesnake Venom*, 8 J. PHYSIOLOGY 203, 208–10 (1887).

8 *See* Carla Cristina Squaiella-Baptistao et al., *The History of Antivenoms Development: Beyond Calmette and Vital Brazil*, 150 TOXICON 86, 87 (2018).

9 *See* Mauricio Arguedas et al., *Comparison of Adjuvant Emulsions for Their Safety and Ability to Enhance the Antibody Response in Horses Immunized with African Snake Venoms*, VACCINE: X, Dec. 2022, at 1, 1.

10 *See, e.g.*, *id.*; Squaiella-Baptistao et al., *supra* note 8, at 91.

11 Henry H. Perritt, Jr., *Undressing AI: Transparency Through Patents*, 33 TEX. INTELL. PROP. L.J. 137, n.74 (2025) ("The press . . . has consistently stoked public hysteria over new technologies, starting with the power loom and the spinning Jenny.").

12 Craig S. Smith, *China's Autonomous Agent, Manus Changes Everything*, FORBES (Mar. 8, 2025), https://www.forbes.com/sites/craigsmih/2025/03/08/chinas-

that make AI a dangerous lone or secondary infringer are also the exact features that make it a powerful antidote for infringement.

This Article outlines the first step in protecting copyrights on social media in the AI era. Corporate actors utilizing AI for profit must also be obligated to use AI to enforce the private rights of copyright holders.[13] Part II of this Article will begin by discussing the safe harbor for social media websites under the Digital Millennium Copyright Act (DMCA). Part III will continue by describing how AI is used on modern social media sites to curate user content. Further, Part IV will discuss how some prominent social media websites have shown the capability to remove or moderate content in recent years, and close by arguing for a rebalancing of the DMCA for social media sites that utilize AI in content curation and moderation.

Part V advocates for the modernization of digital copyright law in the current AI era. Social media companies that deploy AI tools to curate content for their users and enhance the consumer experience can efficiently utilize AI to detect and remove content that violates existing registered copyrights. Although AI may represent the greatest threat to copyright since the advent of the Internet, it can and should serve as an extraordinary tool to strengthen copyright protections in the years ahead.

II. THE DMCA'S FAILING FRAMEWORK: A LAW FROZEN IN THE ANALOG AGE

The Digital Millennium Copyright Act (DMCA), enacted on October 28, 1998, represented America's implementation of the World Intellectual Property Organization (WIPO) Copyright Treaty and the WIPO Performances and Phonogram Treaty.[14] The WIPO Copyright Treaty aimed to protect the exclusive rights of literary and artistic authors to publish and copy their original works internationally while carving out exceptions for "education, research, and access

---

autonomous-agent-manus-changes-everything/ [https://perma.cc/RR49-859Z] ("It is the world's first fully autonomous AI agent, a system that doesn't just assist humans-it replaces them.").

[13] THE FEDERALIST NO. 43 (James Madison) ("The utility of this power will scarcely be questioned. The copyright of authors has been solemnly adjudged, in Great Britain, to be a right of common law…the public good fully coincides in both cases with the claims of [authors]."); U.S. CONST. art. I, § 8, cl. 8 ("Promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.").

[14] *See* Statement on Signing the Digital Millennium Copyright Act (DMCA), 1998 PUB. PAPERS 1902, 1902 (Oct. 28, 1998).

to information."[15] This treaty emerged as an aspirational safeguard for authors' rights during the Internet's nascent stages.[16] As the Senate articulated, "The '[DMCA] of 1998' is designed to facilitate the robust development and worldwide expansion of electronic commerce, communications, research, development, and education in the digital age."[17] This legislation attempted to balance two competing interests—protecting copyright holders and nurturing the fledgling digital economy—a tension that would grow increasingly problematic as technology evolved far beyond what lawmakers could have envisioned at the dawn of the Internet era.

A. FROM PUBLIC ACCESS TO PRIVATE PROFIT: THE EVOLUTION OF CLINTON'S VISION

By attempting to balance the digital innovation of the 1990s with a Constitutional commitment to protect intellectual property, the DMCA was the most consequential intellectual property law at the turn of the century. Concerns about digital piracy intensified as electronic commerce skyrocketed.[18] Even so, Congress was committed to discovering the Internet's commercial potential.[19] This tension between protection and innovation would later prove problematic in ways the original drafters could never have anticipated in the pre-social media, pre-AI era.

The DMCA's provisions originated with President Clinton's formation of the Information Infrastructure Task Force (IITF) in February 1993,[20] a forward-thinking initiative charged with "articulat[ing] and implement[ing] the Administration's vision for the National Information Infrastructure (NII)."[21] The

---

15 WIPO Copyright Treaty art. 6, Dec. 20, 1996, S. TREATY DOC. NO. 105-17, 2186 U.N.T.S. 121, 153.

16 *See* S. REP. NO. 105-190, at 8 (1998).

17 *Id.* at 1–2.

18 *See* H.R. REP. NO. 105-551, pt. 2, at 23 (1998).

19 *See, e.g.*, S. REP. NO. 105-190, at 69; 17 U.S.C. § 109; David Nimmer, *A Riff on Fair Use in the Digital Millennium Copyright Act*, 148 U. PA. L. REV. 673, 683 (2000).

20 *See* S. REP. NO. 105-190, at 2.

21 Bruce A. Lehman, *The Report of the Working Group on Intellectual Property Rights*, *in* INTELLECTUAL PROPERTY AND THE NATONAL INFORMATION INFRASTRUCTURE 1 (1995) [hereinafter "White Paper"]. President Clinton's task force did not fully share Congress's concern that strong IP rights would hurt

Task Force's September 1995 report, commonly referred to as the "White Paper," urged Congress to modernize copyright laws for the digital age.[22] The White Paper sought to balance copyright protection with expanded exemptions for educational, library, and public health purposes[23]—an approach that economic interests would later overtake.[24]

Title I of the DMCA implemented the WIPO treaties to ensure copyrights remained protected and commercially viable in the online environment.[25] Congress prohibited the use of specific technological circumvention devices designed to bypass copyright protection measures, thereby strengthening digital copyright protection.[26] However, mere circumvention capability was insufficient for liability; the device's primary purpose had to be circumventing copyright protections.[27] Section 1204 established significant penalties—up to $1 million in fines and/or 10 years imprisonment—for those attempting to circumvent these protections.[28]

Although Title I reflected some of the White Paper's recommendations and America's WIPO treaty obligations,[29] the evolution from Clinton's original vision to the final legislation was significant.[30] What began as an initiative to embrace public access through the National Information Infrastructure became a

---

the economy, noting that piracy could cost the U.S. economy "$15 to 17 billion annually." *Id.* at 131.

22 *Id.* at 212; *see also* S. REP. NO. 105-190, at 2.

23 White Paper, *supra* note 21, at 9, 225–27. Although the DMCA focused on balancing copyright protection and cultivating electronic commerce, the recommendations in the White Paper were more concerned with expanding access to copyrighted content to the public. *Id.* at 11–13.

24 Christopher A. Cotropia & James Gibson, *Convergence and Conflation in Online Copyright*, 105 IOWA L. REV. 1027, 1037–38 (2020).

25 S. REP. NO. 105-190, at 2.

26 *Id.* at 12; *see also,* 17 U.S.C. § 1201.

27 *See, e.g.*, S. REP. NO. 105-190, at 13; H.R. REP. NO. 105-551, pt. 1, at 10; 17 U.S.C. § 1201.

28 *See* H.R. REP. NO. 105-551, at 14; 17 U.S.C. § 1204.

29 *See* S. REP. NO. 105-190, at 66–67.

30 *See generally* 17 U.S.C. § 512.

law primarily concerned with protecting electronic commerce[31]—a transformation that would have profound implications for today's AI-driven content landscape.

B. SAFE HARBOR OR LEGAL SHIELD? HOW COURTS EXPANDED PLATFORM IMMUNITY

Although the DMCA attempted to strengthen online protection for copyright holders, § 512 simultaneously ensured this protection would not stifle the Internet's burgeoning growth. The safe harbor provisions of 17 U.S.C. § 512 provided four categories of activity that would be immune from liability for service providers and protection for nonprofit and educational services.[32] These safe harbor provisions were driven by a fundamental desire to shield websites from copyright liability for their users' activities.[33] Granted, economic shields made more sense in an era when websites functioned like passive bulletin boards rather than sophisticated, AI-powered content curators.[34]

The DMCA's safe harbors responded directly to the courts' increasingly broad interpretation of the 1976 Copyright Act. Before the DMCA, courts routinely held websites vicariously or contributorily liable for the copyright infringement of their users.[35] In *Columbia Pictures Industries v. Aveco, Inc.*, the Third Circuit ruled that even a video rental company allowing customers to use private viewing rooms violated copyright holders' exclusive display rights.[36] Customers physically inserted the cassettes, but the rental store remained liable for providing the facilities that enabled infringement.[37] This precedent expanded when the Ninth Circuit in *Fonovisa, Inc. v. Cherry Auction, Inc.* held swap meet[38] hosts liable for

---

31 *See* Cotropia & Gibson, *supra* note 24, at 1037–47.

32 *See id.* at 1038.

33 *See id.* at 1039.

34 *See id.* at 1030–31 (describing early social media websites as "a vast electronic message board" and "a small electronic bulletin board service").

35 *See, e.g.*, S. REP. NO. 105-190, at 19 (citing Religious Tech. Ctr. v. Netcom On-Line Commc'ns Servs., Inc., 907 F. Supp. 1361, 1361 (N.D. Cal. 1995); Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1552 (M.D. Fla. 1993); Marobie-FL, Inc. v. Nat'l Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, 1167 (N.D. Ill. 1997)).

36 *See* Columbia Pictures Indus., Inc. v. Aveco, Inc., 800 F.2d 59, 64 (3d Cir. 1986).

37 *See id.* at 62.

38 Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 261 (9th Cir. 1996) (A swap meet is an event "where customers come to purchase various merchandise

contributory copyright infringement merely for "providing the site and facilities for known infringing activity."[39] These physical-world rulings laid the groundwork for the Northern District of California's decision in *Sega Enterprises v. Maphia*,[40] where an electronic bulletin board operator faced liability when users uploaded copyrighted material that others could download.[41] Citing *Fonovisa*, the court deemed the bulletin board "a central depository site for unauthorized games" that "allowed subsequent distribution of the games by user downloads."[42] Simply providing "facilities," even online, established a sufficient affirmative act to be liable for contributory infringement.[43] The Ninth Circuit's approach spread to other district courts using similar theories.[44]

Congress feared these expansive precedents would chill electronic commerce investment, prompting § 512's safe harbor provisions. If online platforms had considered their potential liability, they may have hesitated to invest in improving the "speed and capacity of the Internet."[45] However, if platforms had complete immunity, authors may refrain from publishing content

---

from individual vendors" and the "vendors pay a daily rental fee to the swap meet operators in exchange for booth space.").

39 *Id.* at 264.

40 Sega Enters. Ltd. v. MAPHIA, 948 F. Supp. 923, 936 (N.D. Cal. 1996).

41 *Id.* at 927.

42 *Id.* at 933.

43 *Id.* (stating the operator would still have been liable even under a "higher standard of 'substantial participation'").

44 *See, e.g.*, Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503, 514 (N.D. Ohio 1997) (holding electronic bulletin board operators liable for contributory copyright infringement for having "at least constructive knowledge that infringing activity was likely" occurring on their website); *Marobie-FL*, 983 F. Supp. at 1173–74 (holding web page owner liable for allowing copyrighted material to be available to download by end users and denying summary judgment for the host computer for genuine issues of material fact on their knowledge of the copyrighted material present on the web page); Playboy Enters., Inc. v. Webbworld, Inc., 968 F. Supp. 1171, 1175 (N.D. Tex. 1997) (holding website operator liable for copyright infringement for providing a web page where users uploaded elicit copyrighted photos and other users downloaded these photos) ("Even the absence of the ability to exercise such control [over what images are posted on the website], however, is no defense to liability.").

45 S. REP. NO. 105-190, at 8.

online, diminishing the Internet's informational value.[46] This tension drove negotiations between Congress, copyright owners, and Internet service providers,[47] resulting in a compromise that now appears increasingly one-sided in the AI era: service providers would avoid liability if they had no reason to suspect users were uploading infringing content; in exchange, once notified by copyright owners, service providers would remove the infringing material and provide identifying information on the infringer.[48]

This compromise, codified in 17 U.S.C. § 512, protected five categories of online service providers: (1) providers that transmit data between users, mere conduits of data transmission,[49] (2) caching systems (temporary storage of data on a network),[50] (3) online storage systems where end-users upload data,[51] (4) online data indexing services,[52] and (5) public or nonprofit education providers.[53] To qualify for the safe harbor protections, these five groups must adopt and publish a policy to terminate users who repeatedly use their services to infringe copyrights and allow copyright owners to utilize "standard technical measures" that "identify or protect copyrighted works."[54] The safe harbors in § 512(a) protect

---

46 *See* Mike Scott, *Safe Harbors Under the Digital Millenium Copyright Act*, 9 LEG. & PUB. POLICY 99, 99–100 (2005) ("On the one hand, there was concern that the 'online service providers' (OSPs) that were providing the new technology might become so fearful of incurring liability that they would be reluctant to invest…on the other, there was the danger that copyright holders would refuse to make works available online at all.").

47 Jessica Litman, *Digital Copyright, in* UNIVERSITY OF MICHIGAN LAW SCHOOL SCHOLARSHIP REPOSITORY 134–36 (2006) ("The more that user interests pressed for some limitations on the copyright owners' control of access, the more adamant content lobbyists became that any limitation would be unfair and intolerable.").

48 *Id.* at 135 ("Content owners agreed that Internet service providers should not be liable for their subscribers' infringing transmissions so long as the provider had no reason to suspect infringement was taking place… . Service providers agreed to turn identifying information about accused copyright violators over to complaining copyright holders.").

49 17 U.S.C. § 512.

50 *Id.*

51 *Id.*

52 *Id.*

53 *Id.*

54 *Id.*

Internet service providers from liability for "transmitting, routing, or providing connections, if[:]" (1) the end-user initiated the transmission, (2) the transmission is carried out automatically without direction from the service provider, (3) the service provider does not select the recipient, (4) no copy of the infringing content is maintained on the system ordinarily accessible to the service provider or recipient longer than is needed for the transmission, and (5) the infringing content is transmitted without modifying the contents.[55] Section 512(a) protects providers acting as mere data transmission conduits.[56]

Outside of § 512(a), the other four types of online service providers must comply with § 512(c)(3) notice and takedown procedures at the behest of copyright owners to utilize the safe harbor.[57] Under § 512(c), service providers are not held liable if they do not have actual knowledge of the infringing material on their systems, are "not aware of facts or circumstances" of apparent infringing activity, or, after gaining the requisite knowledge, act "expeditiously to remove, or disable access to," the infringing material.[58] Further, if the provider "has the right and ability to control [infringing] activity," the provider cannot financially benefit from the activity.[59] If the copyright owner notifies the provider under § 512(c)(3) of the infringement, the provider must "expeditiously [] remove, or disable access to" the infringing content.[60]

The responsibility of the copyright owner is equally onerous. For the copyright owner's notice to be adequate to mandate a safe harbor takedown, it must comply with six provisions under § 512(c)(3).[61] Service providers that do not

---

55 17 U.S.C. § 512; Digital Millennium Copyright Act (DMCA), Pub. L. No. 105-304, § 202, 112 Stat. 2860, 2877–78 (1998) [hereinafter DMCA].

56 *See* Matthew Sag, *Internet Safe Harbors and the Transformation of Copyright Law*, 93 NOTRE DAME L. REV. 499, 512 (2018).

57 Scott, *supra* note 46, at 120 (explaining that if a party does not fall into the categories listed in § 512(a), then service providers must comply with § 512(c)(3) notice and takedown procedures should they wish to utilize the safe harbor).

58 17 U.S.C. § 512.

59 *Id.*

60 *Id.*

61 *Id.* Notably, (1) the signature of the owner or authorized agent of the copyright, (2) identification of the copyrighted work, (3) identification of the infringing work with "information reasonably sufficient" to locate the infringing work, (4) contact information for the copyright owner or agent "such as an address, telephone number, and, if available, an" e-mail address, (5) statement of good faith belief the infringing material is not authorized, and

adhere to this notice and takedown procedure cannot claim the safe harbor under § 512(c), and copyright owners that fail to notify in accordance with § 512(c)(3) cannot avoid service provider immunity in enforcing their exclusive rights.[62]

Post-DMCA, the lighthouse went dark; the harbor was safe—perhaps too safe. Courts consistently applied the DMCA to provide greater immunity than providers enjoyed before 1998, as exemplified by *Viacom International, Inc. v. YouTube, Inc*.[63] When YouTube received summary judgment under § 512(c) against direct and contributory infringement claims,[64] the Second Circuit vacated and remanded,[65] noting that "actual knowledge or awareness of facts or circumstances that indicate specific and identifiable instances of infringement" would disqualify a service provider from safe harbor protection.[66] Yet, on remand, the Southern District of New York again granted YouTube summary judgment.[67]

The copyright owner argued that YouTube needed to prove a lack of knowledge regarding 63,060 copyrighted clips to qualify for safe harbor[68]—an argument that the court dismissed as "ingenious, but . . . an anachronistic, pre-[DMCA] concept."[69] With "more than 24 hours of new video" uploaded to YouTube per minute,[70] the court reasoned that "no service provider could possibly

(6) statement the information provided "is accurate, and under penalty of perjury, that the" complainant is authorized to act for the copyright owner. *Id.*

62 *See* H.R. REP. NO. 105-551, pt. 2, at 54–55.

63 *See* Viacom Int'l, Inc. v. YouTube, Inc., 940 F. Supp. 2d 110 (S.D.N.Y. 2013) [hereinafter *2013 Viacom Int'l*].

64 *See* Viacom Int'l, Inc. v. YouTube, Inc., 718 F. Supp. 2d 514, 529 (S.D.N.Y. 2010) [hereinafter *2010 Viacom Int'l*].

65 *See* Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 41-42 (2d Cir. 2012) [hereinafter *2d Cir. Viacom Int'l*].

66 *Id.* at 32, 34; *contra* Sega Enters. Ltd. v. MAPHIA, 948 F. Supp. 923, 933 (N.D. Cal. 1996) ("[P]roviding the site and facilities for known infringing activity is sufficient to establish contributory liability." (quoting Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996))).

67 *2013 Viacom Int'l*, 940 F. Supp. 2d at 123.

68 *Id.* at 113–14. Notably, the plaintiff claimed that YouTube had actual knowledge of user-posted material that infringed the plaintiff's copyrights but not the copyrights in the suit. *See 2d Cir. Viacom Int'l*, 676 F.3d at 33.

69 *2013 Viacom Int'l*, 940 F. Supp. 2d at 114.

70 *Id.* (quoting *2010 Viacom Int'l*, 718 F. Supp. 2d at 518; *2d Cir. Viacom Int'l*, 676 F.3d at 28).

be aware of the contents of each such video," and Congress established the DMCA safe harbor for these types of cases.[71] Thus, the DMCA "places the *burden of notifying* such service providers of infringements *upon the copyright owner*."[72] Other courts similarly shifted the burden to copyright owners,[73] imposing substantial procedural hurdles to protect their exclusive rights because of service providers' technical limitations—limitations from *three decades ago* that bear little resemblance to today's AI-powered content recognition capabilities.

C. THE BROKEN BARGAIN: HOW 1998 ASSUMPTIONS FAILED COPYRIGHT OWNERS

This Article does not seek to judge a 1998 technology-laden law by 2025 standards. However, to determine if the DMCA's justifications remain valid almost three decades later,[74] the Article must examine the original rationales for

---

[71] *Id.* However, the plaintiff alleged YouTube could readily locate infringing material with in-house identification tools. The court did not deny YouTube had this capability but dismissed the assertion because YouTube had "no duty" to utilize these tools. *Id.* at 117. If true, this technology was available fifteen years after the DMCA. It has been another twelve years since this decision came down.

[72] *Id.* at 114–15 (emphasis added).

[73] UMG Recordings, Inc. v. Veoh Networks Inc., 665 F. Supp. 2d 1099, 1108, 1118 (C.D. Cal. 2009) (granting summary judgment for the online service provider) ("[T]he burden is on the copyright holder to provide notice of allegedly infringing material."); *see also* Atlantic Recording Corp. v. Spinrilla, LLC, 506 F. Supp. 3d 1294, 1317 (N.D. Ga. 2020) ("[T]he DMCA has often been construed in favor of service providers requiring little effort by their operations to maintain immunity." (quoting Disney Enters., Inc. v. Hotfile Corp., No. 11-20427-CIV, 2013 WL 6336286, at *19 (S.D. Fla. Sep. 20, 2013))); Flava Works, Inc. v. Gunter, 689 F.3d 754, 758, 764 (7th Cir. 2012) (vacating preliminary injunction) ("Congress wanted to make the safe harbor as capacious as possible—however broadly contributory infringement might be understood, the Internet service provider would be able to avoid liability."); Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102, 1113 (9th Cir. 2007) ("DMCA notification procedures place the burden of policing copyright infringement—identifying the potentially infringing material and adequately documenting infringement—squarely on the owners of the copyright.").

[74] The DMCA was passed over eight years before the release of the first iPhone. *See* John Markoff, *Apple Introduces Innovative Cellphone*, N.Y. TIMES (Jan. 10, 2007), https://www.nytimes.com/2007/01/10/technology/10apple.html [https://perma.cc/FJ9J-2JN5]. In September, 2024, the iPhone 16 was released.

providing safe harbor protections to online service providers and assess whether these foundations still stand in an AI-driven Internet landscape.

When Congress enacted the DMCA, online platforms functioned more like passive bulletin boards than active editors—a fundamental assumption underpinning the § 512 safe harbor provisions discussed above.[75] Under this framework, online service providers resembled sophisticated copy machines: users might employ them for infringing or non-infringing purposes, but the website remained merely an inert tool. Just as copyright law does not hold Xerox liable when users improperly use their machines, Congress sought to shield AOL or Yahoo! from heightened liability.[76] This assumption also explains the function of notice-and-takedown procedures—§ 512(c) only protects service providers when a user posts infringing material, not when the provider creates or actively promotes such content.[77]

A website's increased accessibility compared to a physical copy machine makes it potentially more dangerous to copyright owners' exclusive rights. One person misusing a copy machine does not make information universally available; contrarily, a single upload to the Internet instantly makes copyrighted material accessible to anyone with comparable Internet access. Recognizing this amplification effect, Congress adopted the principle that "with great power comes great responsibility."[78] Service providers must remove infringing content to maintain immunity once adequately notified of infringing content.[79] However, these procedures only function effectively when copyright holders are better

---

Tripp Mickle, *Apple Unveils New iPhones With Built-In Artificial Intelligence*, N.Y. TIMES (Sep. 9, 2024), https://www.nytimes.com/2024/09/09/technology/apple-event-iphone-16-watch.html [https://perma.cc/P6A6-SQYU].

75 Scott, *supra* note 46, at 155; *see also* ALS Scan, Inc. v. RemarQ Cmtys., Inc., 239 F.3d 619, 625 (4th Cir. 2001) ("The DMCA was enacted . . . to provide immunity to service providers from copyright infringement liability for 'passive,' 'automatic' actions." (citing H.R. REP. NO. 105-796, at 72 (1998) (Conf. Rep.))).

76 In *Williams & Wilkins Co. v. United States*, plaintiffs accused defendants of photocopying their copyrighted works, but the company that sold the photocopying machines was not a named defendant. 487 F.2d 1345, 1346–47 (Ct. Cl. 1973), *aff'd*, 420 U.S. 376 (1975) (per curiam).

77 *See* 17 U.S.C. § 512(c)(1).

78 Jim Owsley et al., *Spider-Man vs. Wolverine*, *in* SPIDER-MAN VS. WOLVERINE 1 (Marvel Comics 1987).

79 17 U.S.C. § 512(c)(1)(C).

positioned than service providers to discover infringement—an assumption that collapses when platforms deploy sophisticated AI detection systems.

The technological limitations of the late 1990s further justified this arrangement. Section 512's categories reveal the primitive services Internet businesses offered then: "[t]ransitory digital network communications"[80] (essentially an online version of FedEx), "[s]ystem caching"[81] (comparable to electronic rental lockers), "[i]nformation residing on systems or networks at direction of users"[82] (like electronic file cabinets), and "[i]nformation location tools"[83] (analogous to online indices).[84] These services resembled early paved roads: although stop signs might be obvious, motion-censored traffic lights and automated toll systems represented unanticipated but necessary later developments. The 1998 Internet was still mastering basic user access and exploration; expecting more sophisticated infrastructure oversight could have stunted the industry's growth.[85]

Given this adolescent online ecosystem, Congress sought to avoid regulations that would stunt electronic commerce. By 1998, e-commerce had already become a critical component of the national economy,[86] accounting for 8.2% of the United States' GDP and employing approximately 7.4 million Americans.[87] The Commerce Committee projected e-commerce would grow by a factor of 100 over roughly five years—a trajectory they were determined to protect.[88] Though copyright protection is supposed "to promote the Progress of Science and useful Arts,"[89] Congress opted to limit service provider liability—

---

80 *Id.* § 512(a).

81 *Id.* § 512(b).

82 *Id.* § 512(c).

83 *Id.* § 512(d).

84 These activities were also outlined in the Senate's Judiciary Committee Report. S. REP. NO. 105-190, at 19.

85 Donald P. Harris, *Time to Reboot? Rethinking the Digital Millenium Copyright Act*, Temple 10-Q, https://www2.law.temple.edu/10q/time-to-reboot-rethinking-the-digital-millennium-copyright-act/ [https://perma.cc/V7FZ-7FS5].

86 H.R. REP. NO. 105-551, at 22.

87 *Id.*

88 *Id.*

89 U.S. CONST. art. I, § 8, cl. 8; *see also* THE FEDERALIST NO. 43 (James Madison) ("The utility of this power will scarcely be questioned. The copyright of

liability that could have extinguished the wildfire of online commercial activity as America entered the twenty-first century.[90]

Importantly, Congress did not intend to abandon copyright owners, recognizing that the digital ecosystem would never fully flourish without creators' contributions. They described electronic commerce growth and intellectual property protection as "mutually supportive" goals:[91] "A thriving electronic marketplace provides new and powerful ways for the creators of intellectual property to make their works available to legitimate consumers in the digital environment."[92] Congress understood that technology enabling copying, transmitting, and storing copyrighted works was a recipe for piracy.[93] It attempted to address this through anti-circumvention provisions outlawing technologies explicitly developed for infringing purposes.[94] Despite objections from copyright law professors, the House Commerce Committee deemed these measures crucial, believing "the digital environment poses a unique threat to the rights of copyright owners, and as such, necessitates protections against devices that undermine copyright interests."[95]

Although Congress intended creators to serve as the springboard propelling electronic commerce into the new millennium, authors and artists were crushed beneath the Internet's explosive growth—a consequence of safe harbor provisions that failed to anticipate how technology would fundamentally transform content distribution and monetization.[96] The DMCA allowed the Internet to develop commercially.[97] However, development came at a cost to

---

authors has been solemnly adjudged, in Great Britain, to be a right of common law…the public good fully coincides in both cases with the claims of [authors].").

90 *See* H.R. REP. NO. 105-551, at 22 (describing the DMCA as a bill "about much more than intellectual property").

91 *Id.* at 23.

92 *Id.*

93 *Id.*

94 *Id.* at 23–24.

95 *Id.* at 24–25.

96 *See generally* Joint Comments of the Music Community, Comment Letter on *in re* Section 512 Study: Notice and Request for Public Comment, Docket No. 2015–7, (Apr. 1, 2016) (submitted by Jay Rosenthal & Steven Metalitz, Mitchell Silberberg & Knupp LLP).

97 Harris, *supra* note 85.

copyright owners. As passive virtual bulletin boards transformed into AI-algorithmic content moderators, creators faced greater burdens complying with safe harbor notice and takedown procedures. The justifications are no longer valid: the DMCA needs a makeover.

III. AI'S DUAL ROLE: HOW SOCIAL MEDIA WEAPONIZES TECHNOLOGY AGAINST COPYRIGHT

Social media platforms have transformed from passive message boards into sophisticated AI-powered content engines that actively curate, promote, and monetize user experiences.[98] Far from mere conduits of information—the model the DMCA was designed to protect—today's platforms deploy complex algorithms that scrutinize user behavior, predict preferences, and shape content consumption.[99] Any regular user has experienced this firsthand: casually mention a vacation destination in a post or private message, and suddenly, their feed fills with resort advertisements and travel deals—a capability that would have seemed like science fiction to the DMCA's drafters in 1998.

This evolution extends beyond personalized advertising. User-posted content—photos, comments, and witty posts—is now used to train large AI language models without permission or reward.[100] Yet, platforms that can detect and remove infringing material fail to do so despite their willingness to moderate content in other contexts.

This Section will examine three critical ways social media companies deploy AI that fundamentally challenge the DMCA's passive intermediary assumption: first, how AI-powered personalization algorithms actively curate and promote content; second, how platforms scrape user-generated content to train sophisticated AI models; and third, how these companies selectively use advanced detection tools when copyright enforcement aligns with their business interests. Together, these practices reveal that modern platforms possess both the capability

---

98 *See* Tonya Mosley, *How Social Media Algorithms 'Flatten' Our Culture by Making Decisions For Us*, NAT'L PUB. RADIO (Jan. 17, 2024), https://www.npr.org/2024/01/17/1224955473/social-media-algorithm-filterworld [https://perma.cc/P2WL-N2GW].

99 *See* Nimit Bhardwaj, *The Role of AI and Algorithms in Social Media*, TOWARDS AI (May 1, 2024), https://towardsai.net/p/artificial-intelligence/the-role-of-ai-and-algorithms-in-social-media [https://perma.cc/D7P8-4TYX].

100 Eli Tan, *When the Terms of Service Change to Make Way for A.I. Training*, N.Y. TIMES (Jun. 26, 2024), https://www.nytimes.com/2024/06/26/technology/terms-service-ai-training.html [https://perma.cc/C7NN-AZJB].

and the technological infrastructure to address copyright infringement—they only lack a legal mandate to act.

A. FROM PASSIVE TO PREDATORY: THE ALGORITHMIC REVOLUTION

Social media has evolved far beyond the chronological feed of posts from accounts users choose to follow. Today's platforms deploy sophisticated AI algorithms that actively curate and promote content through features like 'For you' feeds on X, Instagram, and TikTok.[101] Although seemingly benign—showing baseball memes to sports enthusiasts or wedding content to engaged users—these algorithms represent a fundamental shift in the Internet landscape since the DMCA's passage.[102] Although some scholars have warned that these algorithms are far from harmless and increase polarization and divisiveness among the user population,[103] the benefits and drawbacks of social media algorithms are beyond the scope of this Article.[104] Notably, social media websites—far from their ancestral virtual bulletin boards—now actively filter and promote content, akin to album

---

[101] *See, e.g.*, *About Your For You Timeline on X*, X HELP CENTER, https://help.x.com/en/using-x/x-timeline [https://perma.cc/SDS5-XUPW]; *How Instagram Determines Which Posts Appear as Suggested Posts*, INSTAGRAM HELP CENTER, https://help.instagram.com/381638392275939 [https://perma.cc/LZ5K-RPLF]; *For You*, TIKTOK SUPPORT, https://support.tiktok.com/en/getting-started/for-you [https://perma.cc/2YRQ-TCFH].

[102] *See AI in Social Media: Enhancing User Experience, Content Moderation, and Personalization*, POTENTIAL (Oct. 29, 2024), https://www.potential.com/articles/how-ai-is-transforming-social-media/n [https://perma.cc/G8JU-NGRJ].

[103] Brett Milano, *'The Algorithm Has Primacy Over Media . . . Over Each of Us, and It Controls What We Do'*, HARV. L. TODAY (Nov. 18, 2021), https://hls.harvard.edu/today/the-algorithm-has-primacy-over-media-over-each-of-us-and-it-controls-what-we-do/ [https://perma.cc/K2DQ-XDFD] ("[Social Media] can't not polarize the population. No matter where you stand—if masks are your thing, or vaccines, or critical race theory—it doubles down on your perspective or reminds you why the other side is wrong." (quoting Tristan Harris, co-founder and president of the Center for Humane Technology)).

[104] For competing views, compare Samuel Dick, *"Warning: Algorithms Harm Children": How Texas's Failure to Warn Doctrine Can Address the Youth Mental Health Crisis*, 56 TEX. TECH L. REV. 711 (2024) with Nina I. Brown, *Regulatory Goldilocks: Finding the Just and Right Fit for Content Moderation on Social Platforms*, 8 TEX. A&M L. REV. 451 (2021).

producers curating greatest hits collections.[105] This Section will explore how these algorithms determine which content to promote to end-users, the business advantages these algorithms provide, and the courts' treatment of these algorithms. It will conclude with how the use of these algorithms hurts copyright owners.

1. *Engineering Engagement: The Mechanics of AI Content Curation*

At their core, social media algorithms serve a single purpose: showing users what will keep them engaged. These systems analyze every facet of user data—from basic demographic information like age and location[106] to subtle behavioral patterns such as content engagement, scrolling speed, and viewing duration.[107] As users interact with a platform, the algorithm continuously refines its understanding of their preferences, becoming increasingly effective at serving satisfying, engagement-driving content.[108] Social media companies design these algorithms to do two things: keep users on the app as long as possible and bring users back once they inevitably log off.[109]

This personalization relies on multiple AI technologies working in concert:

- Natural Language Processing (NLP) enables algorithms to understand human language and sentiment, categorizing content by topic and

---

[105] CLARE Y. CHO & LING ZHU, CONG. RSCH. SERV., R46662, SOCIAL MEDIA: CONTENT DISSEMINATION AND MODERATION PRACTICES 10 (2025).

[106] Haliza Arfa, *A Mirror of Thoughts: Personalized Social Media Algorithm*, MEDIUM (July 16, 2024), https://medium.com/compfest/a-mirror-of-thoughts-personalized-social-media-algorithm-70fce576ed9b [https://perma.cc/WCM6-2W6P].

[107] *AI in Social Media: Enhancing User Experience, Content Moderation, and Personalization*, *supra* note 102.

[108] Arfa, *supra* note 106.

[109] Ben Smith, *How TikTok Reads Your Mind*, N.Y. TIMES (Dec. 5, 2021), https://www.nytimes.com/2021/12/05/business/media/tiktok-algorithm.html [https://perma.cc/2RZW-VSVL].

viewpoint. For instance, NLP would associate 'diamond' with baseball fields for sports fans but with engagement rings for wedding planners.[110]

- Deep Learning detects complex patterns in massive datasets through neural networks that mimic the human brain's structure. Although decision-making often functions as a "black box," these systems identify non-intuitive connections, such as correlations between baseball content engagement and interest in specific dog breeds.[111]

- Reinforcement Learning refines algorithms through continuous feedback, rewarding systems when they increase content engagement and penalizing them when user interest wanes.[112]

As users continue to engage on the platform, these tools collectively develop increasingly sophisticated models of user preferences, creating feedback loops that drive user satisfaction and platform revenue.[113] As users complain, user engagement decreases, or as content providers begin to "game" the algorithm, social media companies will adjust the algorithm manually to meet market demands.[114]

2. *Monetizing Attention: The Imperative of Algorithmic Personalization*

Personalization algorithms are not merely features—they form the economic backbone of social media platforms. Unlike traditional media, social media companies do not sell content; they monetize user attention through targeted advertising.[115] The free-to-join nature of platforms like Instagram,

---

110 *AI in Social Media: Enhancing User Experience, Content Moderation, and Personalization*, *supra* note 102.

111 Vincent Dumas, *Enigma Machines: Deep Learning Algorithms as Information Content Providers Under Section 230 of the Communications Decency Act*, 2022 WIS. L. REV. 1581, 1593 (2022).

112 Haochen Sun, *The Right to Know Social Media Algorithms*, 18 HARV. L. & POL'Y REV. 1, 26 (2023).

113 Smith, *supra* note 109; Hannah Metzler & David Garcia, *Social Drivers and Algorithmic Mechanisms on Digital Media*, 19 PERSPS. ON PSYCH. SCI. 735 (2024).

114 Metzler & Garcia, *supra* note 113.

115 CHO & ZHU, *supra* note 105.

Facebook, X, and TikTok masks their fundamental business model: generating revenue by selling third-party access to carefully cultivated user engagement.[116]

The longer users remain on platforms, and the more frequently they return, the more valuable each advertising impression becomes. This economic reality drives platforms to continuously refine their personalization capabilities, creating systems that precisely target content most likely to capture and retain attention. The effectiveness of these systems is staggering: AI-driven personalized marketing increases user engagement by 42%,[117] click-through rates on social media advertising by 49%,[118] and revenue by 40%.[119] For social media companies, personalization is not merely an enhancement—it's the engine that powers their entire business model.

3. *Judicial Acquiescence: Courts' Treatment of AI-Powered Distribution*

Even as algorithms actively curate content for users, courts religiously grant platforms safe harbor protection. *Davis v. Pinterest, Inc.* illustrates the contemporary judicial approach. There, the Northern District of California granted Pinterest safe harbor protection despite its algorithm promoting the plaintiff's copyrighted works—posted without authorization—alongside targeted advertisements.[120]

---

116 Robert H. Frank, *The Economic Case for Regulating Social Media*, N.Y. TIMES (Feb. 11, 2021), https://www.nytimes.com/2021/02/11/business/social-media-facebook-regulation.html [https://perma.cc/5P5F-XN8G].

117 Natalie Nkembuh, *Beyond Algorithms: A Comprehensive Analysis of AI-Driven Personalization in Strategic Communications*, 12 J. COMPUT. & COMMC'NS 112, 122 (2024).

118 *Id.* at 123. Click-through rate is defined as "the percentage of people visiting a web page who access a hypertext link to a particular advertisement." *Click-through Rate*, OXFORD ENGLISH DICTIONARY, https://www.oed.com/dictionary/click-through-rate_n?tab=meaning_and_use#10827980100 [https://perma.cc/KQU5-PLD5].

119 Molly Hayes & Amanda Downie, *What Is AI Personalization?*, IBM (Aug. 5, 2024), https://www.ibm.com/think/topics/ai-personalization [https://perma.cc/MML4-YUPC].

120 Davis v. Pinterest, Inc., 601 F. Supp. 3d 514, 517–21, 536 (N.D. Cal. 2022), *aff'd*, No. 22-15804, 2023 WL 5695992 (9th Cir. Sep. 5, 2023) (memorandum opinion).

Pinterest is a social media app that allows users to build virtual bulletin boards with uploaded pictures and videos.[121] Each image or video is a "Pin" that appears on the user's home feed.[122] After the user uploads an image, Pinterest automatically copies the upload and modifies the image to create "variants" that optimize the user experience on the app.[123] These variants are the same image or video but displayed in different sizes to provide a more aesthetically pleasing home feed for the user.[124] Users can remove or add Pins, which adjust their personalized algorithm on Pinterest and affect the content the users see on the app.[125] The *Davis* court provided the following example as illustrative of a user's home feed:

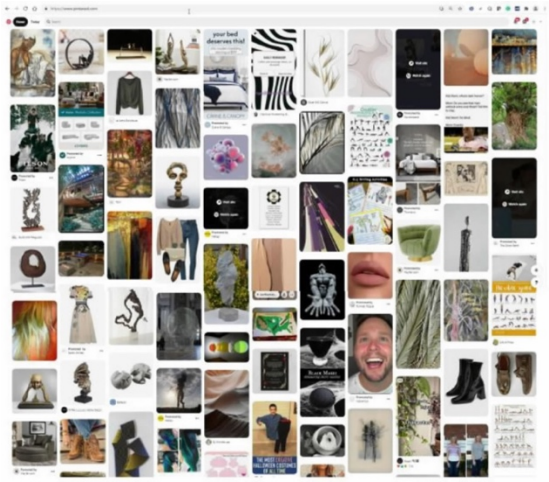

Figure 1. Pinterest User's "Home Feed". [126]

Pinterest offers an alternative "related Pins feed" that provides images and videos of Pins on the user's home feed.[127] Users can also utilize a search function to find content on Pinterest that matches their query.[128] Like most prominent social media websites, Pinterest produces revenue solely through third-party advertising on

121 *Id.* at 518.

122 *Id.*

123 *Id.*

124 *Id.*

125 *Id.*

126 *Davis*, 601 F. Supp. 3d at 519.

127 *Id.*

128 *Id.* at 520.

these separate feeds.[129] "Advertisers may pay Pinterest per click or view for these 'promoted Pins.'"[130] Pinterest notifies users of promoted content through the app, email, and push notifications.[131] The photographer in *Davis* did not challenge users uploading his copyrighted material without permission; he challenged Pinterest's use of his copyrighted works "pinned" adjacent to Pinterest's promoted advertisements as "unauthorized commercial use of his works."[132] Further, he challenged Pinterest's distribution of his copyrighted works in push notifications and emails to users.[133] One of the plaintiff's fifty-one copyrighted works displayed on Pinterest appeared "4,676 times over the course of just two weeks."[134]

The court described the plaintiff's claim as "an end-run around the DMCA."[135] The plaintiff complained that Pinterest did not have a notice-and-takedown procedure to stop the algorithm from promoting his work with third-party advertisements, but allowed the works to remain organically on users' home feeds.[136] The court took issue with this stance. Because "[t]he DMCA does not permit copyright holders to dictate the manner in which service providers run their platforms," the plaintiff could not allow Pinterest users to continue to publish his content on their home page for their aesthetic pleasure without allowing Pinterest to profit from this infringement.[137]

Alternatively, the court granted Pinterest safe harbor relief even if its actions infringed.[138] Citing *Viacom International, Inc. v. YouTube, Inc.*, the court noted that suggesting copyright-infringing user-uploaded content to other users did not constitute "promotion" of infringement but rather "helps facilitate users' access to Pins."[139] Further, Pinterest did not have the "right and ability to control the infringing activity" in this case.[140] The court found Pinterest's deployment of

---

129 *Id.*

130 *Davis*, 601 F. Supp. 3d at 520.

131 *Id.*

132 *Id.* at 520–21 (internal quotations omitted).

133 *Id.*

134 *Id.* at 518, 521.

135 *Davis*, 601 F. Supp. 3d at 530.

136 *Id.* at 531.

137 *Id.* at 530–31.

138 *Id.* at 531.

139 *Id.* at 532–33.

140 *Id.* at 534 (internal quotations omitted).

its algorithm to promote the plaintiff's content alongside third-party advertisements was "indistinguishable from that of YouTube in *Viacom*."[141] Because Pinterest's algorithm's promotion efforts are automatic, Pinterest was not found to be exercising sufficient control to lose safe harbor protection.[142] Most surprisingly, the Northern District of California held that Pinterest did not financially benefit from the infringing activity.[143] Because Pinterest's algorithm determines what promoted pins and user-uploaded pins appear on any given user's feed, Pinterest and the third-party advertisers do not control which content is promoted adjacent to the plaintiff's copyrighted works.[144] The revenue Pinterest produces from promoting the infringing content adjacent to advertised Pins must be "distinctly attributable to the infringing material at issue" for Pinterest to lose safe harbor protections.[145] In a memorandum opinion, the Ninth Circuit affirmed that Pinterest had safe harbor protection under the DMCA.[146]

Contrastingly, the Ninth Circuit denied safe harbor protection when human employees perform similar functions—in *Mavrix Photographs, LLC v. LiveJournal, Inc.*, the Ninth Circuit reversed summary judgment for a platform where volunteer moderators screened uploaded content before publication.[147] Because humans reviewed merely twenty copyrighted photos before allowing their posting, the court found potential liability through agency principles that would not apply to automated systems performing identical functions at a vastly larger scale.[148]

LiveJournal was a social media site that allowed users to create communities and upload content relevant to their communities.[149] Volunteer administrators moderated the content to ensure compliance with the user-made

---

141 *Davis*, 601 F. Supp. 3d at 535.

142 *See id.* at 532–33, 535.

143 *Id.* at 535.

144 *Id*.

145 *Id.* (quoting Ventura Content, Ltd. v. Motherless, Inc., 885 F.3d 597, 613 (9th Cir. 2018)).

146 Davis v. Pinterest, Inc., No. 22-15804, 2023 WL 5695992, at *1–2 (9th Cir. Sep. 5, 2023) (memorandum opinion).

147 Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1049 (9th Cir. 2017).

148 *See id.* at 1048–49.

149 *Id.*

community rules.[150] As their most popular community grew "to 52 million page views per month," LiveJournal hired a full-time moderator to exercise greater control and seek advertisement revenue.[151] The plaintiff alleged LiveJournal posted "twenty of its copyrighted photographs online."[152] Because a team of volunteer moderators reviewed the copyrighted photos before allowing them to be posted on LiveJournal, the plaintiffs claimed LiveJournal was liable through the common law of agency.[153] Although the district court ruled that the common law of agency does not apply to the DMCA's safe harbor analysis, the Ninth Circuit disagreed.[154] Because the users merely uploaded the posts, while the volunteer moderators screened and ultimately publicly posted the uploads, there was a genuine issue of material fact whether the volunteers were acting as LiveJournal's agents in posting the infringing material.[155] If the moderators acted as LiveJournal's agents, LiveJournal would be liable for copyright infringement and denied the DMCA's safe harbor provisions if the moderators knew or should have known the material was copyrighted or if LiveJournal financially benefited from the infringement that the moderators had the right and ability to control.[156]

4. *The Copyright's Venom: Algorithmic Amplification*

This judicial inconsistency creates a perverse incentive structure: social media companies face liability when human agents screen twenty photographs[157] but receive safe harbor protection when their algorithms republish thousands of infringing images alongside profit-generating advertisements.[158] In essence, platforms are penalized for human oversight while rewarded for automated amplification of infringement.

---

150 *Id.*

151 *Id.* at 1050.

152 *Id.* at 1048.

153 *Mavrix Photographs*, 873 F.3d at 1048–49.

154 *Id.* at 1049.

155 *Id.* at 1053–54.

156 *Id.* at 1057–59.

157 *See id.*

158 *See* Davis v. Pinterest, Inc., 601 F. Supp. 3d 514, 528–36 (N.D. Cal. 2022), *aff'd*, No. 22-15804, 2023 WL 5695992 at *1–2 (9th Cir. Sep. 5, 2023) (memorandum opinion).

The result is a system that encourages blind automation while ignoring copyright owners' interests. Courts have inadvertently incentivized platforms to automate content recognition by granting immunity to algorithmic dissemination while penalizing human review. This amplification of infringement contradicts the DMCA's assumption of passive intermediaries. Platforms today actively determine which content reaches specific users, deploy advanced content recognition systems, and profit directly from engagement with all content—including infringing material. Yet, they continue to enjoy safe harbor protections designed for passive bulletin boards, which lacked the technological capacity to monitor user-uploaded content.

B. DATA HARVESTING WITHOUT CONSENT: HOW PLATFORMS EXPLOIT CONTENT FOR AI

Social media companies' relationship with user content extends beyond personalization algorithms—these platforms increasingly harvest users' online activity to train AI models, creating a second revenue stream from user-posted content. Although scholars have explored the privacy implications of this practice,[159] the copyright dimensions present an even more troubling contradiction: the platforms that once claimed the inability to monitor copyright infringement simultaneously demonstrate sophisticated content recognition capabilities when extracting value from that same content for AI training purposes.

1. *Architecture of Intelligence: Understanding Large Language Models*

Large language models (LLMs) represent a revolutionary category of foundation models trained on massive datasets that enable them to understand and generate natural language and other content across diverse tasks.[160] These models respond to human prompts by answering questions, summarizing information, writing content, and translating languages[161]—capabilities that

---

[159] *See, e.g.*, Amanda Levendowski, *Resisting Face Surveillance with Copyright Law*, 100 N.C.L. REV. 1015 (2022); Jon M. Garon, *Prometheus' Digital Fire: The Civic Responsibilities of AI*, 20 OHIO ST. TECH. L.J. 225 (2024).

[160] *What Are Large Language Models (LLMs)?*, IBM (Nov. 2, 2023), https://www.ibm.com/think/topics/large-language-models [https://perma.cc/EUS9-6YRQ].

[161] *What Is a Large Language Model (LLM)?*, UNIV. OF ARIZ. LIBR., https://ask.library.arizona.edu/faq/407985 [https://perma.cc/8L8N-6FU4].

require ingesting vast amounts of training data from across the Internet to engage in unsupervised learning to detect previously unknown patterns.[162]

Combining deep learning AI architectures with natural language processing, LLMs operate on neural networks designed to mimic human brain function, teaching themselves relationships between words, grammatical structures, and knowledge across nearly limitless domains.[163] Their effectiveness depends directly on the breadth and depth of their training data—typically encompassing much of the publicly accessible Internet—and their ability to engage in unsupervised learning to detect previously unrecognized patterns.[164] Popular services employing this technology include OpenAI's ChatGPT, Google's Gemini, and DeepSeek AI.[165]

2. *Data Mining at Scale: How Platforms Extract Value from User Content*

Social media companies routinely utilize users' activities—often without meaningful consent—to train LLMs to become more conversational and responsive.[166] Although personalization algorithms enhance user engagement

---

[162] Michael Chen, *What is Machine Learning?*, ORACLE CLOUD INFRASTRUCTURE (Nov. 25, 2024), https://www.oracle.com/artificial-intelligence/machine-learning/what-is-machine-learning/ [https://perma.cc/L5DL-23CH].

[163] *What is LLM (Large Language Model)?*, AMAZON WEB SERVS., https://aws.amazon.com/what-is/large-language-model/ [https://perma.cc/P58G-5TD2].

[164] *Large Language Models Explained*, NVIDIA, https://www.nvidia.com/en-us/glossary/large-language-models/ [https://perma.cc/W2W8-M5G9].

[165] Cade Metz, *OpenAI Unveils New ChatGPT That Listens, Looks and Talks*, N.Y. TIMES (May 13, 2024), https://www.nytimes.com/2024/05/13/technology/openai-chatgpt-app.html [https://perma.cc/F6A8-9P27] [hereinafter Metz, *OpenAI Unveils New ChatGPT*]; Cade Metz, *Google Releases Gemini, an A.I.-Driven Chatbot and Voice Assistant*, N.Y. TIMES (Feb. 8, 2024), https://www.nytimes.com/2024/02/08/technology/google-gemini-ai-app.html [https://perma.cc/2PW5-963Z]; Cade Metz, *What to Know About DeepSeek and How It Is Upending A.I.*, N.Y. TIMES (Jan. 27, 2025), https://www.nytimes.com/2025/01/27/technology/what-is-deepseek-china-ai.html [https://perma.cc/3EEU-2VDH].

[166] Claire Duffy, *Social Media Platforms are Using What You Create for AI. Here's How to Opt Out*, CNN (Sep. 23, 2024),

with the platform, AI training extracts value from user-generated content to develop models that better simulate "[c]onversational nuances, regional slang, evolving trends, and diverse perspectives."[167] This practice represents a secondary exploitation of the same content that platforms claimed they could not effectively monitor for copyright infringement.

The notification methods for this data scraping vary widely among platforms, revealing inconsistent approaches to transparency and consent:

- Meta publicly announced using Facebook and Instagram posts to train its AI at its 2023 annual conference. However, it excluded private chats, selective-audience posts, and LinkedIn content from the training datasets.[168]

- LinkedIn scraped user data, including resumes and professional posts, to train its AI model and shares this data with Microsoft's partner, OpenAI, under its terms of service.[169] Although users can opt out of future data collection, LinkedIn retains already-scraped content used in previous model training.[170]

- X (formerly Twitter) defaulted all users to allowing content scraping for training its Grok AI model without public notice in July 2024. Users could only opt out of future posts, while content already used for training remained in the model. [171]

---

https://www.cnn.com/2024/09/23/tech/social-media-ai-data-opt-out/index.html [https://perma.cc/UZ62-2DJK].

167 Poonacha Machaiah, *Your AI Training Data: How Social Media Giants Are Mining Your Digital Life*, MEDIUM (Jan. 4, 2025), https://medium.com/@poonacha/your-ai-training-data-how-social-media-giants-are-mining-your-digital-life-d5e32c2c432f [https://perma.cc/JXF8-E8T5].

168 Katie Paul, *Meta's New AI Assistant Trained on Public Facebook and Instagram Posts*, REUTERS (Sep. 28, 2023), https://www.reuters.com/technology/metas-new-ai-chatbot-trained-public-facebook-instagram-posts-2023-09-28/ [https://perma.cc/4ABU-36DW].

169 Machaiah, *supra* note 167; Duffy, *supra* note 166.

170 Duffy, *supra* note 166.

171 John Koetsier, *Here's How To Stop X From Using Your Data To Train Its AI*, FORBES (July 26, 2024), https://www.forbes.com/sites/johnkoetsier/2024/07/26/x-just-gave-itself-

- Snapchat's terms of service permit the use of AI-created pictures for further training and advertising purposes.[172]

- Reddit's terms grant the company a free license to sell user content to AI developers, including arrangements with Google and OpenAI.[173]

In most cases, content posted before opt-out options became available has already been incorporated into training datasets, resulting in the irreversible appropriation of potentially copyrighted material.[174]

3. *Copyright Infringement by Design: Legal Implications of Training AI*

Given the prevalence of copyright infringement on social media platforms, training LLMs on user content inevitably means training them on copyrighted material without authorization.[175] Previous litigation reveals the scale of this issue: in *Viacom International, Inc. v. YouTube, Inc.*, YouTube's financial advisor "estimate[d] that more than 60% of YouTube's content was 'premium' copyrighted content—and that only 10% of the premium content was authorized."[176] Similarly, one plaintiff's copyrighted photo in *Davis v. Pinterest, Inc.* appeared "4,676 times over the course of just two weeks" without authorization.[177] These cases predated ChatGPT's initial release, suggesting the scope of copyright materials in training data is likely substantial.[178]

---

permission-to-use-all-your-data-to-train-grok/ [https://perma.cc/EJA5-6BGN].

172 Duffy, *supra* note 166.

173 *Id.*

174 *See* Koetsier, *supra* note 171.

175 Lauren Leffer, *Your Personal Information Is Probably Being Used to Train Generative AI Models*, SCI. AM. (Oct. 19, 2023), https://www.scientificamerican.com/article/your-personal-information-is-probably-being-used-to-train-generative-ai-models/ [https://perma.cc/E6HH-NN8X].

176 *2d Cir. Viacom Int'l*, 676 F.3d 19, 33 (2nd Cir. 2012). Employee website surveys "estimated that 75–80% of all YouTube streams contained copyrighted material." *Id.* at 33–34 (finding no specific knowledge of infringing material).

177 Davis v. Pinterest, Inc., 601 F. Supp. 3d 514, 521 (N.D. Cal. 2022), *aff'd*, No. 22-15804, 2023 WL 5695992 (9th Cir. Sep. 5, 2023) (memorandum opinion).

178 Metz, *OpenAI Unveils New ChatGPT*, *supra* note 165.

Legal challenges to these practices have begun to emerge, with the District of Delaware recently granting partial summary judgment to a copyright owner whose exclusive rights were violated when his copyrighted material was used to train a legal research AI tool.[179] However, copyright owners face a fundamental remedy challenge—these models cannot be "untrained" once they have ingested data.[180] The impossibility of removing specific training data from neural networks leaves traditional injunctive relief largely ineffective.

Given the economic importance of AI development—comparable to the significance of electronic commerce in 1998—courts may hesitate to impose remedies that significantly impede innovation.[181] The situation resembles Pandora's Box—once opened, it cannot be closed. Nevertheless, although exclusive rights have been compromised in training current LLMs, AI technologies remain the most promising mechanism for protecting those same rights in the future. This fundamental contradiction illuminates the central argument of this Article: the same technologies that threaten copyright protection can and should be harnessed to enforce it.

C. SELECTIVE ENFORCEMENT: PLATFORMS' CAPACITY FOR COPYRIGHT PROTECTION

As established at the outset, this Article's core argument is that AI should be deployed to detect and combat online copyright infringement, protecting authors' and creators' exclusive rights. This approach would require social media platforms to develop AI tools to detect and remove infringing material. However, "develop" is a misleading term—these companies already possess sophisticated

---

179 Thomson Reuters Enterp. Ctr. GMBH v. Ross Intel. Inc., No. 1:20-cv-613-SB, 2025 WL 458520, at *10 (D. Del. Feb. 11, 2025).

180 Leffer, *supra* note 175.

181 *See* Cecilia Kang, *Emboldened by Trump, A.I. Companies Lobby for Fewer Rules*, N.Y. TIMES (Mar. 24, 2025), https://www.nytimes.com/2025/03/24/technology/trump-ai-regulation.html [https://perma.cc/686W-SSRH] ("After the President made A.I. dominance a top priority, tech companies changed course from a meeker approach under the Biden administration."). Copyright owners may be viewed similar to non-practicing entities seeking injunctive relief in patent cases due to America's commitment to win the AI race. *See* eBay, Inc. v. MercExchange, LLC, 547 U.S. 388, 396 (2006) (J. Kennedy, concurring) ("[A]n injunction, and the potentially serious sanctions arising from its violation, can be employed as a bargaining tool to charge exorbitant fees to companies that seek to buy licenses to practice the patent.").

content recognition technologies capable of identifying when and where copyrighted works appear on their platforms.[182] The technological capability to proactively address infringement has existed for years; what's missing is not the technical means but the legal obligation to deploy these tools beyond selective DMCA compliance.

Social media companies have been aware of widespread copyright infringement on their platforms for over a decade.[183] Evidence from *Viacom* revealed that as early as 2010, YouTube knew that more than 60% of uploaded content was copyrighted.[184] Despite this knowledge, the company deliberately restricted employee access to proprietary content identification tools that could have detected infringing material.[185] Perhaps most tellingly, YouTube possessed advanced technological measures for discovering infringement twelve years before ChatGPT's release—yet still received safe harbor protection because the DMCA "disclaims any affirmative monitoring requirement."[186] These detection capabilities have become increasingly sophisticated over time. One service provider even had to instruct users how to remix songs to bypass their copyright detection software, demonstrating both the existence and effectiveness of these technologies.[187]

Today, social media platforms deploy various sophisticated systems to identify infringing content—when it serves their interests to do so. YouTube's Content ID system enables copyright owners who "own exclusive rights to a substantial body of original material that is frequently uploaded to YouTube" to

---

182 Claire Cain Miller, *YouTube Ads Turn Videos Into Revenue*, N.Y. TIMES (Sep. 2, 2010), https://www.nytimes.com/2010/09/03/technology/03youtube.html [https://perma.cc/3DES-HTL6]; Sandy Beeson, *TikTok Copyright Explained: How to Use Copyrighted Music on TikTok*, UPPBEAT BLOG (July 7, 2025), https://uppbeat.io/blog/tiktok/tiktok-copyright [https://perma.cc/WSX7-7S8M].

183 *2d Cir. Viacom Int'l*, 676 F.3d at 33 (citing specific examples that YouTube executives were aware of infringing material posted on their platform).

184 *Id.* at 40–41.

185 *Id.*

186 *Id.* at 41.

187 Atlantic Recording Corp. v. Spinrilla, LLC, 506 F. Supp.3d 1294, 1302 nn.6–7 (N.D. Ga. 2020).

protect their works.[188] This system automatically compares uploaded videos against a database of copyrighted audio and visual files; upon detecting potential infringement, Content ID can block the video, monetize it on the copyright owner's behalf, or track viewership statistics to resolve infringement disputes.[189] YouTube recently announced plans to enhance Content ID to address AI-generated works that violate creators' copyrights and privacy rights[190]—a tacit acknowledgment of the technical feasibility of such screening and its importance in the AI era.

Although TikTok lacks automated preventative technologies, it offers creators a "Video Sound Copyright Check" function to verify copyright compliance before monetizing videos.[191] These systems help platforms avoid litigation rather than comprehensively protect copyright holders' interests.

The critical insight here is that these detection systems exist and represent proven technological capabilities that could be deployed more broadly. The same AI technologies that enable platforms to curate content, target advertisements, train large language models, and selectively enforce copyright when commercially advantageous could be employed to protect creators' rights systematically.

What's missing is not the technological capacity but the legal framework that would transform these selective tools into mandatory protections. As generative AI continues to evolve, threatening to undermine creators' exclusive rights, platforms must be further incentivized—or required—to deploy their existing detection capabilities more comprehensively. Otherwise, copyright risks becoming little more than legal fiction in the digital age—not because protection is technically impossible, but because platforms are discouraged from implementing the technologies they have already developed and deployed for other moderation purposes. Under current law, social media providers that automate promoting infringing content face no liability, while those who make any effort to moderate infringement expose themselves to liability. As AI systems

---

188 *How Content ID works*, YOUTUBE HELP, https://support.google.com/youtube/answer/2797370?hl=en [https://perma.cc/K58C-BH6A].

189 *Id.*

190 Amjad Hanif, *New Tools to Protect Creators and Artists*, YOUTUBE OFF. BLOG (Sep. 5, 2024), https://blog.youtube/news-and-events/responsible-ai-tools/ [https://perma.cc/69G3-F668].

191 *Video Sound Copyright Check Before Posting*, TIKTOK SHOP ACAD. (Feb. 27, 2023), https://seller-my.tiktok.com/university/essay?knowledge_id=6837846988130050&default_language=en&identity=1 [https://perma.cc/5859-5VEQ].

advance, incentivizing online service providers to remain passive rather than actively moderate content poses mounting dangers to copyright owners' protection.

IV. SELECTIVE ENFORCEMENT: PLATFORMS' DEMONSTRATED CAPACITY FOR CONTENT MODERATION

Asking social media platforms to identify and remove copyright-infringing content proactively is neither technologically unprecedented nor operationally unreasonable. These companies actively moderate massive volumes of user-generated content across multiple sensitive domains—from political discourse to public health information to community standards violations. Like digital town squares, social media has become society's primary venue for information exchange, social commentary, and public debate in the twenty-first century.[192] Yet, despite their claims of passive intermediary status when facing copyright obligations, these platforms routinely exercise significant editorial control through sophisticated content moderation systems.

The challenge of content moderation is substantial—anonymous users, emboldened by distance, often share uninformed, misleading, or deliberately harmful content. Platforms have developed comprehensive systems to "demote, remove, or label" content that violates their policies.[193] Social media companies can monitor and restrict content published on their platforms when adequately motivated.

This Section examines three significant domains where platforms have demonstrated their content moderation capabilities: election-related content, COVID-19 health information, and community standards enforcement. These examples collectively establish that platforms already operate as active content curators rather than passive intermediaries—a reality that should inform our approach to copyright enforcement in the AI age. If platforms can develop sophisticated systems to identify and moderate content across these domains, they can undoubtedly apply similar technologies to protect creators' exclusive rights.

---

[192] For a discussion on the free speech concerns with moderating user content on social media sites, compare Ariana S. Wilner, *The Constitutionality of Platform Content Moderation Bans from a Historical Perspective*, 17 N.Y.U.J.L. & LIBERTY 83 (2023) with Philip Hamburger, *Courting Censorship*, 4 J. FREE SPEECH L. 195 (2024).

[193] Sandra Gonzalez-Bailon, et. al., *The Diffusion and Reach of (Mis)Information on Facebook During the U.S. 2020 Election*, 11 SOCIOLOGICAL SCI. 1124, 1126–28 (2024).

A. DEMOCRATIC DISCOURSE UNDER WATCH: THE POLICING OF ELECTION CONTENT

Social media platforms have played increasingly consequential—and controversial—roles in recent United States presidential elections. After concerns about foreign election interference in 2016, platforms instituted vast content moderation schemes for the 2020 election.[194] Before the 2020 race, major social media companies updated their misinformation policies and developed tiered enforcement mechanisms.[195] These ranged from relatively mild interventions—such as Facebook and Twitter labeling posts that fact-checkers deemed misleading about the election process[196]—to more aggressive measures, including removing demonstrably false content, adjusting algorithms to limit its promotion, or even suspending accounts of repeat violators.[197] Facebook deployed independent third-party fact-checkers to identify misinformation,[198] while Twitter later developed

---

194 Jordan L. Couch, *Who Watches the Watchmen? Content Moderation in Social Media*, 40 GPSOLO 55, 56–57 (2023); Mike Isaac, *Facebook Moves to Limit Election Chaos in November*, N.Y. TIMES (Sep. 22, 2020), https://www.nytimes.com/2020/09/03/technology/facebook-election-chaos-november.html [https://perma.cc/7KCQ-N4AL].

195 THE ELECTION INTEGRITY PARTNERSHIP, THE LONG FUSE: MISINFORMATION AND THE 2020 ELECTION 216 (2021).

196 Samantha Bradshaw et. al, *An Investigation of Social Media Labeling Decisions Preceding the 2020 U.S. election*, PLOS ONE, Nov. 15, 2023, at 6. Labels included "Stay informed: Learn about US 2020 election security efforts" with an attached link and "Missing context: The same information was checked in another post by independent fact-checkers." *See* THE ELECTION INTEGRITY PARTNERSHIP, *supra* note 195, at 216–18.

197 Stuart A. Thompson, *To Fight Election Falsehoods, Social Media Companies Ready a Familiar Playbook*, N.Y. TIMES (Aug. 23, 2022), https://www.nytimes.com/2022/08/23/technology/midterms-misinformation-tiktok-facebook.html [https://perma.cc/93XR-WLQQ]; Sheera Frenkel, *The Rise and Fall of the 'Stop the Steal' Facebook Group*, N.Y. TIMES (Nov. 5, 2020), https://www.nytimes.com/2020/11/05/technology/stop-the-steal-facebook-group.html [https://perma.cc/7RNT-ZBY4]; Guy Rosen & Monika Bickert, *Our Response to the Violence in Washington*, META (Jan. 7, 2021), https://about.fb.com/news/2021/01/responding-to-the-violence-in-washington-dc/ [https://perma.cc/PY9N-NXN3]; THE ELECTION INTEGRITY PARTNERSHIP, *supra* note 195, at 215–16.

198 Sandra Gonzalez-Bailon, *Asymmetric Ideological Segregation in Exposure to Political News on Facebook*, 381 SCI. 392, 394 (2023).

"Birdwatch," enabling average users to write "community notes" providing context to disputed claims.[199]

For the 2024 election, platforms adjusted their approaches in response to both public criticism and changing political dynamics.[200] Following lawsuits and significant staff reductions, many companies moderated content less aggressively than they did in 2020; the introduction of generative AI tools presented new challenges, such as fabricated endorsements, leading some to believe that this election was defined by misinformation.[201] Given these companies' commitments to producing generative AI models by scraping posted content for training material and users utilizing generative AI tools to post content for the first time in American presidential election history, social media companies struggled to moderate the beast they were creating.[202] However, social media companies had valid reasons for curtailing their efforts in 2024. X and Facebook notably exempted high-profile users like presidential candidates from specific removal policies, citing the "newsworthy" nature of their posts.[203] Facebook maintained some fact-

---

199 Cotter et. al, *Fact-Checking the Crisis: COVID-19, Infodemics, and the Platformization of Truth*, 8 SOC. MEDIA + SOC'Y 1, 5 (2022).

200 CHO & ZHU, *supra* note 105, at 1; AD HOC COMMITTEE FOR 2024 ELECTION FAIRNESS AND LEGITIMACY, 24 FOR '24: URGENT RECOMMENDATIONS IN LAW, MEDIA, POLITICS, AND TECH FOR FAIR AND LEGITIMATE 2024 U.S. ELECTIONS 20 (September 2023), chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://law.ucla.edu/sites/default/files/PDFs/Safeguarding_Democracy/24_for_24-REPORT-FINAL.pdf [https://perma.cc/JLC5-FW35] [hereinafter 24 Recommendations].

201 24 Recommendations, *supra* note 200, at 20; Neil Vigdor, *Trump Promotes A.I. Images to Falsely Suggest Taylor Swift Endorsed Him*, N.Y. TIMES (Aug. 19, 2024), https://www.nytimes.com/2024/08/19/us/politics/trump-taylor-swift-ai-images.html [https://perma.cc/3EMF-HJCH]; NORA BENAVIDEZ, FREE PRESS, BIG TECH BACKSLIDE: HOW SOCIAL-MEDIA ROLLBACKS ENDANGER DEMOCRACY AHEAD OF THE 2024 ELECTIONS 3–5 (2023).

202 BENAVIDEZ, *supra* note 201, at 4; Sam Stockwell et al., *AI-Enabled Influence Operations: Safeguarding Future Elections*, *in* CENTRE FOR EMERGING TECHNOLOGY AND SECURITY 20–40 (2024).

203 Jordan Kraemer et al., *A Guide to Social Media Moderation Policies for the Post-Election Period*, TECH POLICY.PRESS (Nov. 2, 2024), https://www.techpolicy.press/a-guide-to-social-media-moderation-policies-for-the-post-election-period/ [https://perma.cc/2X87-Y667]; THE ELECTION INTEGRITY PARTNERSHIP, *supra* note 195, at 227 n.6.

checking, while X relied primarily on community notes.[204] Following President Trump's election, Meta discontinued its fact-checking program entirely in favor of a community notes system.[205]

As described above, platforms have demonstrated their willingness and ability to:

- Develop sophisticated content detection systems capable of identifying specific types of material among billions of posts,
- Deploy both algorithmic and human review mechanisms at a massive scale,
- Implement multi-tiered response systems from labeling to demotion to removal, and
- Continuously refine these systems in response to evolving challenges and stakeholder feedback.

If social media companies can build systems sophisticated enough to detect election misinformation—a far more contextual and nuanced determination than identifying unauthorized copies of registered works—they possess the technological capacity to address copyright infringement proactively. Platforms have adjusted their content moderation approaches as political winds have shifted. With appropriate legal incentives and obligations, social media companies could apply this same technological sophistication to copyright enforcement, protecting creators' exclusive rights with the same vigor they have demonstrated in addressing other forms of "problematic" content.

B. PUBLIC HEALTH IMPERATIVES: PLATFORMS' DEMONSTRATED ABILITY TO MODERATE

Sociologists, epidemiologists, and legal scholars will analyze the COVID-19 pandemic's causes and effects for decades. During this unprecedented global

---

[204] Mike Isaac & Theodore Schleifer, *Meta to End Fact-Checking Program in Shift Ahead of Trump Term*, N.Y. TIMES (Jan. 7, 2025), https://www.nytimes.com/2025/01/07/technology/meta-fact-checking-facebook.html [https://perma.cc/KH6W-4GGD]; Kate Conger, *Elon Musk Wants People on X to Police Election Posts. It's Not Working Well.*, N.Y. TIMES (July 25, 2024), https://www.nytimes.com/2024/07/25/technology/elon-musk-x-community-notes-election.html [https://perma.cc/4JBA-45SR].

[205] *Id.*

health crisis, social media platforms faced extraordinary challenges in managing the flood of information and misinformation on their services. Their response offers another compelling example of platforms' sophisticated content monitoring capabilities when adequately motivated by public pressure and regulatory concern.

Recognizing the dangers of false health information, the Director-General of the World Health Organization declared, "[W]e're not just fighting an epidemic; we're fighting an infodemic."[206] Companies employed various strategies and tools to fight the infodemic.[207] Facebook, Twitter, and YouTube are committed to removing content deemed harmful to public health.[208] When fact-checkers identified false or misleading posts, Facebook and Twitter applied warning labels directing users to authoritative information sources.[209] YouTube did not use warning labels; instead, they attached independent fact-check links for certain search queries; however, what prompted these links remained obscure.[210] Each major platform adjusted its algorithm to limit content identified as false, inaccurate, or misleading.[211] Twitter's tiered response system illustrates one example of how platforms choose to moderate content:

---

206 Cotter et. al, *supra* note 199, at 1.

207 Nandita Krishnan et al., *Examining How Various Social Media Platforms Have Responded to COVID-19 Misinformation*, 2 HARV. KENNEDY SCH. MISINFORMATION REV. 1, 1-2 (2021).

208 Cotter et. al, *supra* note 199, at 6.

209 *Id.* at 6–8.

210 *Id.* at 8 ("For example, if someone searches for 'did a tornado hit Los Angeles,' they might see a relevant fact check article, but if they search for a more general query like 'tornado,' they may not." (citing The YouTube Team, *Expanding fact checks on YouTube to the United States*, YOUTUBE OFFICIAL BLOG (Apr. 28, 2020), https://blog.youtube/news-and-events/expanding-fact-checks-on-youtube-to-united-states/ [https://perma.cc/HU8E-XL8C])).

211 *Id.* at 5.

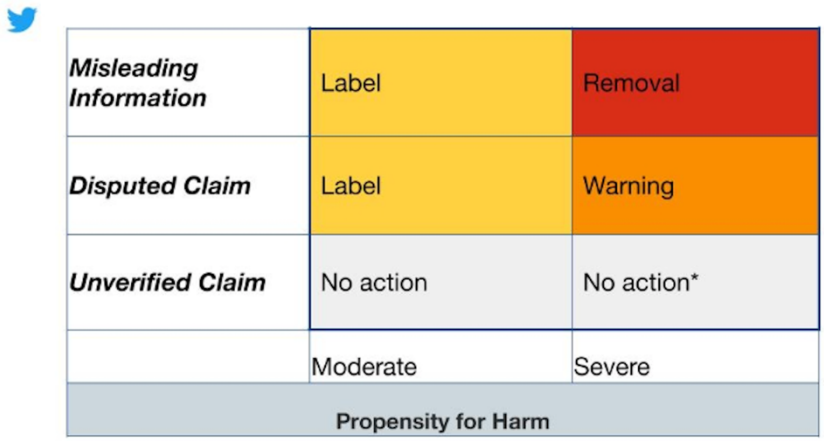

Figure 2. Twitter's Content Moderation Table. [212]

Other platforms implemented less rigorous moderation systems, highlighting the variance in approaches even when addressing critical public health concerns.[213]

John Locke—the British philosopher whose ideas fundamentally influenced the Declaration of Independence—argued that everyone is entitled to life, liberty, and property.[214] Yes, public health takes priority over intellectual property rights.[215] However, these rights are not at odds when combating digital infringement. If platforms can be trusted to safeguard our liberty during elections, and our health during pandemics, surely they can be trusted to defend our property when they seek to profit from it.

---

[212] *Id.*; Yoel Roth & Nick Pickles, *Updating Our Approach to Misleading Information*, X BLOG (May 11, 2020), https://blog.x.com/en_us/topics/product/2020/updating-our-approach-to-misleading-information [https://perma.cc/7XUR-5GDD]. On November 23, 2022, X stopped enforcing this COVID-19 misleading information policy.

[213] *See generally* Krishnan et al., *supra* note 207.

[214] Kenneth D. Stern, *John Locke and the Declaration of Independence*, 15 CLEV. MARSHALL L. REV. 186, 189 (1966); Brenee Goforth Swanzy, *How John Locke Influenced the Declaration of Independence*, JOHN LOCKE FOUND. (July 4, 2019), https://www.johnlocke.org/john-locke-and-the-declaration-of-independence/ [https://perma.cc/W2JV-UX55].

[215] Cordis Corp. v. Bos. Sci. Corp., 99 Fed. App'x. 928, 935 (Fed. Cir. 2004) ("Thus, for good reason, courts have refused to permanently enjoin [infringing] activities that would injure the public health." (citing Vitamin Tech., Inc. v. Wis. Alumni Res. Found., 146 F.2d 941, 944 (9th Cir. 1945)); City of Milwaukee v. Activated Sludge, 69 F.2d 577, 593 (7th Cir. 1934).

This observation is not about imposing unreasonable technical or economic burdens—platforms have already demonstrated these capabilities. Instead, it highlights a selective application of existing content monitoring technologies. The same algorithms that identify potentially misleading health claims could be deployed to identify unauthorized copies of creative works. The same tiered response systems developed for COVID-19 content—labeling, demonetization, limiting distribution, or removal—provide a proven framework that could be applied to copyright enforcement. The key missing element is not technological capability but rather the legal framework that would align platforms' practices with creators' rights.

C. CONSENSUS ENFORCEMENT: THE INFRASTRUCTURE FOR CONTENT CONTROL

Content moderation need not always be controversial. Nearly all Americans would agree that child sex abuse material, revenge pornography, and similarly harmful content have no legitimate place on any platform.[216] These broadly shared values demonstrate that effective content moderation can represent a social good rather than merely a limitation on expression.

Content that promotes or depicts self-harm, child abuse, harassment, bullying, and hate speech is moderated by all the major platforms.[217] These policies are not merely aspirational; platforms have developed sophisticated detection systems that combine algorithmic screening with human review to identify and remove violating content—often before it reaches public view.

---

[216] *See* Chandler Brindley, *MN Sen. Klobuchar, TX Sen. Cruz Celebrate U.S. Senate Passage of Take It Down Act*, WXOW.COM (Dec. 17, 2024), https://www.wxow.com/news/mn-sen-klobuchar-tx-sen-cruz-celebrate-u-s-senate-passage-of-take-it-down/article [https://perma.cc/7AAZ-DKBS]; *see also* Take It Down Act, S. 4569, 118th Cong. (2024).

[217] *Community Standards*, META, https://transparency.meta.com/policies/community-standards/ [https://perma.cc/B6DC-QWV8]; *Rules and Policies*, X HELP CENTER, https://help.x.com/en/rules-and-policies [https://perma.cc/28YH-CZMC]; *Community Guidelines*, YOUTUBE, https://www.youtube.com/howyoutubeworks/policies/community-guidelines/ [https://perma.cc/9CN3-W4GX] [hereinafter *Community Guidelines*, YOUTUBE]; *Community Guidelines*, TIKTOK (Apr. 17, 2024), https://www.tiktok.com/community-guidelines/en [https://perma.cc/8496-H2RF].

For example, Facebook reported removing 18.1 million pieces of content for violating its child nudity and sexual exploitation policies in a single quarter of 2023, with 99.1% of this content detected proactively before any user reported it.[218] Similarly, through mostly automated processes, YouTube removed 158,480 channels and 6,847,361 videos for child safety violations in the same period.[219] Prohibited content is vast; too vast for 1998 service providers to control. Yet, modern social media companies combat this obscene content with powerful automated content detection and removal systems, which have equal applicability to mitigating copyright infringement.

The effectiveness of these enforcement mechanisms relies on a combination of technologies, like those needed for copyright protection:

- Hash matching: Platforms maintain databases of known prohibited content and automatically block uploads that match these digital fingerprints—functionally identical to YouTube's Content ID system for copyright protection.[220]

- Machine learning classification: AI systems trained to recognize patterns indicative of prohibited content can flag potential violations for review—the same approach that could identify unauthorized use of copyrighted works.[221]

---

218 *Child Endangerment: Nudity and Physical Abuse and Sexual Exploitation*, META TRANSPARENCY CENTER, https://transparency.meta.com/reports/community-standards-enforcement/child-nudity-and-sexual-exploitation/facebook/ [https://perma.cc/MDT4-BPCX].

219 *YouTube Community Guidelines Enforcement*, GOOGLE TRANSPARENCY REPORT, https://transparencyreport.google.com/youtube-policy/removals [https://perma.cc/7S3T-8PVN].

220 *See How Technology Detects Violations*, META TRANSPARENCY CENTER (Oct. 18, 2023), https://transparency.meta.com/enforcement/detecting-violations/technology-detects-violations/ [https://perma.cc/QZV7-YABJ]; Hanif, *supra* note 190.

221 *See* Robert Gorwa et al., *Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance*, BIG DATA & SOC'Y, Jan.–June 2020, at 9–10 (citing examples of how Facebook and YouTube use machine learning algorithms to automatically flag potentially violating content, such as hate speech).

- Automated removal: When high-confidence matches are found, content can be automatically removed without human review—a capability directly applicable to clear copyright infringement cases.[222]

Whether modern content moderation practices are theoretically justified is not a question this Article answers. Regardless, modern social media platforms are willing and capable of moderating content at mammoth-like scales through automated processes when it serves the platforms' interests. The vastness of user-posted content has driven the development of sophisticated automated processes to detect and address violating content—methods that could be equally applied to copyright enforcement.[223]

If platforms can proactively deploy advanced AI systems to identify and remove content that violates community standards, they can apply similar technologies to protect creators' exclusive rights. The necessary tools are not theoretical—they exist and operate daily across these platforms.[224] What's missing is not technological capability but a legal framework that aligns platforms' content moderation practices with consideration for copyright holders.

V. THE ANTIVENOM SOLUTION: MODERNIZING COPYRIGHT ENFORCEMENT FOR THE AI ERA

History repeats itself, even in the digital realm. As President Clinton's Information Infrastructure Task Force warned in 1995, "We are once again faced with significant changes in technology that upset the balance that currently exists under the Copyright Act."[225] Almost three decades later, copyright owners face even greater changes. AI makes the 1998 Internet unrecognizable. Still, the DMCA regulates the AI Internet. However, unlike the Internet, AI can also be a shield.

The evidence presented in previous Parts reveals a stark reality: today's social media platforms bear little resemblance to the passive intermediaries the DMCA was designed to protect. Today's companies deploy sophisticated AI algorithms to curate content, scrape user data to train generative models, and selectively moderate material when motivated. Despite possessing technological capabilities that would have seemed like science fiction to the DMCA's drafters, these platforms continue to enjoy safe harbor protections designed for passive bulletin boards of the 1990s.

---

222 *See* CHO & ZHU, *supra* note 105, at 13.

223 *See* Gorwa et al., *supra* note 221, at 2.

224 *See, e.g.*, *Community Guidelines*, YOUTUBE, *supra* note 217.

225 Lehman, *supra* note 21, at 14.

This Part argues that AI must serve as a shield for copyright in the digital age. Just as venom is essential in creating lifesaving antivenom, the technologies that threaten to undermine copyright protection—AI-powered content curation, recognition, and moderation—should be harnessed to protect creators' exclusive rights. This approach maintains the DMCA's original goal of balancing innovation and intellectual property protection while acknowledging the radically transformed technological landscape.

The following Sections will examine why the DMCA's original justifications no longer apply in the AI era, why social media providers that benefit from AI should have an affirmative duty to police infringement, and how a reformed legal framework could transform AI from copyright's greatest threat into its most impenetrable protector.

A. OBSOLETE ASSUMPTIONS: WHY THE DMCA'S JUSTIFICATIONS NO LONGER APPLY

Social media platforms have undergone a profound transformation since 1998. However, online service provider regulations and safe harbors remain frozen in time. The DMCA may have been justified when dial-up connections and AOL dominated the Internet landscape. Still, today's digital ecosystem bears little resemblance to that era—social media as we know it did not even exist when the DMCA was drafted.[226] Yet, as is often the case, the law has failed to keep pace with technological evolution. The safe harbors designed for digital canoes now shield massive cruise liners. Once-passive intermediaries have now metamorphosed into sophisticated algorithmic platforms that actively curate, promote, and monetize content to maximize user engagement. Unless Congress and courts adapt to this new reality, creators and authors will continue trading their constitutionally guaranteed exclusive rights for a lifetime of unpaid enforcement duties.

The DMCA's safe harbor provisions were primarily justified by the need to nurture electronic commerce without subjecting online service providers to crushing liability for contributory copyright infringement.[227] By this measure, the DMCA succeeded spectacularly. In the fourth quarter of 1999, e-commerce sales totaled a modest $5.3 billion, representing roughly 0.64% of total retail sales.[228] By

---

[226] *See* Asha Velay, *Using the First Fair Use Factor to Screen DMCA Takedowns*, 17 VA. SPORTS & ENT. L.J. 54, 59–60 (2017).

[227] *See* H.R. REP. NO. 105-551, pt. 2, at 21 (1998).

[228] *Retail E-Commerce Sales for Fourth Quarter 1999 Reach $5.3 Billion, Census Bureau Reports*, U.S. DEP'T OF COMMERCE (Mar 2, 2000),

the fourth quarter of 2024, these figures had exploded to $308.9 billion, constituting approximately 16.4% of total sales.[229] Annual e-commerce sales now approach $1.2 trillion—nearly 60 times larger than in 1999.[230]

This remarkable growth demonstrates that electronic commerce no longer requires special legal protection to flourish. However, as electronic commerce has expanded, so have the burdens placed on copyright owners. The proliferation of social media platforms and the exponential increase in user-generated content have inevitably led to more widespread infringement.[231] Copyright owners must now hire specialized third-party enforcement organizations to implement the DMCA's notice-and-takedown procedures, forcing them to pay to combat lost sales from pirated content; yet, platforms profit regardless of the enforcement effectiveness.[232] While platform revenues soar, copyright owners' enforcement costs have escalated. The DMCA no longer maintains a balanced approach; it imposes a disproportionate burden on creators.

The DMCA deliberately placed the infringement identification burden on copyright holders to avoid overwhelming service providers with review requirements.[233] However, this justification has been rendered obsolete by technological advances. Today's platforms no longer need to review every user post manually; AI can perform that function nearly instantaneously.[234] Moreover, these detection systems would only improve if platforms faced liability for algorithmically promoting infringing content.[235] Confronted with potential liability for false negatives and user frustration from false positives, platforms

---

https://www2.census.gov/retail/releases/historical/ecomm/99q4.pdf [https://perma.cc/RB45-WLBW].

229 *Quarterly Retail E-Commerce Sales 4th Quarter 2024*, U.S. DEP'T OF COMMERCE (Feb. 19, 2025), https://www2.census.gov/retail/releases/historical/ecomm/24q4.pdf [https://perma.cc/X8SQ-QY6T].

230 *Id.* at 1.

231 Garry A. Gabison & Miriam C. Buiten, *Platform Liability in Copyright Enforcement*, 21 COLUM. SCI. & TECH. L. REV. 237, 264 (2020).

232 *Id.* at 256.

233 *See* 17 U.S.C. § 512(c)(3); *see also* S. REP. NO. 105-190, at 45–47 (1998).

234 *See Video Sound Copyright Check Before Posting*, *supra* note 191 (describing how TikTok presents users the option to use AI to detect infringing audio before uploading a video).

235 *See* Gabison & Buiten, *supra* note 231, at 259.

would quickly develop more sophisticated copyright detection AI to protect their market position.[236]

The pace of AI innovation underscores this potential. ChatGPT released its first large language model to the public in late 2022.[237] By April 2025, it had already advanced to model 4-o.[238] If improved copyright detection tools could reduce liability and increase revenue, platforms would undoubtedly invest in their development. The same technological revolution that produced DALL-E, ChatGPT, Gemini, LLaMa, Claude, and DeepSeek is more than capable of creating AI systems to detect and prevent copyright infringement before it spreads through personalization algorithms.

Under current case law, however, platforms have no incentive to aid in enforcement. *Viacom International, Inc. v. YouTube, Inc.* vividly illustrates this problem. There, the copyright owner presented the following damning evidence:

- YouTube's director of video partnerships requested that "clearly infringing, official broadcast footage" be removed before meeting with Premier League owners to discuss broadcast rights. Once YouTube decided against bidding for those rights, the infringing videos remained on the platform.[239]

- One YouTube founder acknowledged awareness of "episodes and clips" on the platform—some owned by the plaintiff—describing them as "blatantly illegal."[240]

- YouTube's founders knew about infringing commercials and space shuttle footage pirated from CNN, with one founder urging colleagues not to remove the content until receiving a cease-and-desist letter, which would likely take two weeks.[241]

- YouTube strategically decided "to keep substantially all infringing videos on the site as a draw to users, unless and until YouTube received a

---

236 *See id.*

237 Metz, *OpenAI Unveils New Image Generator*, *supra* note 178.

238 *Id.*

239 *2d Cir. Viacom Int'l*, 676 F.3d 19, 33 (2d Cir. 2012).

240 *Id.*

241 *Id.* at 34.

'takedown notice' from the actual copyright owner identifying a specific infringing clip by URL and demanding its removal from the site."[242]

Despite that evidence, YouTube received safe harbor protection on remand from the Second Circuit because it lacked "sufficient knowledge of the specific clips in suit," could not "control the infringement," and made copies of infringing material only through automated processes "to make stored videos more readily accessible."[243] The Ninth Circuit has adopted a similar approach. In *Davis v. Pinterest, Inc.*, even though Pinterest's algorithm promoted one plaintiff's copyrighted work 4,676 times alongside paid advertisements within just two weeks, the platform avoided liability because it did not induce users to upload infringing material; further, Pinterest's profit from the infringement did not disqualify it from safe harbor protection.[244] As the court noted, their hands were tied; "Congress, not [the 9th Circuit], decided as a policy matter who should bear the burden of identifying infringement in the first instance."[245]

Congress did not merely make copyright owners the sole enforcement authority; it actively discouraged platforms from assisting in policing efforts. This perverse incentive is evident in the Ninth Circuit's ruling in *Mavrix Photographs, LLC v. Livejournal, Inc.*, where human agents reviewing content before publication could cause a platform to lose safe harbor protection.[246] This "hear no evil, see no evil" approach contradicts the collaborative enforcement model Congress claimed to promote when passing the DMCA.[247] Furthermore, it creates the legal fiction

---

242 *2013 Viacom Int'l*, 940 F. Supp. 2d 110, 119 (S.D.N.Y. 2013) (internal citations omitted).

243 *Id.* at 113–23.

244 Davis v. Pinterest, Inc., 601 F. Supp. 3d 514, 521, 531-36 (N.D. Cal. 2022), *aff'd*, No. 22-15804, 2023 WL 5695992 at *1–2 (9th Cir. Sep. 5, 2023) (memorandum opinion).

245 *Id.* at 531.

246 *See generally* Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045 (9th Cir. 2017) (holding that human agents may cause a platform to have actual or "red flag" knowledge of infringing content, which would disqualify safe harbor protection).

247 *See* S. REP. NO. 105-190, at 8 ("Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy."); *see also* H.R. REP. NO. 105-796, at 72 (1998) (Conf. Rep.) ("Title II preserves strong incentives for service providers and copyright owners to

that platforms control human agents more than they control proprietary automated algorithms that form the core business assets of these companies.

The DMCA must be updated or reinterpreted to address the modern Internet landscape. Courts have consistently held that social media providers can automate the promotion of infringing content without liability.[248] Copyright owners face an endless avalanche of notice and takedown requirements as algorithms increase their ability to disseminate infringing content instantly to thousands, if not millions, of users. This Congressional compromise was designed for passive hosts, not automated publishing machines. Today's copyright owners confront outdated enforcement mechanisms while platforms operate largely unconstrained by intellectual property concerns thanks to increasingly anachronistic safe harbor protections. This negative feedback loop can only be resolved by requiring platforms to employ the same powerful AI technologies driving their personalization algorithms and large language models to detect and prevent copyright infringement.

B. A DUTY TO PROTECT: WHY AI-POWERED PLATFORMS MUST POLICE INFRINGEMENT

Those who can, do; those who cannot . . . should be granted safe harbor. Safe harbors remain essential for nascent online service providers who lack AI capabilities for content curation or moderation. However, platforms that deploy AI-powered personalization algorithms or scrape user data to train large language models can no longer reasonably claim the status of passive intermediaries—because they are demonstrably active participants in content distribution. Analogous to affirmative duties in tort law, where only those capable of acting bear any responsibility, only those capable of deploying AI should be expected to help combat infringement.[249] This framework appropriately protects creators' interests while simultaneously allowing startup platforms to innovate without fear of crushing liability.

---

cooperate to detect and deal with copyright infringements that take place in the digital networked environment.").

248 *See supra* Section II.B.

249 *See* Francis H. Bohlen, *Moral Duty to Aid Others as a Basis of Tort Liability*, 56 U. PA. L. REV. & AM. L. REG. 217, 219 (1908).

1. *Responsibility Through Action: Lessons from Tort Law's Affirmative Duties*

Generally, tort law imposes no duty to act;[250] however, specific duties may arise from certain conduct or special relationships.[251] These established exceptions provide a helpful framework for reconsidering platform responsibilities in the AI era. Tort law recognizes five primary categories of affirmative duties:

First, special relationships between one party and a victim, particularly where the victim depends on the first party, create duties of care.[252] Examples include "common carrier-passenger, innkeeper-guest, employer-employee, and school-student" relationships.[253]

Second, parties that voluntarily assist a victim assume a duty of reasonable care.[254] The assisting party must not leave the victim worse off through the victim's reliance on voluntary care.[255] This resembles a trust fall exercise: one person's commitment to catch another creates a responsibility to follow through.

Third, parties whose acts create dangerous risks to potential victims bear a duty to act.[256] Even when initial actions are not foreseeably risky, once an actor knows or should know that their actions create risk, they must exercise reasonable care to prevent injury.[257] The Restatement (Second) of Torts illustrates this principle with a golfer who, after hitting a ball toward what appeared to be an empty area, must warn someone who unexpectedly appears in the ball's path.[258]

Fourth, parties whose actions—tortious or innocent—harm a victim must prevent further injury.[259] If someone inadvertently serves poisoned wine to a

---

250 RESTATEMENT (SECOND) OF TORTS § 314 (AM. L. INST. 1965) ("The fact that the actor realizes or should realize that action on his part is necessary for another's aid or protection does not of itself impose upon him a duty to take such action.").

251 KENNETH S. ABRAHAM, FORMS AND FUNCTIONS OF TORT LAW 260 (5th ed. 2017).

252 Kenneth S. Abraham & Leslie Kendrick, *There's No Such Thing as Affirmative Duty*, 104 IOWA L. REV. 1649, 1655 (2019).

253 *Id.*

254 *Id.* at 1656.

255 *Id.*

256 *See* RESTATEMENT (SECOND) OF TORTS § 321.

257 *Id.*

258 *Id.*

259 *Id.* § 322.

friend, believing it safe, they must "exercise reasonable care" to minimize the illness and seek medical assistance.[260]

Fifth, statutory mandates can create affirmative duties,[261] such as drivers' obligation to aid accident victims (no hit-and-run statutes), adults' duty to report child abuse, and "easy rescue" laws requiring citizens to help others in peril when it poses no personal danger.[262] This list is not exhaustive but provides helpful insights for social media companies, end-users, and copyright owners.[263]

2. *Platform Accountability: Applying Affirmative Duties to Social Media*

Under the DMCA's current safe harbor framework, online service providers receive broad immunity from copyright liability.[264] However, using tort law principles as an analogy reveals why sophisticated AI-deploying platforms should bear greater responsibility.[265]

Under the special relationship exception, social media platforms resemble common carriers in providing shared communication infrastructure and implementing safety measures for democratic and public health concerns. However, this duty might not extend to copyright enforcement, since infringement harms content owners rather than platform users. Similarly, platforms' voluntary content moderation efforts might not create duties to copyright owners specifically, as these systems primarily protect users rather than creators.

The third exception—creating a dangerous environment—provides a stronger basis for platform liability. Social media platforms are specifically designed to maximize content dissemination and user engagement. The DMCA

---

260 *See id.*

261 Jennifer L. Groninger, *No Duty to Rescue: Can Americans Really Leave a Victim Lying in the Street? What Is Left of the American Rule, and Will It Survive Unabated?*, 26 PEPP. L. REV. 353, 367 (1999).

262 *Id.* at 367–69.

263 For a more thorough picture of affirmative duties to act, see generally *id.*; Abraham & Kendrick, *supra* note 252; Nancy Levit, *Kindness of Strangers: Interdisciplinary Foundations of a Duty to Act*, 40 WASHBURN L.J. 463 (2001); McCall C. Carter, *Morality, Law and the Duty to Act: Creating a Common Law Duty to Act Modeled After the Responsibility to Protect Doctrine*, 2 WASH. U. JURIS. REV. 138 (2010).

264 *See* 17 U.S.C. § 512(c).

265 *See supra* Parts III & IV.

recognized that user-driven content sharing inevitably creates copyright infringement, even if not intentionally promoted.[266] As platforms have expanded their reach, they have correspondingly increased the volume of infringing uploads.[267] Since this growth creates a perilous environment for copyright owners, platforms should bear reasonable responsibility for preventing infringement.

Viacom vividly illustrates this principle. There, YouTube knew about the widespread infringement but faced no duty to mitigate or prevent further violations without specific copyright owner intervention.[268] Under affirmative duty principles, this knowledge would trigger responsibility to address the danger that YouTube's service created.

The fourth exception—preventing further harm from innocent actions—applies directly to cases like *Davis*. When Pinterest learned that its algorithm had promoted the plaintiff's copyrighted works over 4,000 times alongside paid advertisements,[269] the platform should have assumed responsibility for halting infringements caused by its proprietary system, rather than profiting mindlessly.

Finally, and most crucially, Congress should impose a statutory duty on AI-utilizing social media platforms to ensure their algorithms do not amplify copyright infringement beyond initial user posts. Platforms deploying any AI capabilities should be required to apply those same technologies to detect and remove copyright-infringing content.

3. *Platforms' Responsibility: Balancing Innovators' and Creators' Rights*

Importantly, platforms undertaking copyright enforcement warrant appropriate safe harbor protection for reasonable errors. Like "Good Samaritan" laws that shield those who aid injured victims from tort liability,[270] a reformed DMCA should protect platforms making "reasonable" efforts to enforce copyright,

---

266 *See* S. REP. NO. 105-190, at 20 ("Title II preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment. At the same time, it provides greater certainty to service providers concerning their legal exposure for infringements that may occur [online].").

267 *See* Gabison & Buiten, *supra* note 231, at 264.

268 *2d Cir. Viacom Int'l*, 676 F.3d 19, 33 (2d Cir. 2012); *2013 Viacom Int'l*, 940 F. Supp. 2d 110, 113–123 (S.D.N.Y. 2013).

269 Davis v. Pinterest, Inc., 601 F. Supp. 3d 514, 520–21, 536 (N.D. Cal. 2022), *aff'd*, No. 22-15804, 2023 WL 5695992 (9th Cir. Sep. 5, 2023) (memorandum opinion).

270 Levit, *supra* note 263, at 466–67.

even when these efforts occasionally under- or over-enforce. Given the acknowledged complexity of the fair use doctrine[271] and the inevitable imperfections of newly deployed AI detection tools, this balanced approach would encourage platforms to develop robust enforcement mechanisms without fearing liability for good-faith mistakes.

This framework recognizes that different platforms possess different capabilities. Startups lacking AI infrastructure remain appropriate candidates for traditional safe harbor protection. However, sophisticated platforms that leverage AI for content curation and monetization should bear sophisticated responsibilities to deploy these technologies for copyright protection—the result: a more equitable digital ecosystem that protects innovators' and creators' rights.

C. ANTIVENOM: A MANDATE FOR TECHNOLOGY-ENABLED COPYRIGHT ENFORCEMENT

If I have seen further, it is by standing on the shoulders of giants.
— Sir Isaac Newton

To see beyond the DMCA's outdated framework, we must follow the path illuminated by Francesco Redi, Henry Sewall, and Dr. Albert Calmette. These pioneering scientists taught us the fundamental process for creating antivenom: identify the poison, understand its mechanisms, and transform it into a remedy.[272] Alan Turing theorized about AI.[273] Social media providers have harnessed AI to personalize content, train large language models, and maximize user engagement.[274] Instead of allowing AI to remain copyright's most potent venom, we must convert it into creators' most effective antidote. If AI can curate content with laser precision, answer any prompt by drawing on Internet-wide data, and recognize patterns across billions of interactions, it can detect and remove copyright infringement on social media platforms.

---

271 *See, e.g.*, Tess Toland, *What Is Fair?: Why Fair Use Should Be Reevaluated as a Defense to Copyright Infringement*, 52 AM. INTELL. PROP. L. ASSOC. Q.J. 143, 145–47 (2024) ("[I]t is often impossible to predict how a particular [fair use] matter will turn out.").

272 *Supra* notes 5–10 and accompanying text.

273 B.J. Copeland, *History of Artificial Intelligence (AI)*, ENCYC. BRITANNICA (July 30, 2025), https://www.britannica.com/science/history-of-artificial-intelligence [https://perma.cc/QAB9-L9G5].

274 CHO & ZHU, *supra* note 105, at 3, 10–11; *supra* notes 160–168 and accompanying text.

1. *AntIvenom: A Model for Automated Copyright Protection*

Consider a sophisticated AI model we might call AntIvenom. This system would be trained on every registered copyright in the U.S. Copyright Office database, supplemented with comprehensive copyright case law covering a wide range of topics, from DMCA safe harbor provisions to emerging AI fair use precedents. Social media platforms would deploy AntIvenom to screen all user-posted content for potential infringement systematically.

AntIvenom could automatically remove the content and notify the posting user with a detailed explanation of the removal grounds for obvious cases of verbatim copying or clear infringement. For more nuanced situations—where fair use considerations or free speech protections create ambiguity—AntIvenom could flag the content for platform review, preventing its algorithmic promotion or monetization until human assessment confirms its legality.

The system could incorporate user verification of copyright ownership or licensing rights. Users could upload proof of copyright ownership or licensing to balance aggressive enforcement with authorized publishing. Thus, AntIvenom could distinguish between legitimate and infringing uses.

AntIvenom represents not a technological pipe dream but a natural evolution of platforms' capabilities. AI has demonstrated far more complex capabilities than copyright recognition. The absence of such systems stems not from technical impossibility but from the lack of legal incentives under the current DMCA framework. Congress and the courts must create these incentives to develop the antidote to digital copyright infringement.

2. *Judicial Pathways: Reinterpreting the DMCA for the AI Era*

Though admittedly challenging given the current judicial consensus, one potential approach would involve reinterpreting existing DMCA safe harbor provisions. Under § 512(c)(1), service providers avoid liability "for infringement of copyright by reason of the storage *at the direction of a user* of material that resides on a system or network controlled or operated by or for the service provider."[275] When social media algorithms actively promote infringing content to non-uploading users, this material no longer exists on the network solely "at the direction of a user"; the platform's proprietary algorithm determines its new virtual location.

Additionally, as *Davis* noted, "Section 512(c) is unavailable to a service provider where 'the service provider has the right and ability to control

[275] 17 U.S.C. § 512(c)(1) (emphasis added).

[infringing] activity.'"[276] Courts have consistently declined to hold platforms liable when their algorithms promote user-uploaded infringing content,[277] recognizing the platforms' control over algorithmic distribution but not the initial upload.[278] By reinterpreting "control [of] infringing activity" to encompass the promotion of infringing content—not merely the initial upload—courts could establish an affirmative duty for personalization algorithms to mitigate the effects of copyright infringement.

This interpretation aligns with the principles of affirmative duty in tort law. Since personalization algorithms demonstrably increase the harmful exposure of infringing works, the platforms that perfect these algorithms should reasonably bear responsibility for mitigating unauthorized distribution. Moreover, these algorithms represent platforms' primary revenue generators.[279] Under safe harbor provisions, providers cannot "receive a financial benefit directly attributable to the infringing activity."[280] Personalization algorithms that promote engagement by generating infringing content alongside advertisements create precisely such benefits.

Further, under § 512(a)(3), providers avoid liability for transmitting infringing content when "the service provider does not select the recipients of the material except as an automatic response to the request of another person."[281] When algorithms promote infringing content to non-uploading users, this distribution occurs not at the original uploader's behest but in service of the platform's advertising revenue.[282] The algorithm's automatic execution does not

---

276 Davis v. Pinterest, Inc., 601 F. Supp. 3d 514, 534 (N.D. Cal. 2022), *aff'd*, No. 22-15804, 2023 WL 5695992 (9th Cir. Sep. 5, 2023) (memorandum opinion) (citing 17 U.S.C. § 512(c)(1)(B)).

277 *See id.* at 534–35.

278 *See id.* at 518–20.

279 *See supra* notes 112–116 and accompanying text.

280 17 U.S.C. § 512(c)(1)(B).

281 *Id.* § 512(a)(3).

282 *See Davis*, 601 F. Supp. 3d at 530–31 ("In other words, rather than notify Pinterest of alleged copyright infringement on its platform so Pinterest can remove it, Plaintiff wants Pinterest to continue to display his images on its website and mobile application, but he does not want Pinterest to profit in any way from doing so."). The algorithms transmit this content from one user's personal feed to another user's "For You" feed, or platform equivalent. *See id.* at 519–20.

absolve the platform's responsibility for programming it to transmit infringing content, exponentially compounding injury to copyright owners.

Considering the circuit court's consistent application of the safe harbor provisions, reinterpretation faces significant challenges.[283] A comprehensive legislative amendment provides a clearer path forward.

3. *Legislative Imperatives: Amending the DMCA for the AI Era*

Congress should enact legislation denying safe harbor protections to social media platforms that deploy AI for content personalization or data scraping without corresponding copyright protection efforts. This reform could be accomplished through straightforward additions to § 512:

> No online service provider that utilizes AI to promote online advertisements or other material made available online by a person other than the service provider shall be entitled to the protections under subsection (c)(1).
>
> No online service provider that utilizes material posted by persons other than the online service provider on the service provider's platform to train an AI model that is
>
> (1) owned by the online service provider, or
>
> (2) owned by a person or persons that is not the online service provider, but acquired the material from the online service provider through sale or voluntary relinquishment
>
> shall be entitled to the protections under subsection (c)(1).

These statutory additions require definitions of previously novel DMCA terms like "AI" and "train." Congress has already defined AI as:

---

[283] *Cf. 2d Cir. Viacom Int'l*, 676 F.3d 19 (2d Cir. 2012); Davis v. Pinterest, Inc., 601 F. Supp. 3d 514 (N.D. Cal. 2022), *aff'd*, No. 22-15804, 2023 WL 5695992 (9th Cir. Sep. 5, 2023) (memorandum opinion); BWP Media USA, Inc. v. Clarity Digit. Grp., LLC, 820 F.3d 1175, 1181 (10th Cir. 2016) ("[I]f the infringing content has merely gone through [an] automated process, the ISP will generally benefit from the safe harbor's protection."); CoStar Grp., Inc. v. LoopNet, Inc., 373 F.3d 544, 555 (4th Cir. 2004) ("[A]utomatic copying, storage, and transmission of copyrighted materials, when instigated by others, does not render an ISP strictly liable for copyright infringement.").

> a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine and human-based inputs to—
>
> (A) perceive real and virtual environments;
>
> (B) abstract such perceptions into models through analysis in an automated manner; and
>
> (C) use model inference to formulate options for information or action.[284]

"Train" could be newly defined as:

> The process of systematically feeding data into an AI system to enable the model to recognize patterns, improve its ability to generate responses, and/or enhance its understanding of language through iterative learning and adjustment of its underlying algorithms. This process may include, but is not limited to, data collection, data preprocessing, model optimization, validation, and fine-tuning to improve accuracy and performance.

Such an amended DMCA would establish affirmative duties on AI-powered social media providers. For example, consider Instagram employing AI algorithms to curate personalized "Reels" feeds for its two billion users.[285] When Instagram's proprietary algorithm promotes user-uploaded content, including copyrighted photographs, videos, or music, to non-uploading users, the platform will not qualify for § 512(c) safe harbor protection under the amendment. The first proposed amendment would apply because Instagram "utilizes AI to promote online advertisements or other material made available online by a person other than the service provider." Similarly, if Instagram scrapes user-posted content to train Meta's LLaMa generative AI model—such as using posted photographs to develop image recognition systems or written captions to enhance natural language processing capabilities—the second proposed amendment would disqualify the platform from safe harbor protection, as it "utilizes material posted

---

[284] 15 U.S.C. § 9401(3).

[285] *Instagram Statistics: Key Demographics and User Numbers*, BACKLINKO (Mar. 11, 2025), https://backlinko.com/instagram-users [https://perma.cc/Y7U5-99TD].

by persons other than the online service provider on the service provider's platform to train an AI model."

This statutory framework creates clear incentives for responsible platform behavior. Social media companies would face a straightforward choice: either deploy AI capabilities while accepting affirmative duties to protect copyright or maintain traditional passive intermediary status with corresponding § 512 protections.[286] Platforms like YouTube, which already possess sophisticated Content ID systems capable of detecting copyrighted material,[287] would need to apply these technologies proactively rather than selectively. Those choosing to remain truly passive—eschewing AI-powered content curation and deep learning—would maintain their current safe harbor protections. This balanced approach preserves the DMCA's original intent to protect nascent internet businesses while acknowledging that sophisticated AI-powered social media platforms have evolved far past the passive intermediaries Congress shielded in 1998.[288]

Congressional action is imperative. Beyond partisan considerations, the Constitution's Article I, Section 8, Clause 8 exists to "secur[e] for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries"—not to foster electronic commerce at creators' expense.[289] The time has come to restore balance to copyright protection in the digital age by harnessing AI's power to defend the rights it threatens.

VI. CONCLUSION: HARNESSING AI TO RESTORE COPYRIGHT'S CONSTITUTIONAL PURPOSE

The DMCA will forever be lauded for allowing the Internet to blossom into an electronic commerce titan. However, it has failed to protect copyright

---

286 *See supra* notes 249–263 and accompanying text (discussing affirmative duties from tort law principles).

287 *See supra* notes 188–192 and accompanying text (describing YouTube's Content ID system).

288 *See supra* notes 74-95 and accompanying text (discussing DMCA's original justifications); S. REP. NO. 105-190, at 8 (describing Congressional intent to promote electronic commerce).

289 U.S. CONST. art. I, § 8, cl. 8; *see also* THE FEDERALIST NO. 43 (James Madison) ("The utility of this power will scarcely be questioned. The copyright of authors has been solemnly adjudged, in Great Britain, to be a right at common law. . . . The public good fully coincides in both cases, with the claims of [the authors].").

owners almost three decades later. To be sure, it was not drafted to tackle the problems that arise in the AI era. Gone are the days of passive intermediaries and conduits of information; today's platforms promote, curate, detect, and moderate content for user enjoyment and commercial profit.

These technological advances demand a corresponding evolution in copyright protection frameworks. As AI becomes increasingly powerful—creating unprecedented threats to intellectual property and novel content recognition capabilities—copyright law should harness these technologies as protective mechanisms. Congress could restore the balance between innovation and intellectual property rights by requiring social media platforms to proactively deploy their AI capabilities to detect and prevent copyright infringement.

Like extracting venom to create lifesaving antivenom, using AI for proactive copyright enforcement represents a natural application of existing technologies to solve the problems they create. This approach honors the DMCA's original intent—enabling digital marketplace growth without undermining creators' exclusive rights—while acknowledging the radically transformed technological environment.

Amending the DMCA acknowledges the reality of twenty-first-century technological advancement and the substantial market power now wielded by social media platforms. Considering their economic advantage, social media companies must filter out infringing content before it can be monetized or distributed through personalized algorithms to effectuate the promises of copyright law, including the DMCA.

The proposal outlined in this Article—requiring companies that utilize AI tools for profit to employ these same technologies for copyright protection—represents not a radical departure but a logical application of established principles. In tort law, those who create risk bear responsibility for minimizing resulting harm. Thus, social media companies that profit from platforms that create riskier environments—using automated dissemination tools to personalize user experiences or scrape user data for LLM training—for copyrighted works should shoulder the burden of detecting and mitigating the infringement. The proposed amendments pair existing AI capabilities with common law affirmative duties. By rebalancing the DMCA, the amendments restore an equitable legal environment for copyright owners who are overwhelmed by innovative technology that was not anticipated in 1998.

AI is copyright's greatest threat and its most likely savior. Congress must establish effective copyright protections that will serve creators, platforms, and the public interest for decades—or at least until the next technological revolution demands further adaptation of our intellectual property frameworks.