UC DAVIS LAW REVIEW

VOL. 58, NO. 4 APRIL 2025

Infringing Information Architectures

Michael P. Goodyear[*]

Information architectures — systems that facilitate storing and sharing data and content — underpin daily life, from streaming sites like Netflix and

 Acting Assistant Professor, New York University School of Law. J.D., University of Michigan Law School; B.A., University of Chicago. I am grateful to the following for helpful comments and conversations on earlier drafts: Amy Adler, Lori Andrews, Anna Arons, Mark Bartholomew, Barton Beebe, Richard Chused, Eric Claeys, Kevin Collins, Haiyun Damon-Feng, Dan Deacon, Graeme Dinwoodie, Rochelle Dreyfuss, John Duffy, Jeannie Fromer, Brian Frye, Andrew Gilden, Jane Ginsburg, James Grimmelmann, David Hannon, Jim Hathaway, Daniel Hemel, Scott Hemphill, Rob Heverly, Laura Heymann, Chris Holman, Aldona Kapačinskaitė, Sonia Katyal, Joshua Kresh, Will Danielson Lanier, Mark Lemley, Erika Lietzan, Elise Bernlohr Maizel, Jacob Noti-Victor, Fidelice Opany, Isaac Park, Adam Pritchard, Michael Risch, Nathan Rouse, Jason Schultz, Mark Schultz, Nicola Searle, Sepehr Shahshahani, Michal Shur-Ofry, Jessica Silbey, David Simon, Ben Sobel, Chris Sprigman, Kathy Strandburg, Rebecca Tushnet, Saurabh Vishnubhakat, Chris Whitman, Fred Yen, Kenji Yoshino, and participants in the Thomas Edison Innovation Law and Policy Fellowship workshops, AALS Intellectual Property Emerging Scholars Panel, Fourteenth Annual Tri-State Region IP Workshop, NYU Privacy Research Group, NYU Lawyering Scholarship Colloquium, Regulating the Decentralised Autonomous Organisation Conference, and Eleventh Annual Governance of Emerging Technologies and Science Conference, as well as presentations at the NYU Engelberg Center and Columbia Law School. I would also like to thank the editors of the UC Davis Law Review. The research and writing of this paper was supported by the Thomas Edison Innovation

Hulu to social media platforms like Instagram and TikTok. Since the printing press, these systems and their novel features have challenged the bounds of copyright law, leading to accusations that providers and users directly infringe others' copyrights. Almost fifty years ago, however, a largely unexplored paradigm shift occurred. Copyright owners started to allege that information architecture providers should be broadly secondarily liable for all their users' infringements. These claims, which this Article terms architectural infringement claims, pose an acute challenge to the balance copyright law strives to achieve between protecting authors' rights and providing access to their works. Overbroad protection and up to $150,000 in damages per infringement risk stymying innovation while reduced rights threaten copyright's incentive to create. Scholars have recognized this challenge in individual cases but have not identified the overarching challenges of architectural infringement claims or offered a framework for addressing them.

By examining architectural infringement claims systematically for the first time, this Article surfaces courts and Congress' use of intent as a hidden polestar for refining copyright secondary liability doctrine in response to these claims. Here, intent refers to an actor's action or inaction, once aware of a particular alleged infringement, that is substantially certain to facilitate or further the infringement. This revealed framework can help improve the evolution of copyright law in response to architectural infringement claims against emerging information architectures, such as generative AI and blockchain. As technologies continue to develop at a breakneck pace, intent-based refinements to secondary liability provide an additional path toward an innovation-promoting, copyright-respectful future.

TABLE OF CONTENTS

Law and Policy Fellowship, Center for Intellectual Property x Innovation Policy, George Mason University – Antonin Scalia Law School.

INTRODUCTION

We live in a society increasingly saturated with information technology. We record content when and where we want.[1] We access billions of pieces of content — everything from recipes to news — through the Internet.[2] We communicate with friends, family, and colleagues through email and messaging.[3] We send files instantaneously across the globe.[4] Even fifty years ago, these information technologies or information architectures — systems that facilitate storage and

[1] *See* David Carr, *Barely Keeping Up in TV's New Golden Age*, N.Y. TIMES (Mar. 9, 2014), https://www.nytimes.com/2014/03/10/business/media/fenced-in-by-televisions-excess-of-excellence.html.

[2] *See* Julian Ring, *30 Years Ago, One Decision Altered the Course of Our Connected World*, NPR (Apr. 30, 2023, 7:00 AM), https://www.npr.org/2023/04/30/1172276538/world-wide-web-internet-anniversary [https://perma.cc/R8KC-FWL7].

[3] *See* Eric Barton, *Love It or Loathe It, Email Changed the World*, BBC (Jan. 13, 2015), https://www.bbc.com/worklife/article/20150109-love-it-or-loathe-it-email-changed-the-world [https://perma.cc/3NMS-FR9R].

[4] *What is a File Transfer*, IBM (Sept. 16, 2024), https://www.ibm.com/topics/file-transfer [https://perma.cc/MJU9-J9CA].

sharing of content — were unimaginable. Today, they are essential to everyday life.

From the start, new information architectures like these tested the bounds of copyright law. Concerns about the printing press and its mass reproduction of other works led to the English Statute of Anne of 1710, the forebearer of U.S. copyright law.[5] Many subsequent information architectures similarly alarmed copyright owners and strained copyright's bounds.[6] In response, copyright owners brought infringement claims against the makers and users of these technologies for directly copying their works.[7]

The burden was on courts and Congress to respond in an innovation-promoting, copyright-respectful manner. It is well established that intellectual property law can stymie innovation.[8] Recognizing this,

[5] Russ Ver Steeg, *The Roman Law Roots of Copyright*, 59 MD. L. REV. 522, 528 (2000).

[6] *See infra* Part I.

[7] *See infra* Part I.

[8] *See, e.g.*, Julie E. Cohen & Mark A. Lemley, *Patent Scope and Innovation in the Software Industry*, 89 CALIF. L. REV. 1, 5 (2001) ("[I]t is also possible that the patent system may constrain innovation if it draws protection too broadly."); Rochelle C. Dreyfuss & James P. Evans, *From* Bilski *Back to* Benson*: Preemption, Inventing Around, and the Case of Genetic Diagnostics*, 63 STAN. L. REV. 1349, 1360 (2011) (discussing how the murkiness of patent waivers "could foster litigation, dampen innovation, and impair business."); Jeanne C. Fromer, *Claiming Intellectual Property*, 76 U. CHI. L. REV. 719, 761 (2009) (describing how clear notice of patents and copyrights is preferable to maintain "the delicate balance of intellectual property laws."); Jeanne C. Fromer, *Machines as the New Oompa-Loompas: Trade Secrecy, the Cloud, Machine Learning, and Automation*, 94 N.Y.U. L. REV. 706, 708 (2019) ("Like other intellectual property rights, trade secret law has a body of built-in limitations to ensure that the incentives offered by the law's protection do not become so great that they harm follow-on innovation . . . ."); Mark A. Lemley & R. Anthony Reese, *Reducing Digital Copyright Infringement Without Restricting Innovation*, 56 STAN. L. REV. 1345, 1350 (2004) ("Optimal digital copyright policy with respect to p2p networks would do two things: deter technological innovators as little as possible and permit cost-effective enforcement of copyright in the digital environment."); Peter S. Menell & David Nimmer, *Unwinding* Sony, 95 CALIF. L. REV. 941, 1023 (2007) [hereinafter Menell & Nimmer, *Unwinding Sony*] ("The concern of expansive liability standards discouraging nascent technologies should not be underestimated."); Philip J. Weiser, *The Internet, Innovation, and Intellectual Property Policy*, 103 COLUM. L. REV. 534, 538 (2003) (explaining that the challenge for intellectual property law in regulating software infrastructure will be "to protect investment incentives that facilitate innovation while at the same time ensuring open access to dominant software products"); Tim Wu, *Intellectual Property, Innovation, and*

many scholars have explained that copyright law must strive to keep pace with technology and maintain balance between protecting authors' rights to incentivize new creative works and providing public access to those works.[9] Copyright law relied upon the tools available to it, such as

Decentralized Decisions, 92 VA. L. REV. 123, 125 (2006) ("While we may accept that intellectual property offers strong ex ante incentives to innovate (as did the Fifth Generation project), there is a flip-side danger of too much centralization of decisionmaking.").

[9] *See, e.g.*, Shyamkrishna Balganesh, *Copyright as Legal Process: The Transformation of American Copyright Law*, 168 U. PA. L. REV. 1101, 1146 (2020) (describing the historical need to modernize the Copyright Act of 1909 to "keep[] the system afloat" due to technological changes); Jane C. Ginsburg, *Copyright and Control over New Technologies of Dissemination*, 101 COLUM. L. REV. 1613, 1616-17 (2001) (discussing the nuanced approach of courts and Congress to resolving tensions "between the exercise of control under copyright on the one hand and the availability of new technology on the other"); Mark A. Lemley & Pamela Samuelson, *Interfaces and Interoperability After* Google v. Oracle, 100 TEX. L. REV. 1, 38 (2021) (describing courts' concerns about copyright law stifling innovation in software); Jessica D. Litman, *Real Copyright Reform*, 96 IOWA L. REV. 1, 3-4 (2010) (describing how new technologies were initially stymied by outdated copyright laws); Peter S. Menell, *Tailoring Legal Protection for Computer Software*, 39 STAN. L. REV. 1329, 1330-31 (1987) ("Given the many interrelated stages of the computer industry . . . and the high costs of contracting among the diverse producers and consumers at each stage, expansive legal protection at an early stage inhibits innovation at the other stages."); Gideon Parchomovsky & Alex Stein, *Intellectual Property Defenses*, 113 COLUM. L. REV. 1483, 1496-97 (2013) (describing how various copyright infringement defenses permit technological innovation); Kal Raustiala & Christopher Jon Sprigman, *The Second Digital Disruption: Streaming and the Dawn of Data-Driven Creativity*, 94 N.Y.U. L. REV. 1555, 1606 (2019) ("[C]opyright provides its incentive to create at a price."); Pamela Samuelson, *Toward a "New Deal" for Copyright in the Information Age*, 100 MICH. L. REV. 1488, 1498 (2002) (arguing that the DMCA was an attempt at a balanced copyright law); Pamela Samuelson & Suzanna Scotchmer, *The Law and Economics of Reverse Engineering*, 111 YALE L.J. 1575, 1650 (2002) (explaining that outlawing reverse engineering under copyright law would immunize computer programs "from an important source of competition for almost a century, which would likely impede innovation in the software industry"); Christopher Sprigman, *Reform(aliz)ing Copyright*, 57 STAN. L. REV. 485, 488-90 (2004) (arguing for a scheme for "reformalizing" copyright in a way that accounts for technology and international treaty obligations); Harry Surden, *Technological Cost as Law in Intellectual Property*, 27 HARV. J.L. & TECH. 135, 137-38, 149 (2013) (positing that technological developments drive shifts in the scope of intellectual property law that allow infringing activities); Alfred C. Yen, *Third-Party Copyright Liability After* Grokster, 91 MINN. L. REV. 184, 213-14 (2006) [hereinafter Yen, *Third Party Copyright Liability*] (discussing how courts must "balance the advantages and disadvantages of third-party copyright liability" to achieve copyright's goals).

fair use, which has been called the "*de facto* regulator of new media technologies," to maintain this balance.[10]

But almost fifty years ago, a new type of copyright infringement claim emerged that posed unique challenges to copyright law and introduced a new, underappreciated balancing tool. Unlike the previous *direct* infringement claims against information architecture users and providers, rights owners started to bring what this Article terms architectural infringement claims — systemic *secondary* liability claims against the providers of information architectures that seek to hold them liable for all their users' infringements.[11] For example, architectural infringement claims alleged that Internet service providers and online platforms should be liable for hosting or transmitting all their users' infringements.[12]

Architectural infringement claims can pose an acute challenge to copyright's goals. When these architectural infringement claims are successful, information technology providers are liable for up to $150,000 per each of their users' infringements, potentially threatening the viability of the new information technology and increased access to works.[13] But outright barring such claims would restrict copyright owners' rights, permitting mass infringement and potentially discouraging creativity.[14] Either outcome could undercut the very goals of creation and dissemination that copyright seeks to achieve.[15]

In response to these claims, secondary liability has become an important but undertheorized instrument in copyright's technology toolkit. Prior scholarship, while not identifying architectural

[10] BJ Ard, *Copyright's Latent Space: Generative AI and the Limits of Fair Use*, 110 CORNELL L. REV. (forthcoming 2025) (manuscript at 4).

[11] *See infra* Part I.

[12] Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1365 (N.D. Cal. 1995).

[13] *See* Lemley & Reese, *supra* note 8, at 1350 ("[L]awsuits based on indirect liability sweep together both socially beneficial and socially harmful uses of a program or service, either permitting both uses or condemning both.").

[14] *See* Jane C. Ginsburg, *Creation and Commercial Value: Copyright Protection of Works of Information*, 90 COLUM. L. REV. 1865, 1915 (1990) ("[T]he second comer's free reuse of the first compilation may not advance the public access policies . . . but may simply discourage production of these kinds of works.").

[15] *See infra* Part I.

infringement claims as such, examined these claims individually.[16] But this approach missed the overarching consideration animating courts and Congress' refinements to copyright law in response to these claims.

By reexamining these systemic secondary liability claims holistically as architectural infringement claims, this Article contributes to the literature by surfacing how courts and Congress typically use — and should continue to use — intent as a polestar for refining secondary liability in response to architectural infringement claims to help maintain copyright's balance between incentives and access.[17] In this Article, intent does not have its more common, narrower meaning under criminal or tort law, where a defendant purposefully intends an outcome to occur.[18] Instead, I employ the broader second meaning of intent under the *Restatement (Third) of Torts*: an actor's action or inaction, once aware of a particular alleged infringement, that is substantially certain to facilitate or further the infringement.[19] While knowing the optimal balance between incentives and access remains elusive, proxies such as intent help guide courts' refinements to copyright law in a balanced manner. Intent also offers several additional normative benefits,

[16] *See, e.g.*, Mark Bartholomew & Patrick F. McArdle, *Causing Infringement*, 64 VAND. L. REV. 675, 680 (2011) (describing how courts have relied on criminal and tort law to expand contributory infringement law); Stacey L. Dogan, *Infringement Once Removed: The Perils of Hyperlinking to Infringing Content*, 87 IOWA L. REV. 829, 853 (2002) [hereinafter Dogan, *Infringement Once Removed*] (describing how linking to infringing content could form the basis for a secondary liability claim); Lemley & Reese, *supra* note 8, at 1346-47 (describing the rise in secondary liability claims stemming from online infringements); Alfred C. Yen, *Torts and the Construction of Inducement and Contributory Liability in* Amazon *and* Visa, 32 COLUM. J.L. & ARTS 513, 530 (2009) [hereinafter Yen, *Torts and the Construction of Inducement*] (advocating for increased consideration of the difference between intentional tort and negligence in secondary infringement cases). *See generally* Mark Bartholomew & John Tehranian, *The Secret Life of Legal Doctrine: The Divergent Evolution of Secondary Liability in Trademark and Copyright Law*, 21 BERKELEY TECH. L.J. 1363, 1369-94 (2006) (tracing the origins of secondary liability and comparing contributory and vicarious copyright and trademark infringement liability).

[17] *See infra* Part II.

[18] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL AND EMOTIONAL HARM § 1 (AM. L. INST. 2010).

[19] *Id.*; *see also* Garratt v. Dailey, 304 P.2d 681, 681 (Wash. 1956) (holding that knowledge "with substantial certainty" of an outcome was sufficient to assert intent). The definition also appears in the more widely adopted *Restatement (Second)*, but there it is not disaggregated from the first definition of intent. *See infra* note 65.

including being flexible enough for courts and Congress to respond to unforeseen future technologies and helping actualize the goals of secondary liability under tort law more broadly.[20]

Courts and Congress did not make intent an element of secondary liability but subconsciously used it as a guide for refining the doctrine. For example, in the context of the Internet, new elements such as notice-and-takedown, willful blindness, repeat infringer policies, right and ability to control, and knowing failure to prevent infringement were adopted as part of refined secondary liability tests and a new safe harbor for Internet service providers.[21] While intent is a broad polestar, this very flexibility gives courts and Congress the necessary freedom to adapt secondary liability doctrine to new technologies.

As history shows, new information architectures — and accompanying architectural infringement claims — will continue to emerge and strain the bounds of copyright.[22] Emerging information architectures with novel features could face architectural infringement claims in the near future, including generative AI and blockchain. In response, courts and Congress should consciously use the surfaced intent framework for secondary liability to further refine copyright law in an innovation-promoting, copyright-respectful manner.

In Part I, this Article surveys the history of copyright and information architectures and elucidates the category of architectural infringement claims and the unique challenges they pose to copyright law. Part II uncovers the solution courts have tacitly adopted by surfacing the use of intent as the guiding polestar for balanced copyright and refining secondary liability doctrine in cases involving videocassette recorders, Internet service providers and platforms, and peer-to-peer file exchanges. In Part III, this Article argues that intent is a beneficial framework for refining copyright law's secondary liability doctrine in response to architectural infringement claims, both by providing an explicit guide and actualizing the goals of secondary liability in tort law. The remainder of the Article, Part IV, presents a case study on prospective architectural infringement claims against generative AI and

[20] *See infra* Part III.

[21] *See infra* Part II.B.

[22] *See infra* Part I and Part II (discussing many examples of copyright law responding to different information architectures).

blockchain-based technologies. Both information architectures, like their predecessors, have novel aspects — content generation and immutability, respectively — that do not comport with extant copyright secondary liability doctrines. The growing legal literature on those technologies has not yet examined these architectural infringement risks or how copyright law should respond.[23]

I. INFORMATION ARCHITECTURES AND THE ARCHITECTURAL INFRINGEMENT PROBLEM

From the very beginning, copyright law has needed to respond to challenges posed by new information architectures, systems that facilitate the storage or dissemination of information. According to some sources, the printing press sparked the need for copyright protection, leading the English parliament to enact the Statute of Anne of 1710, the "doctrinal blueprint" for U.S. copyright law.[24] While the risk of widespread copying of a written work by hand was relatively low, the printing press permitted unprecedented mass reproduction.[25]

[23] *See, e.g.*, EDWARD LEE, CREATORS TAKE CONTROL: HOW NFTS REVOLUTIONIZE ART, BUSINESS, AND ENTERTAINMENT 156 (2023) (describing NFTs as part of De-IP, which "provides an alternative way to update copyright law for the twenty-first century"); Amy Adler, *Artificial Authenticity*, 98 N.Y.U. L. REV. 706, 760 (2023) (positing that NFTs are the culmination of the struggle over authenticity in art); Shaanan Cohney, David A. Hoffman, Jeremy Sklaroff & David Wishnick, *Coin-Operated Capitalism*, 119 COLUM. L. REV. 591, 601 (2019) (describing how "[initial coin offerings] expand the role played by computer code in governing transactional relationships"); Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson & Harlan Yu, *Accountable Algorithms*, 165 U. PA. L. REV. 633, 678 (2017) (describing how computer science techniques could be used to counter the discriminatory effects of machine learning); Mark A. Lemley & Bryan Casey, *Fair Learning*, 99 TEX. L. REV. 743, 776-79 (2021) [hereinafter Lemley & Casey, *Fair Learning*] (arguing that training an AI system on copyrighted content should be fair use under copyright law); Pamela Samuelson, *Fair Use Defenses in Disruptive Technology Cases*, 71 UCLA L. REV. 1484, 1557–59 (2024) (considering the ingestion of training data by AI systems to be copyright fair use because it is a non-expressive use); Katherine J. Strandburg, *Rulemaking and Inscrutable Automated Decision Tools*, 119 COLUM. L. REV. 1851, 1857 (2019) (discussing how the inscrutability of AI tools creates barriers to explaining AI-powered decisions).

[24] Oren Bracha, *The Statute of Anne: An American Mythology*, 47 HOUS. L. REV. 877, 877-78 (2010); *see also* Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 430 (1984).

[25] Rosalind S. Kurz, *Addressing the Reprographic Revolution: Compensating Copyright Owners for Mass Infringement*, 15 MICH. J.L. REFORM 261, 262 n.5 (1982).

Copyright law was, in theory at least, intended to protect authors from this potential mass unauthorized reproduction of their works.[26]

Copyright law is especially likely to implicate information architectures given that they transmit information. However, the category of information architectures delineates those technologies that facilitate the dissemination of information from other items copyright law can implicate. The category does not include new media, such as software or blueprints.[27] Nor does it include physical places, such as swap meets.[28] Information architectures is also a helpful differentiator for technologies that contain mixed properties for information dissemination and other uses, including plagiarism checkers and generative AI.[29] The storage and sharing of information function poses particularly thorny questions for copyright law given the importance of free expression and the dissemination thereof.

Many more information architectures followed in the wake of the printing press, perennially straining the bounds of copyright law. As Arthur Miller surmised, "In every age, a new technology has appeared about which people have expressed fear and concern, claiming that it defies the boundaries of the existing legal system."[30] New technologies, almost by definition, have novel aspects that distinguish them from

[26] Ver Steeg, *supra* note 5, at 528. *But see* Oren Bracha, *The Ideology of Authorship Revisited: Authors, Markets, and Liberal Values in Early American Copyright*, 118 YALE L.J. 186, 193 (2008) (discussing how publishers used authors' rights as a lobbying tactic to achieve copyright laws).

[27] *See, e.g.*, 17 U.S.C. § 120 (providing copyright protection for any pictorial representation of architecture, including blueprints); MAI Sys. Corp. v. Peak Comput., Inc., 991 F.2d 511, 518 (9th Cir. 1993) (holding that software copied into random access memory ("RAM") was sufficiently permanent to be a copy).

[28] *See, e.g.*, Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996) (discussing secondary copyright infringement claims involving the operator of a swap meet).

[29] *See, e.g.*, A.V. *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 645 (4th Cir. 2009) (discussing whether a plagiarism checker made a fair use of copyrighted works); Complaint at 23, Getty Images (US), Inc. v. Stability AI Inc., No. 23-cv-00135-UNA (D. Del. Feb. 3, 2023) (alleging copyright infringement claims against a generative AI provider).

[30] Arthur R. Miller, *Computers and Authorship: The Copyrightability of Computer-Generated Works*, *in* WIPO WORLDWIDE SYMPOSIUM ON THE INTELLECTUAL PROPERTY ASPECTS OF ARTIFICIAL INTELLIGENCE 241, 245 (1991).

their predecessors and have not yet been contemplated by copyright law. These include, for example, home recordings of televised programming and the ability to share content seamlessly across the Internet.[31] Congress and the courts have expanded and contracted copyright in response to new information architectures to avoid unduly stymying the information architectures' utility while remaining faithful to the goals of copyright.[32]

In response to new information architectures such as the printing press, copyright owners initially alleged that the providers or users of information architectures should be liable for *direct* copyright infringement because they were copying the rights owners' works. Courts and Congress largely responded to these infringement claims through four tools in copyright's technology toolkit: compulsory licensing, fair use, statutory exceptions, and direct liability refinements.[33] For example, Congress imposed compulsory licensing regimes for musical works and broadcast retransmissions in response to, respectively, player pianos and cable television.[34] In other cases, courts found new technological uses of copyrighted works to be non-infringing fair uses, including photocopying (under the right circumstances), search engines, Google Books, and plagiarism checkers.[35] Later, courts also refined direct liability for copyright

[31] Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 419 (1984); A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).

[32] *See infra* Part II.

[33] *See* Matthew Sag, *God in the Machine: A New Structural Analysis of Copyright's Fair Use Doctrine*, 11 MICH. TELECOMMS. & TECH. L. REV. 381, 408 (2005) ("[F]air use has a role to play in maintaining a constitutionally acceptable balance between copyright and freedom of speech."); Jacob Victor, *Reconceptualizing Compulsory Copyright Licenses*, 72 STAN. L. REV. 915, 920 (2020) ("This Article argues that the compulsory licensing regime should be understood as a mechanism for modulating the 'incentives/access tradeoff,' the tension between copyright's two competing utilitarian priorities: financially incentivizing creators to produce works that are valuable to the public and ensuring public access to such works."); Michael P. Goodyear, *Artificial Infringement*, U.C. L.J. (forthcoming 2026) (manuscript at 23-24) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5184405.

[34] *See* Act of Mar. 4, 1909, ch. 320, § 1(e), 35 Stat. 1075 (amended 1976); ABC, Inc. v. Aereo, Inc., 573 U.S. 431, 441-42 (2014).

[35] Authors Guild v. Google, Inc., 804 F.3d 202, 225 (2d Cir. 2015); A.V. *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 645 (4th Cir. 2009); Perfect 10, Inc. v.

infringement in response to new information architectures. For example, faced with increasingly complex machines, courts introduced the requirements of volition and causation into the direct liability test.[36] Under this test, the provider of a remote-storage digital video recorder was not liable for infringement, but the providers of remote antennae services and a digital music file resale system were liable.[37]

But fifty years ago, a paradigm shift occurred that introduced a new balancing instrument into copyright law's technology toolkit.[38] Instead of solely alleging *direct* infringement by the information architecture provider or its users, copyright owners increasingly alleged that the provider should be *secondarily* liable for all the infringements of its users. This Article terms this type of secondary liability claim at scale architectural infringement. Architectural infringement claims would hold the technology *provider* broadly liable for its *users*' copyright infringements due to the technology's architecture (or setup) allowing user infringements to proliferate. Plaintiffs had brought secondary liability claims before, notably in cases involving dance halls and swap meets, and such individualized secondary infringement claims have continued ever since for offline and online infringements.[39] But claims that sought to hold the information architecture provider liable for all its users' infringements due to the architecture were a new development. The widespread systemic nature distinguishes

Amazon.com, Inc., 508 F.3d 1146, 1168 (9th Cir. 2007); Williams & Wilkins Co. v. United States, 487 F.2d 1345, 1362 (Ct. Cl. 1973), *aff'd by an equally divided Court*, 420 U.S. 376 (1975).

[36] MELVILLE NIMMER & DAVID NIMMER, 4 NIMMER ON COPYRIGHT § 13.08[C][1] (2021). For more detail on the refinements to copyright's direct liability doctrine in response to new technologies, see generally Goodyear, *supra* note 33, at 28-33.

[37] *Compare* Cartoon Network, LP, v. CSC Holdings, Inc., 536 F.3d 121, 131 (2d Cir. 2008), *cert. denied*, Cable News Network, Inc. v. CSC Holdings, Inc., 557 U.S. 946 (2009) (finding no liability), *with ABC*, 573 U.S. at 444 (finding liability), *and* Capitol Recs., LLC v. ReDigi Inc., 934 F. Supp. 2d 640, 657 (S.D.N.Y. 2013), *aff'd*, 910 F.3d 649 (2d Cir. 2018) (finding liability).

[38] A 2006 student note did consider a "seismic shift" in copyright enforcement from direct to secondary claims, but it cabined the analysis to peer-to-peer file-sharing, which is only a small part of the architectural infringement claims rights owners have brought. Sverker K. Högberg, Note, *The Search for Intent-Based Doctrines of Secondary Liability in Copyright Law*, 106 COLUM. L. REV. 909, 910 (2006).

[39] *E.g.*, Fonovisa v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996).

architectural infringement claims from regular secondary liability ones. Courts and Congress' responses to those claims made secondary copyright infringement a tool for regulating new information architectures too.

Architectural infringement claims are different from classic direct and secondary copyright infringement. Direct infringement requires being the person who actually infringes the exclusive right.[40] Secondary liability punishes defendants for the direct infringement of others.[41] There are three types of secondary copyright liability: contributory, vicarious, and inducement.[42] Contributory infringement requires knowing of a specific infringement and materially contributing to it.[43] Vicarious infringement requires one to have the right and ability to control infringing content and receive a financial benefit directly attributable to the infringement.[44] Inducement requires one to distribute a device and promote its infringing capabilities.[45] For example, if A, an employee of B Corp., copied a Picasso painting as part of his job and posted it to C Platform, A would be the direct infringer, B Corp. would potentially be vicariously liable, and C Platform could be contributorily liable if it knew A's post was infringing but declined to remove it. C Platform could also be liable for inducement if it encouraged users to post infringing content.

The emergence of architectural infringement claims was likely due to the relative ease with which end users could make and disseminate

[40] *See, e.g.*, ABKCO Music, Inc. v. Sagan, 50 F.4th 309, 321 (2d Cir. 2022) ("Direct liability requires 'volitional conduct' that 'causes' the copying or distribution."). *But see* David Nimmer, *Volition in Violation of Copyright*, 43 COLUM. J.L. & ARTS 1, 36 (2019) (questioning whether *Aereo* abrogated the volition requirement).

[41] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 930 (2005).

[42] Courts and commentators disagree on whether inducement is a separate strain of secondary liability or a part of contributory liability, but I include it separately for clarity. *Compare* Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 670 (9th Cir. 2017) (referring to contributory copyright infringement as either materially contributing to or inducing with knowledge of another's infringement), *with* Arista Recs. LLC v. Lime Grp. LLC, 784 F. Supp. 2d 398, 424 (S.D.N.Y. 2011) ("[I]nducement of copyright infringement constitutes a distinct cause of action.").

[43] *Giganews*, 847 F.3d at 670 (quoting Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 795 (9th Cir. 2007)).

[44] *Id.* at 673.

[45] *Grokster*, 545 U.S. at 936-37.

copies, the cost-effectiveness of targeting providers rather than individual users, and the increasing complexity of the technologies.[46] Architectural infringement claims posed significant challenges to three major information architectures that will be discussed in more detail in the following Part: videocassette recorders, Internet service providers and platforms, and peer-to-peer file exchanges. As Mark Lemley and Anthony Reese have explained, the anonymity of millions of users made it difficult to enforce copyright infringement claims against users, and the more cost-effective option was suing the information architecture providers and platforms.[47] Furthermore, the technologies were complex, involving both provider and user choices and novel structural aspects that copyright law had not yet addressed.[48] These claims resulted in some of the canonical copyright law debates and cases of the past half-century.[49]

Two primary goals of copyright are providing exclusive rights to incentivize the creation of new works and disseminating those works. On the one hand, the Framers enshrined their desire to generate new works in the U.S. Constitution.[50] As Justice Sandra Day O'Connor explained, "By establishing a marketable right to the use of one's expression, copyright supplies the economic incentive to create and disseminate ideas."[51] On the other hand, copyright seeks not just the creation of new works, but also the "dissemination of [said] creative works."[52] As the Supreme Court noted nearly fifty years ago in *Twentieth Century Music Corp v. Aiken*, "[P]rivate motivation must ultimately serve the cause of promoting broad public availability of literature, music, and

[46] Lemley & Reese, *supra* note 8, at 1374-76.

[47] *Id.* at 1375-76.

[48] *See infra* Part II (discussing examples of these complexities).

[49] JESSICA D. LITMAN, DIGITAL COPYRIGHT 61, 127-28, 155-56 (2001).

[50] U.S. CONST. art. I, § 8, cl. 8 (stipulating that "Congress shall have Power . . . [t]o 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").

[51] Harper & Row Publishers, Inc. v. Nation Enters., 471 U.S. 539, 558 (1985).

[52] Stewart v. Abend, 495 U.S. 207, 228 (1990).

the other arts."[53] The benefits of creation would be nullified if no one could access them.[54]

To achieve these two sometimes competing goals, the Supreme Court has noted that copyright law seeks "a balance between a copyright holder's legitimate demand for effective — not merely symbolic — protection of the statutory monopoly, and the rights of others freely to engage in substantially unrelated areas of commerce [including new information technologies]."[55] Many copyright law scholars, including Jessica Litman, Pam Samuelson, and Chris Sprigman, echoed this sentiment when they concluded that "well-functioning copyright law carefully balances the interests of the public and of copyright owners."[56] Jane Ginsburg likewise noted how the law should "strike a happier balance between the copyright owner's, the intermediary's, and the end-user's interests (or greeds) . . . to continue to afford a hospitable environment for the creation and dissemination of works of authorship, to the ultimate enrichment of the public."[57] Maintaining this balance between incentives and access is essential to achieving the Constitution's mandate to "promote the progress of knowledge and learning."[58]

Architectural infringement claims pose an acute risk to this delicate incentives-access balance. When architectural infringement claims are successful, these information technology providers and platforms are liable for all their users' infringements — up to $150,000 per

[53] 422 U.S. 151, 156 (1975).

[54] *See* Malla Pollack, *What Is Congress Supposed to Promote?: Defining "Progress" in Article I, Section 8, Clause 8 of the United States Constitution, or Introducing the Progress Clause*, 80 NEB. L. REV. 754, 809 (2001).

[55] Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

[56] Pamela Samuelson, Jon A. Baumgarten, Michael W. Carroll, Julie E. Cohen, Troy Dow, Brian Fitzgerald, Laura Gasaway, Daniel Gervais, Terry Ilardi, Jessica Litman, Lydia Pallas Loren, Glynn Lunney, Tyler Ochoa, R. Anthony Reese, Jule Sigall, Kate Spelman, Christopher Sprigman, Michael Traynor, Tara Wheatland & Jeremy Williams, *The Copyright Principles Project: Directions for Reform*, 25 BERKELEY TECH. L.J. 1175, 1181 (2010).

[57] Jane C. Ginsburg, *How Copyright Got a Bad Name for Itself*, 26 COLUM. J.L. & ARTS 61, 64 (2002).

[58] Lydia Pallas Loren, *Untangling the Web of Music Copyrights*, 53 CASE W. RSRV. L. REV. 673, 675 (2003).

infringement if it was committed willfully — disincentivizing working with or innovating on the technology.[59] In the aggregate, such awards could easily bankrupt even wealthy technology providers. But if courts overcorrected secondary liability to permit these technologies, the interests of rights owners could be unduly harmed, disincentivizing creativity.[60] The scale of architectural infringement claims and the novel aspects of new information architectures are especially prone to upset copyright's incentives-access balance.

Beyond potentially negating copyright's goals, architectural infringement claims also pose additional issues for society by stymying technological progress, competition, and free speech. Information architectures are essential for creating and sharing knowledge in society and causing societal change.[61] Just consider the advancements in information technology from medieval parchment to today's Internet. Recognizing the role of technology in human progress, Haochen Sun has even advocated for a fundamental right to technology.[62] Expansive copyright liability could also harm technological progress by imposing unduly high costs that discourage new market entrants, harming robust competition and the innovation that flows therefrom. Overly restricting new information architectures can also have consequences for free speech. As Jack Balkin has recognized, a looser regulatory system "open[s] up possibilities for a wide variety of new applications and

[59] 17 U.S.C. § 504(c) (providing for statutory damages of $750–$30,000, up to $150,000 for willful infringement, and as low as $200 for innocent infringement); *see also* Lemley & Reese, *supra* note 8, at 1350 ("[L]awsuits based on indirect liability sweep together both socially beneficial and socially harmful uses of a program or service, either permitting both uses or condemning both."); A. Samuel Oddi, *Contributory Copyright Infringement: The Tort and Technological Tensions*, 64 NOTRE DAME L. REV. 47, 50 (1989) ("Indiscriminately broad application of the [contributory liability] doctrine, however, would exacerbate tensions between copyright and technology."); Yen, *Third Party Copyright Liability*, *supra* note 9, at 185 ("[T]hird-party copyright cases have become high stakes affairs that potentially affect the viability of entire industries.").

[60] *See* Shyamkrishna Balganesh, *The Uneasy Case Against Copyright Trolls*, 86 S. CAL. L. REV. 723, 747 (2013) (explaining the goal of copyright to incentivize creative works).

[61] Narcyz Roztocki, Piotr Soja & Heinz Roland Weistroffer, *The Role of Information and Communication Technologies in Socioeconomic Development: Towards a Multi-Dimensional Framework*, 25 INFO. TECH. FOR DEV. 171, 171 (2019).

[62] Haochen Sun, *The Fundamental Right to Technology*, 48 HOFSTRA L. REV. 445, 458 (2019).

services that can let people share information and opinions, build things together, and form online communities."[63]

Architectural infringement claims and these accompanying challenges are not limited to past information architectures, such as the videotape recorder and Internet, but are a recurring issue that will be significant for future information architecture revolutions too. As shown in Part II below, when new information architectures with novel features emerge, courts and Congress are obliged to refine copyright law to maintain the incentives-access balance. Understanding these claims and the theoretical approach courts and Congress have taken to resolve them is thus a critical step in achieving copyright law's goals and advancing innovation and free speech in the face of new information technology revolutions.

II. THE HIDDEN POLESTAR OF INTENT

Prior scholarship has missed the polestar that courts and Congress have followed in responding to architectural infringement by largely discussing the issues in these prior cases as separate rather than unitary concerns.[64] By understanding these types of intricate claims holistically

[63] Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 432 (2009).

[64] *See, e.g.*, LITMAN, *supra* note 49, at 89-150 (reviewing the DMCA's legislative history); Shyamkrishna Balganesh & Gideon Parchomovsky, *Equity's Unstated Domain: The Role of Equity in Shaping Copyright Law*, 163 U. PA. L. REV. 1859, 1877-78 (2015) (discussing how *Sony* and *Grokster* sought to adhere to the spirit of copyright by balancing incentives and access); Stacey L. Dogan, *"We Know It When We See It": Intermediary Trademark Liability and the Internet*, 2011 STAN. TECH. L. REV. 7, 7-8 [hereinafter Dogan, *"We Know It When We See It"*] (describing *Sony* and *Grokster*'s role in differentiating between good and bad actors); Jane C. Ginsburg, *Separating the* Sony *Sheep from the* Grokster *Goats: Reckoning the Future Business Plans of Copyright-Dependent Technology Entrepreneurs*, 50 ARIZ. L. REV. 577, 601-02 (2008) (describing *Sony*, *Grokster*, and the DMCA as aimed at differentiating good actors from the bad); Lemley & Reese, *supra* note 8, at 1355-72 (explaining that *Sony* is an important decision, but focusing on the infringement issues raised by peer-to-peer and online service providers); Menell & Nimmer, *Unwinding Sony*, *supra* note 8, at 943 (focusing on the continued importance of the *Sony* safe harbor); Peter S. Menell & David Nimmer, *Legal Realism in Action: Indirect Copyright Liability's Continuing Tort Framework and* Sony*'s De Facto Demise*, 55 UCLA L. REV. 143, 172-86 (2007) [hereinafter Menell & Nimmer, *Legal Realism in Action*] (discussing the *Sony* case and its aftereffects); Matthew Sag, *Internet Safe Harbors and the*

as architectural infringement claims, we can better appreciate not only the challenges these claims pose for copyright's incentives-access balance, but also this missing polestar for how they can be resolved. This Article surfaces intent as the framework courts and Congress have subterraneanly, and perhaps unconsciously, used to refine secondary liability doctrine in response to these claims.

Here, intent refers to one facilitating or furthering alleged infringement through their own action or inaction once they are aware of a particular infringement. It considers one's physical actions (or lack thereof) in response to infringement, but not necessarily their purpose as to the infringement. This is akin to the second meaning of intent under the *Restatement (Third) of Torts*, not just intending infringement to occur, but knowing that the infringement is substantially certain to occur or be furthered if an action is or is not taken.[65] Knowledge triggers a duty to act, as action or inaction in response to knowledge provides indicia of intent. This broader definition also captures actions whose purpose is infringement, which is provided by the narrower first definition under the *Restatement*.[66] This opportunity to respond arises not only when launching a product — such as under the inducement

Transformation of Copyright Law, 93 NOTRE DAME L. REV. 499, 505 (2017) [hereinafter Sag, *Internet Safe Harbors*] (describing "how the DMCA notice-and-takedown regime and DMCA-plus agreements negotiated in the shadow of that regime have shifted the locus of power with respect to copyright"); Yen, *Third Party Copyright Liability*, *supra* note 9, at 229-39 (explaining how *Grokster* offered an improved framework for secondary copyright infringement liability); Michael Modak-Truran, Note, *Is a Fair Use Forever Fair?*, 98 N.Y.U. L. REV. 962, 976-84 (2023) (discussing the fair use analysis for information architecture systems, including in *Sony* and *Napster*).

[65] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL AND EMOTIONAL HARM § 1 (AM. L. INST. 2010); *see also* DAN B. DOBBS, PAUL T. HAYDEN & ELLEN M. BUBLICK, THE LAW OF TORTS § 29 (2d ed. 2024) (elaborating on intent). This meaning of intent is also in the *Restatement (Second) of Torts*, but the *Restatement (Second)* blends this definition with the other, desiring to cause an outcome. RESTATEMENT (SECOND) OF TORTS § 8A (AM. L. INST. 2024). The *Restatement (Third)* accepts this prior definition but disaggregates the two meanings "to accommodate courts that in particular contexts might want to distinguish between intent in the sense of purpose and intent in the sense of knowledge." RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL AND EMOTIONAL HARM § 1 cmt. a (AM. L. INST. 2010).

[66] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL AND EMOTIONAL HARM § 1 (AM. L. INST. 2010).

doctrine from the Supreme Court's decision in *Grokster* — but upon each infringement.

Intent is not an additional element of secondary liability, nor does it supplant existing tests. Instead, as this Article shows, courts and Congress have used it as a guide to refine secondary liability in response to architectural infringement claims. As shown in the rest of this Part, there has been a consistent creep of courts and Congress adopting intent-based secondary liability doctrines in response to architectural infringement claims.

The use of intent may seem almost counterintuitive for copyright law, but not secondary liability. Courts typically consider copyright infringement to be a strict liability claim that does not consider intent.[67] But secondary liability does not have the same limitations as direct copyright infringement liability. Indeed, secondary liability entered copyright through common law tort — in which intent holds a prominent place.[68] Scholars have noted that secondary liability is a far more flexible doctrine due to this common law origin, permitting adaptation in response to new technologies.[69] The flexibility of

[67] *See* Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1361, 1372 (N.D. Cal. 1995) (describing direct copyright infringement as a strict liability tort for which knowledge and intent are irrelevant). *But see* Steven Hetcher, *The Immorality of Strict Liability in Copyright*, 17 MARQ. INTELL. PROP. L. REV. 1, 8 (2013) (arguing that copyright's fair use doctrine functions as a fault-based standard); Eva E. Subotnik, *Intent in Fair Use*, 18 LEWIS & CLARK L. REV. 935, 943-45 (2014) (arguing that intent has a role in copyright law, including in secondary liability and fair use).

[68] Yen, *Third Party Copyright Liability*, *supra* note 9, at 189 n.23.

[69] *See, e.g.*, Shyamkrishna Balganesh & Gideon Parchomovsky, *Structure and Value in the Common Law*, 163 U. PA. L. REV. 1241, 1244 (2015) (finding that common law concepts, including secondary liability, are designed to accommodate change); Graeme B. Dinwoodie, *Secondary Liability for Online Trademark Infringement: The International Landscape*, 37 COLUM. J.L. & ARTS 463, 479 (2014) (arguing that sensitivity to individual context is valuable because intermediaries' behaviors occupy a spectrum of trademark infringement liability and culpability); Ginsburg, *supra* note 64, at 601-02 (advocating for copyright law being able to distinguish between a range of service providers that operate copyrighted content-using technologies); Yen, *Third Party Copyright Liability*, *supra* note 9, at 212-21 (deducing that courts have not carefully delineated fault-based contributory liability and strict vicarious liability, allowing for adaptation). *But see* Felix T. Wu, *The Structure of Secondary Copyright Liability*, 61 HOUS. L. REV. 385, 387 (2023) (arguing that "the current rules of secondary copyright liability are framed too much in terms of *mens rea* and fault").

secondary liability facilitated its refinement in response to new information architectures in a way that other approaches — licensing, fair use, and direct liability — may not allow. This has led copyright law to somewhat depart from the secondary liability standards employed for patent law and other torts in order to maintain copyright's balance between incentives and access.[70] Utilizing the malleability of secondary liability, courts refined copyright law to ultimately permit videocassette recorders, Internet services,[71] and peer-to-peer file exchanges while not preventing successful infringement claims under the right circumstances.[72]

Intent fits within a time-honored legal tradition of using rough proxies to achieve intangible goals such as the incentives-access balance. Although the incentives-access balance is universally desired, it is impossible to directly ascertain the optimal balance. Instead, copyright law uses imperfect proxies to tease out what threatens and fosters the incentives-access balance to maintain it. The doctrine of fair use is one example. Fair use — the most prominent exception to copyright infringement — permits socially beneficial uses such as research, teaching, news reporting, and commentary.[73] But it is notoriously difficult to define.[74] Instead of a clear definition, it relies on four non-exclusive factors that, together, function as a sort of proxy for differentiating between socially beneficial uses we wish to encourage and socially detrimental uses we would rather prohibit.[75] But as Gideon Parchomovsky and Philip Weiser have noted, "[F]air use alone cannot, and should not, provide the *sole* policy tool available to policymakers in

[70] *See* Wu, *supra* note 69, at 393-95 (noting that while secondary patent and copyright standards are similar, the cases are not).

[71] Congress later built upon secondary liability in the Internet context when it passed the Digital Millennium Copyright Act ("DMCA"). *See infra* Part II.B.

[72] *See infra* Parts II.A–C.

[73] 17 U.S.C. § 107.

[74] *See, e.g.*, LAWRENCE LESSIG, FREE CULTURE: HOW BIG MEDIA USES TECHNOLOGY AND THE LAW TO LOCK DOWN CULTURE AND CONTROL CREATIVITY 99 (2004) (describing fair use as bounded by "fuzzy lines"); Paul Goldstein, *Fair Use in Context*, 31 COLUM. J.L. & ARTS 433, 433 (2008) (explaining that fair use is difficult, if not impossible, to define).

[75] 17 U.S.C. § 107.

the digital age."[76] Instead, other tools, including secondary liability, are necessary to fill out copyright's larger policy toolkit. Proxy-like tools such as fair use and — as this Article shows — intent in secondary liability refinements are at the core of maintaining the incentives-access balance, and they promote related norms such as technological progress and free speech.

To demonstrate the role of intent in refining copyright's secondary liability doctrine, this Part will examine the major historical architectural infringement claims in turn. These claims centered around three information architectures: videocassette recorders, Internet service providers and platforms, and peer-to-peer file exchanges.

A. The Betamax and Sony

The first information architecture that faced an architectural infringement claim was Sony's Betamax player, a type of videocassette recorder ("VCR"). The Betamax could record a broadcast for later viewing, even if the owner was not home or watching another channel.[77] Users could pause or fast-forward recorded programming and reuse Betamax tapes to record new programming.[78] The Betamax transformed the TV viewing experience. For viewers of the time, they no longer had to miss episodes of their favorite TV shows, such as *Three's Company* or *M*A*S*H*, but could watch them when they liked.

Universal Pictures and Disney filed a lawsuit against Sony, accusing it of widespread copyright infringement and attempting to stop the sale of Betamax players.[79] The time-shifting of televised content by the Betamax was a novel attribute that had not yet been addressed by law.[80] The answer's uncertainty potentially deterred other would-be entrants,

---

[76] Gideon Parchomovsky & Philip J. Weiser, *Beyond Fair Use*, 96 CORNELL L. REV. 91, 95 (2010).

[77] Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 422-23 (1984).

[78] *Id.*

[79] JOSHUA M. GREENBERG, FROM BETAMAX TO BLOCKBUSTER: VIDEO STORES AND THE INVENTION OF MOVIES ON VIDEO 3 (2010).

[80] *See Sony*, 464 U.S. at 458 (Blackmun, J., dissenting).

leaving Sony's Betamax and JCR's VHS as the main two competitors in the videocassette recorder business.[81]

In 1984 — eight years after the litigation started, and following two Supreme Court oral arguments[82] — the Supreme Court determined that the Betamax was lawful. Below, the Central District of California held Sony not liable for infringement, but the Ninth Circuit reversed.[83] Like the district court, the Court imported the staple article of commerce doctrine from patent law, which says that manufacturers, distributors, retailers, and advertisers of products suitable for substantial noninfringing uses do not have constructive (i.e., automatic) knowledge of infringement stemming from use of their product, and applied it to the Betamax.[84] From this decision emerged the canonical *Sony* safe harbor, which holds that one cannot be contributorily liable on the basis of constructive knowledge for merely offering a product that could be used for copyright infringement if it is capable of substantial noninfringing uses.[85] The Betamax had substantial noninfringing uses. While the respondents opposed the Betamax, many other producers authorized time-shifting of their programming because it would enlarge the entire viewing audience.[86] Furthermore, home time-shifting was found to be a protected fair use.[87]

Sony was decided by only the narrowest of margins. It was a 5–4 decision overturning a Ninth Circuit decision that had reached a "diametrically opposite result[]" from the district court.[88] Furthermore, the papers of Supreme Court Justice Harry Blackmun indicate that, initially, five justices were in favor of upholding the Ninth Circuit

[81] *Sony Goes to Battle for Its Favorite Child*, SONY, https://www.sony.com/en/SonyInfo/CorporateInfo/History/SonyHistory/2-02.html (last visited Jan. 21, 2025) [hereinafter *Sony Goes to Battle*].

[82] *See* Sony Corp. v. Universal City Studios, Inc., 463 U.S. 1226, 1226 (1983) (mem.).

[83] Universal City Studios, Inc. v. Sony Corp., 480 F. Supp. 429, 457 (C.D. Cal. 1979), *rev'd*, 659 F.2d 963, 975-76 (9th Cir. 1981).

[84] *Sony*, 464 U.S. at 456; *see also* Menell & Nimmer, *Unwinding Sony*, *supra* note 8, at 976-82 (describing how the Supreme Court incorporated patent law's staple article of commerce doctrine into copyright law).

[85] *See Sony*, 464 U.S. at 442.

[86] *Id.* at 443-46.

[87] *Id.* at 454-55.

[88] *Id.* at 457, 487 (Blackmun, J., dissenting).

decision, at least in part.[89] But Justice Sandra Day O'Connor switched sides, joining the decision penned by Justice John Paul Stevens.[90] One justice made the difference.

At the heart of the *Sony* decision was Sony's intent, or rather lack of intent, to act knowing that infringements of specific copyrighted works were substantially certain to occur. The *Sony* court's incorporation of the staple article of commerce doctrine from patent law to protect developers of products that had substantial non-infringing uses was animated by the court's desire not to impute knowledge of infringement based on the product alone.[91] This suggests a consideration of intent. As the Supreme Court later noted in *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, "*Sony*'s rule limits imputing culpable intent as a matter of law from the characteristics or uses of a distributed product."[92] Sony did not specifically intend to infringe and could not stop purchasers' infringements after selling a Betamax. Justices Ginsburg and Breyer debated the exact confines of the *Sony* test and how much breathing room new technologies should be permitted in their dueling concurrences in *Grokster*, but they agreed that *Sony* was aimed at striking a balance, and Justice Ginsburg noted that part of that balance was capturing "culpable behavior."[93]

Sony was rightly decided and maintained copyright's balance, facilitating further innovation in time-shifting technologies while respecting existing rights. The VCR market that the *Sony* rule facilitated led to post-VCR technologies, including TiVo, on-demand, and streaming devices such as Roku and Apple TV.[94] Commentators have

[89] Jessica Litman, *The Sony Paradox*, 55 CASE W. RSRV. L. REV. 917, 929-41 (2005) (discussing Justice Blackmun's papers and the story they presented on the *Sony* deliberations).

[90] *Id.*

[91] *See Sony*, 464 U.S. at 439, 442.

[92] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 934 (2005).

[93] *Id.* at 942 (Ginsburg, J., concurring); *id.* at 956 (Breyer, J., concurring).

[94] *See* Chaim Gartenberg, *TiVo's Skip Button Changed How We Watch TV Forever*, THE VERGE (Feb. 21, 2020, 9:16 AM), https://www.theverge.com/2020/2/21/21136537/tivo-skip-button-tv-dvr-fast-forward [https://perma.cc/TUY3-YXU6] (describing the later history of TV time-shifting technology). *But see* Fox News Network, LLC v. TVEyes, Inc., 883 F.3d 169, 181 (2d Cir. 2018) (holding that the TVEyes clip-watching product that copied and allowed viewers to watch televised programming for a commercial purpose was not

since lauded *Sony* as an "innovation safe harbor" and the "Magna Carta" of the technology age.[95] As Peter Menell and David Nimmer remarked, "In the unrelenting process of adapting copyright law to technological advance, no case stands out more prominently than the Supreme Court's 1984 decision in *Sony*."[96]

A postlude to *Sony* emerged in the form of digital audio tapes several years later. Digital audio tape technology allowed users to make flawless copies of CD sound recordings.[97] While this sort of space-shifting technology would seem to be squarely within the boundaries of the *Sony* rule, the recording industry opposed digital audio tapes and songwriter Sammy Cahn sued Sony, again the maker of the information architecture.[98] The case settled a year later, and the various interest groups ultimately hammered out a deal in the form of the Audio Home Recording Act of 1992 ("AHRA").[99]

Although the AHRA was technically unnecessary under *Sony*, it also seemed to consider intent. The AHRA bans the importation, manufacture, and distribution of any digital audio recording device that does not block the making of second-generation digital copies, which would more likely be for infringement purposes.[100] This could suggest that these devices were more substantially certain to lead to infringements. Therefore, permitting second-generation copying could provide indicia of providers' intent to facilitate infringement. But the AHRA is of limited importance today. The first court decision to address the AHRA limited its use to yesterday's technology. In *RIAA v. Diamond Multimedia Sys, Inc.*, the Ninth Circuit held that the AHRA applied

fair use because "TVEyes is unlawfully profiting off the work of others by commercially re-distributing all of that work that a viewer wishes to use, without payment or license," unlike *Sony*, where the viewer was able to view content he otherwise was authorized to see, albeit at a different time).

[95] Litman, *supra* note 89, at 951-60; Randal C. Picker, *Rewinding* Sony*: The Evolving Product, Phoning Home and the Duty of Ongoing Design*, 55 CASE W. RSRV. L. REV. 749, 765 (2005).

[96] Menell & Nimmer, *Unwinding Sony*, *supra* note 8, at 942.

[97] Taro J. Kawamura, Note, *Digital Audio Tape Technology: A Formidable Challenge to the American Copyright System*, 4 AM. U. J. INT'L L. & POL'Y 409, 409-10 (1989).

[98] Menell & Nimmer, *Legal Realism in Action*, *supra* note 64, at 162.

[99] *Id.*

[100] 17 U.S.C. § 1002(a).

narrowly to digital audio recording devices and not general computer technology, so the maker of an MP3 player was not subject to the AHRA.[101]

B. The Internet and the DMCA

Following the Betamax and digital audio tapes, the next major series of architectural infringement claims involved Internet service providers and platforms. As Lawrence Lessig has explained, the Internet, supported by digital technologies, "changed the marketplace for making and cultivating culture."[102] The Internet brought a sea change to how copyrights are infringed. Infringers can directly and perfectly copy and distribute others' works across the web; prior technologies did not allow such easy or widespread dissemination.[103] The Internet allowed anonymous or pseudonymous users to easily distribute infringing works to millions.[104] Even if the directly infringing user was identifiable, litigation against them offered a low return.[105] These considerations understandably led rightsholders to want to hold more identifiable and wealthier parties liable for the infringement, namely Internet service providers and online platform operators that hosted user-generated content.[106] As Lemley and Reese have explained, this resulted in a deluge

[101] *See* 180 F.3d 1072, 1076 (9th Cir. 1999); *see also* All. of Artists & Recording Cos., Inc. v. DENSO Int'l Am., Inc., 947 F.3d 849, 855 (D.C. Cir. 2020) (holding that the AHRA does not apply to "personal computers and computer storage media").

[102] LESSIG, *supra* note 74, at 9.

[103] Jacqueline D. Lipton, *Secondary Liability and the Fragmentation of Digital Copyright Law*, 3 AKRON INTELL. PROP. J. 105, 106, 109 (2009); *see also* Mark Bartholomew, *Copyright, Trademark and Secondary Liability After* Grokster, 32 COLUM. J.L. & ARTS 445, 464 (2009) ("Digital technology permits infringers to perfectly replicate a copyrighted item, in effect, removing all control over distribution of that expressive product from the hands of the copyright owners.").

[104] *See* INFO. INFRASTRUCTURE TASK FORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE: THE REPORT OF THE WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS 10 (1995) ("Just one unauthorized uploading of a work onto a bulletin board, for instance — unlike, perhaps, most single reproductions and distributions in the analog or print environment — could have devastating effects on the market for the work.").

[105] Lemley & Reese, *supra* note 8, at 1349.

[106] MICHAEL J. MCCUE, SECONDARY LIABILITY FOR TRADEMARK AND COPYRIGHT INFRINGEMENT 1, https://www.lewisroca.com/assets/htmldocuments/M.%20McCue%20

of secondary liability claims against them.[107] These claims took the form of architectural infringement claims and, like Sony's Betamax, threatened copyright's balance between incentives and access, as well as innovation more broadly.

But users sharing or posting content through providers' Internet services, rather than having a publisher approve the content, posed a novel issue for courts and a potential barrier to would-be innovators in the space. It was unclear what, if any, liability service providers should have for their users' infringements. As Senator Orrin Hatch noted, "Without clarification of their liability, service providers may hesitate to make the necessary investment in the expansion of the speed and capacity of the Internet."[108]

One example of this early Internet litigation is *Religious Technology Center v. Netcom On-Line Communication Services, Inc.* In that case, the plaintiffs sued Netcom for direct copyright infringement because it provided Internet services to the online bulletin board on which a user — a former Scientology minister — posted several copyrighted Scientology texts.[109] Prior to *Netcom*, the few cases to decide parallel facts held the service providers liable for the infringement.[110]

Judge Ronald Whyte rejected this architectural infringement theory and distinguished the prior decisions, finding that "it does not make sense to adopt a rule that could lead to the liability of countless parties whose role in the infringement is nothing more than setting up and operating a system that is necessary for the functioning of the

Utah%20Cyber%20Symposium%20SECONDARY%20LIABILITY%20Sept%2023.pdf (last visited Jan. 21, 2025) [https://perma.cc/57PY-BABU].

[107] Lemley & Reese, *supra* note 8, at 1353-54, 1377-78; *see also* 5 WILLIAM F. PATRY, PATRY ON COPYRIGHT § 21:55 (2025) (describing a surge in contributory infringement lawsuits that has paralleled Internet growth).

[108] S. Rep. No. 105-190, at 8 (1998).

[109] Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1365-66 (N.D. Cal. 1995).

[110] *See* Sega Enters. Ltd. v. MAPHIA, 857 F. Supp. 679, 686 (N.D. Cal. 1994) (holding liable a service that encouraged users to download infringing Sega games, suggesting contributory liability); Playboy Enters., Inc. v. Frena, 839 F. Supp. 1552, 1556-57 (M.D. Fla. 1993) (holding the operator of a platform liable for violating the distribution and display rights when its customers used it to disseminate infringing photographs).

Internet."[111] His perspective seemed to be influenced by the lack of intent, as Netcom, similarly to Sony, had merely provided the information architecture.[112] Instead, he ruled that Netcom had to act with some sort of volition or causation to be directly liable, which it did not do.[113] As Stacey Dogan has noted, *Netcom* (at least implicitly) recognized that secondary liability should evolve with new technological developments to maintain copyright's balance.[114]

Acknowledging the concerns of rights owners and the risk of platform liability for user-generated content that had started to crystalize in cases like *Netcom* and its liability-finding predecessors, Congress intervened with the Digital Millennium Copyright Act ("DMCA").[115] The House Judiciary Committee considered codifying the rule from *Netcom* that there is no liability for passive, automatic acts in response to user action.[116] But instead, Congress — after a long, complicated bargaining process — passed a version of the DMCA that created four distinct liability safe harbors for user-generated infringement with their own sets of requirements for different types of online service providers to achieve balance between them and rights owners.[117] Congress thus departed from the broader standard in *Netcom* to create a more nuanced approach to service provider liability.[118]

The DMCA aims to preserve the incentives-access balance in large part through intent-driven requirements. It attempts to address mass piracy concerns and protect service providers from liability for their users' copyright infringements by imposing a series of requirements in

---

[111] *Netcom*, 907 F. Supp. at 1372.

[112] *See id.* ("Only the subscriber should be liable for causing the distribution of plaintiffs' work, as the contributing actions of the BBS provider are automatic and indiscriminate.").

[113] *Id.* at 1369-70.

[114] Dogan, *Infringement Once Removed*, *supra* note 16, at 871.

[115] *See* Michael P. Goodyear, *Synchronizing Copyright and Technology: A New Paradigm for Sync Rights*, 87 MO. L. REV. 95, 103-09 (2022) (discussing how copyright law changed in response to technological innovations).

[116] H.R. REP. NO. 105-551, pt. 1, at 11 (1998).

[117] Digital Millennium Copyright Act of 1998, Pub. L. No. 105-304, 112 Stat. 2860. On the history of the complicated bargaining to reach the final DMCA, see LITMAN, *supra* note 49, at 122-45.

[118] *See* Nimmer, *supra* note 40, at 10-11.

exchange for liability safe harbors for user-generated content.[119] As Jane Ginsburg has explained, these requirements are meant to help separate good actors from the bad.[120]

At the time, 17 U.S.C. § 512(a) appeared to be one of the most important safe harbors because it immunized Internet service providers like Netcom for infringing content in "transitory digital network communications."[121] To avail itself of the safe harbor, the service provider must not select or modify the content or recipients and cannot retain a copy.[122] These requirements, like *Netcom*, implicitly recognize the lack of intent of the service provider to take action that would reasonably lead to infringement.

Perhaps the more intent-driven requirement, however, is that any service provider must have and enforce a repeat infringer policy to avail itself of the DMCA safe harbor.[123] This is one of two threshold requirements for any of the four DMCA safe harbors.[124] This requirement is aimed at forcing service providers to respond to repeated instances of infringement by the same user, as there is a greater chance they will recidivate and providers can terminate their access to prevent this once they are aware of the problem. Failing to terminate those repeat infringers could suggest indicia of intent to facilitate ongoing infringement. The repeat infringer requirement has teeth. In *BMG Rights Managements (US) LLC v. Cox Communications Inc.*, the Fourth Circuit held that Internet provider Cox could not avail itself of the

[119] *See* 17 U.S.C. § 512; *see also* 144 CONG. REC. 9234 (1998) (explaining the goal of the DMCA).

[120] *See* Ginsburg, *supra* note 64, at 601-02. While some have criticized the DMCA, imposing broad monitoring or affirmative takedown duties on platforms would be nigh impossible since rights owners know their works and brands best. Online platforms cannot reasonably be expected to know every work in the world and police uses appropriately. *See* Sag, *Internet Safe Harbors*, *supra* note 64, at 549 (describing how platform's proactive infringement recognition systems are particularly likely to fail to recognize noninfringing uses such as de minimis and fair uses).

[121] 17 U.S.C. § 512(a).

[122] *Id.*

[123] *Id.* § 512(i)(1)(A).

[124] *Id.* § 512(i). The other requirement is accommodating and not interfering with standard technical measures but, as a practical matter, this requirement is toothless because no court has yet found anything to be a standard technical measure. *See* 4 NIMMER & NIMMER, *supra* note 36, at § 12B.02[B][3][a].

DMCA safe harbor because it "made every effort to avoid reasonably implementing that policy," resulting in a $25 million judgment against Cox.[125]

The most widely used safe harbor in litigation, however, is § 512(c), which is for user-generated content on platforms such as posts on Facebook or listings on eBay.[126] Although the Communications Decency Act's Section 230 safe harbor for torts and other claims has garnered more accolades as "the twenty-six words that created the Internet,"[127] the DMCA may have also facilitated the emergence of more online platforms with user-generated content by reducing the risk of successful architectural infringement claims.[128] Section 512(c) contains a host of requirements for service providers to qualify for the liability safe harbor for user-generated infringements, including:

1. No actual knowledge that user-generated content is infringing;[129]
2. No red flag knowledge that user-generated content is infringing;[130]
3. Expeditiously remove infringing content once known (including in response to takedown notices);[131]
4. May not both receive a direct financial benefit from the infringing content and have the right and ability to control it;[132]

[125] 881 F.3d 293, 298, 303 (4th Cir. 2018).

[126] *See* KEVIN K. HICKEY, CONG. RSCH. SERV., DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA) SAFE HARBOR PROVISIONS FOR ONLINE SERVICE PROVIDERS: A LEGAL OVERVIEW (2020), https://crsreports.congress.gov/product/pdf/IF/IF11478#:~:text=Under%20section%20512(c)%2C,infringing%20material%20on%20its%20platform.

[127] *See generally* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019) (describing the importance of Section 230 in the development of the Internet).

[128] *See* Edward Lee, *Decoding the DMCA Safe Harbors*, 32 COLUM. J.L. & ARTS 233, 269 (2009) ("[T]he DMCA safe harbors have helped to foster tremendous growth in web applications . . . .").

[129] 17 U.S.C. § 512(c)(1)(A)(i).

[130] *Id.* § 512(c)(1)(A)(ii).

[131] *Id.* §§ 512(c)(1)(A)(iii), (c)(1)(C).

[132] *Id.* § 512(c)(1)(B).

5. Have a designated service agent to which rights owners can submit takedown notices;[133]
6. Adopt, inform users of, and reasonably implement a repeat infringer policy;[134] and
7. Accommodate and not interfere with any standard technical measures to identify or protect one's works.[135]

The DMCA also provides service providers with a liability safe harbor for removing and restoring reported material, even if it later turns out to be noninfringing, if it follows a counter notification procedure under § 512(g):

1. Notify the user when the content has been removed or disabled;[136]
2. Notify the person who submitted a takedown notice if it receives a counter notification;[137] and
3. Replace removed material within 10–14 days in response to a proper counter notification if it does not learn that the reporting party has filed an action in court.[138]

At the heart of the DMCA's § 512(c) safe harbor (and § 512(d) too) is a notice-and-takedown system. Under this system, a service provider is only obligated to remove infringing content once it learns it is infringing, it gains red flag knowledge that it is infringing, or a rights owner reports that it is infringing.[139] This structure is premised on the belief that it is infeasible for a platform to know by itself whether content is infringing, but that once a rights owner informs the platform,

[133] *Id.* § 512(c)(2).

[134] *Id.* § 512(i)(1)(A).

[135] *Id.* § 512(i)(1)(B). However, as a practical matter, no court has found a standard technical measure to exist, so this requirement is, at present, a dead letter. *See* 4 NIMMER & NIMMER, *supra* note 36, at § 12B.02 ("Even as of many years after enactment of the Online Copyright Infringement Liability Limitation Act, it is unclear whether there is any such thing as 'standard technical measures.'").

[136] 17 U.S.C. § 512(g)(2)(A).

[137] *Id.* § 512(g)(2)(B).

[138] *Id.* § 512(g)(2)(C).

[139] *Id.* §§ 512(c)(1)(A), (c)(1)(C).

it is reasonable to require the platform to act.[140] These requirements are steeped in intent; a service provider is only obligated to remove infringing content once they are aware of infringements on their website because then — and only then — are they able to intentionally act in response. Obliging platforms are thus shielded from liability, while those that do not comply face a risk of being found liable for infringement.

Related to the red flag knowledge restriction, courts have prohibited willful blindness to infringement in order to qualify for the § 512(c) safe harbor. Again guided by intent, willful blindness means a provider "cannot willfully bury its head in the sand to avoid obtaining such specific knowledge" that would give it the opportunity to act.[141] This doctrine was elucidated in complex cases such as *Viacom International Inc. v. YouTube, Inc.*, where YouTube was aware that seventy-five to eighty percent of streams on its platforms contained copyrighted materials yet only ten percent was authorized, which raised an inference of willful blindness at the Second Circuit.[142] But, on remand, the district court rejected the argument because YouTube was only aware of the type of content that was being infringed, not where the specific instances of infringement were on its platform.[143] In a later case, the Second Circuit found that MP3tunes was willfully blind to infringement of pre-2007 MP3s and pre-2010 Beatles song MP3s because they could have known of specific instances of infringement after knowing these categories were never authorized for online distribution prior to those dates.[144]

The right and ability to control element could also suggest a role for intent. Courts have interpreted this element, in the DMCA context, as meaning effectively prescreening and learning of user content.[145] This

[140] James Grimmelmann & Pengfei Zhang, *An Economic Model of Online Intermediary Liability*, 38 BERKELEY TECH. L.J. 1011, 1045 (2023).

[141] UMG Recordings, Inc. v. Shelter Cap. Partners LLC, 718 F.3d 1006, 1023 (9th Cir. 2013).

[142] Viacom Int'l, Inc. v. YouTube, Inc., 676 F.3d 19, 33 (2d Cir. 2012).

[143] Viacom Int'l, Inc. v. YouTube, Inc., 940 F. Supp. 2d 110, 116-17 (S.D.N.Y. 2013).

[144] EMI Christian Music Grp., Inc. v. MP3tunes, LLC, 844 F.3d 79, 93 (2d Cir. 2016).

[145] Mavrix Photographs, LLC v. LiveJournal, Inc., 873 F.3d 1045, 1058 (9th Cir. 2017) (stating that the right and ability to control includes "prescreen[ing] sites, giv[ing] them

makes sense as a matter of intent, as the platform would then be electing to allow unauthorized content on its platform at its own discretion rather than solely the user's.

Even if a service provider loses its DMCA safe harbor under any of these or other requirements, it would not automatically be liable for copyright infringement; it would have to meet the elements of contributory or vicarious liability.[146] At present, courts impose contributory liability when platforms know of the infringement and materially contribute to it (usually meaning failure to delete it).[147] Courts impose vicarious liability when platforms have the right and ability to control — which, unlike the similar provision under the DMCA, is often understood as the ability to delete — infringing content on its platform and receive a financial benefit directly attributable to the infringement.[148]

In response to the rise of the Internet, courts modified the contributory and vicarious liability tests to attempt to preserve the incentives-access balance.[149] To demonstrate, compare the Ninth

extensive advice" (quoting Perfect 10, Inc. v. Cybernet Ventures, Inc. 213 F. Supp. 2d 1146, 1182 (C.D. Cal. 2002))).

[146] *See* 17 U.S.C. § 512(l) ("The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense."); *see also* Finley v. YouTube, LLC, No. 20-cv-04888, 2022 WL 704835, at *1 (N.D. Cal. Mar. 9, 2022) ("[T]he DMCA provides a series of statutory safe harbors, not a cause of action.").

[147] *See, e.g.*, Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 671 (9th Cir. 2017) (focusing on the removal of images once reported as infringing); Costar Grp. Inc. v. Loopnet, Inc., 164 F. Supp. 2d 688, 707 (D. Md. 2001), *aff'd*, 373 F.3d 544 (4th Cir. 2004) (defining material contribution as "failure to halt the [infringing] activity"); *see also* Bartholomew & McArdle, *supra* note 16, at 686-88 (explaining how courts expanded the definition of "material contribution" for service providers).

[148] *Giganews*, 847 F.3d at 673 (quoting Perfect 10, Inc. v. Visa Int'l Serv. Ass'n, 494 F.3d 788, 802 (9th Cir. 2007)); *see also* Arista Recs. LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 157 (S.D.N.Y. 2009) (holding that a service provider need not have the "formal power to control"; the ability to block infringers' access is enough).

[149] *See, e.g.*, Sony Music Ent. v. Cox Commc'ns, Inc., 93 F.4th 222, 227-28, 237 (4th Cir. 2024) (upholding a finding that Internet provider Cox was contributorily liable after it could not avail itself of the DMCA); Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1164 (C.D. Cal. 2002), *abrogated on other grounds by* Fabian Perez Art Publ'g LLC v. Las Brujas Inc., No. CV15-1847-DMG, 2015 WL 11430871 (C.D. Cal. Mar. 27, 2015)

Circuit's decisions in *Fonovisa, Inc. v. Cherry Auction, Inc.*, involving a swap meet operator, and *Perfect 10, Inc. v. Amazon.com, Inc.*, involving Google.[150] The knowledge requirement for contributory liability became more difficult for a plaintiff to establish, as *Perfect 10* required "*actual* knowledge" of "*specific* infringing material" on its system, compared to *Fonovisa* assuming knowledge at the swap meet.[151] However, the Ninth Circuit seems to have perhaps eased the plaintiff's burden for establishing the material contribution requirement. The *Fonovisa* court said that providing "site and facilities" such as space, utilities, parking, advertising, parking, and customers was enough for a material contribution.[152] But the *Perfect 10* court said that if the service provider could merely take "simple measures" to prevent further damage to copyrighted works, that was sufficient material contribution.[153] *Perfect 10* echoed the DMCA's consideration of intent in refining contributory liability, noting that "a service provider's knowing failure to prevent infringing actions could be the basis for imposing contributory liability [because] [u]nder such circumstances, intent may be imputed."[154] A recent decision from the Fourth Circuit in *Sony Music Entertainment v. Cox Communications, Inc.* underlines the role of intent in the material contribution element, as it noted that:

> [S]upplying a product with knowledge that the recipient will use it to infringe copyrights is exactly the sort of culpable conduct sufficient for contributory infringement. . . . In such a situation, providing the means to infringe *is* culpable [conduct] pursuant

(finding that the service provider was unlikely to successfully avail itself of the DMCA safe harbor and would likely be held contributorily and vicariously liable); *see also* Lemley & Reese, *supra* note 8, at 1368 (concluding that service providers are more likely to be found liable for contributory and vicarious copyright infringement today than in the past).

[150] *Compare* Fonovisa v. Cherry Auction, Inc., 76 F.3d 259 (9th Cir. 1996), *with* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007).

[151] *Compare Perfect 10*, 508 F.3d at 1172 (quoting A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001)), *with* Fonovisa, Inc. v. Cherry Auction, Inc., 847 F. Supp. 1492, 1496 (E.D. Cal. 1994), *rev'd on other grounds*, 76 F.3d at 264 (9th Cir. 1996).

[152] *Fonovisa*, 76 F.3d at 264.

[153] *Perfect 10*, 508 F.3d at 1172.

[154] *Id.*

> to the common law rule that a person is presumed to intend the substantially certain results of his acts.[155]

The court found Cox contributorily liable because it knew of specific repeat infringers and "chose to continue providing monthly internet access to those users despite believing the online infringement would continue."[156]

The right and ability to control in vicarious liability, however, became more difficult to prove and was less tied to intent. Courts had already somewhat loosened the direct financial benefit prong of the vicarious liability test in *Fonovisa* and prior cases by considering infringement as a draw for customers to satisfy the prong.[157] But while the direct financial benefit requirement became easier to satisfy, the right and ability to control requirement became more difficult. In *Fonovisa*, operating a swap meet satisfied the right and ability to control prong of vicarious liability because the operator could terminate vendors for any reason.[158] But in *Perfect 10*, terminating an advertising partnership — which generated traffic to the infringement — was not sufficient for the right and ability to control.[159] The service provider had to be able to stop the infringement for its action or inaction to provide indicia of intent.

For now, the developments in copyright infringement liability in response to architectural infringement claims have permitted the broad, interactive Internet we have today while preserving copyright's balance. In the aggregate, early challenges like those in *Netcom* presented significant headwinds for the interactive web. E-commerce, user reviews, social media, chatrooms, blogs, domain names, and many other facets of the modern Internet would likely not be possible without the intent-focused balance the DMCA and litigation achieved, even if, as a recent Copyright Office study found, the DMCA could use some fine-tuning to achieve optimality.[160]

---

[155] Sony Music Ent. v. Cox Commc'ns, Inc., 93 F.4th 222, 236 (4th Cir. 2024).

[156] *Id.*

[157] *See* Lemley & Reese, *supra* note 8, at 1367-68.

[158] Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996).

[159] 508 F.3d at 1173-74.

[160] U.S. COPYRIGHT OFF., SECTION 512 OF TITLE 17, at 1 (2020).

C. Peer-to-Peer File-Sharing from Napster to BitTorrent

The next major architectural infringement claims involved peer-to-peer networks, where individual users' computers are directly connected with each other and files are copied from one computer to the other without passing through or being stored on a central server.[161] Like the Betamax and Internet services, peer-to-peer networks raised novel legal issues, in this case decentralized connection to the infringement. This new challenge could have unbalanced copyright law by stymying the technology or minimizing copyright owners' rights.

One of the most notorious peer-to-peer providers was Napster, which specialized in allowing users to share free (copyrighted) music files, including chart-topping hits like NSNYC's "Bye Bye Bye" and Britney Spears' "Toxic." Napster's peer-to-peer file sharing system and MusicShare software allowed users to make their files available to others and search for files on others' computers through a central file directory.[162] Record companies, music publishers, composers, and recording artists sued Napster, alleging that the service was contributing to infringement.[163] The district court rejected Napster's *Sony* safe harbor defense, finding that Napster had minimal non-infringing uses because it was used for downloading and uploading popular music, the vast majority of which was copyrighted.[164] The Ninth Circuit disagreed and found that the *Sony* safe harbor should apply because Napster *could* be used for non-infringing purposes, even if that was not often the case.[165] But the Ninth Circuit only ruled out Napster's *constructive* knowledge of its users' infringements.[166] The Ninth Circuit determined that Napster likely had *actual* knowledge of specific infringements because it routed every user query through its system (even if the eventual file transfer was peer-to-peer).[167] Therefore, the

[161] *See* A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1012-13 (9th Cir. 2001).

[162] *See id.* at 1011.

[163] *See* A&M Recs., Inc. v. Napster, Inc., 114 F. Supp. 2d 896, 900 (N.D. Cal. 2000).

[164] *Id.* at 912.

[165] *See Napster*, 239 F.3d at 1021.

[166] *See id.* at 1020-21.

[167] *Id.* at 1021-22.

court enjoined Napster because it was likely contributorily (and vicariously) liable for copyright infringement.[168]

Subsequently, new peer-to-peer providers Grokster and StreamCast decided to design their software specifically around the *Napster* ruling to avoid liability. They used a protocol that circulated queries through a dynamic network of "nodes" rather than a centralized file directory and could not delete user accounts.[169] The Ninth Circuit, relying on its ruling in *Napster*, held that even though Grokster and StreamCast were specifically designed to bypass copyright law and were rife with infringing content, they could not be contributorily liable since they did not maintain control over the files and could not disable user accounts.[170]

But the Supreme Court reversed 9–0 and held Grokster liable. It explained that "nothing in *Sony* requires courts to ignore evidence of intent [to facilitate infringement] if there is such evidence."[171] The Court adopted the inducement test, which holds liable those who are "actively inducing" infringement through "purposeful, culpable expression and conduct" — including creators of products that would otherwise be protected by the *Sony* safe harbor.[172] Grokster was promoting infringement-enabling benefits, failing to filter infringement, depending on a high volume of infringement, and actively soliciting former Napster customers.[173] Altogether, Grokster's intent to induce infringement was "unmistakable."[174] While this mode of intent could qualify as purposefully acting to achieve a particular outcome, it also reflects Grokster knowing that infringements would likely occur and acting in a way that encouraged them. However, the Court was more

[168] *See id.* at 1027, 1029.

[169] *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 921-22 (2005).

[170] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 380 F.3d 1154, 1163-64 (9th Cir. 2004), *vacated*, 545 U.S. 913 (2005).

[171] *Grokster*, 545 U.S. at 934.

[172] *Id.* at 937, 942.

[173] *Id.* at 923-25, 938-40. *But see id.* at 939 n.12 ("Of course, in the absence of other evidence of intent, a court would be unable to find contributory infringement liability merely based on a failure to take affirmative steps to prevent infringement, if the device otherwise was capable of substantial noninfringing uses.").

[174] *Id.* at 938-40.

willing to impose categorical liability in *Grokster* due to purposeful intent compared to the knowledge-based intent that was employed in earlier Internet cases. Grokster arguably reinforces and clarifies *Sony* through its emphasis on intent, preserving well-meaning systems while punishing the worst offenders in an innovation-promoting, copyright-reliant manner.[175]

Despite the outcome, *Grokster* did not destroy peer-to-peer file sharing. Examples still exist, such as Dropbox and BitTorrent.[176] However, *Grokster* shattered certain information sharing business models that actively facilitated widespread infringement. For example, courts found other unsympathetic peer-to-peer platforms to have induced or contributorily infringed, including Usenet, LimeWire, Aimster, and Grooveshark.[177] One might query how many defendants would pursue this type of active inducement model after *Grokster*,

[175] *See* Menell & Nimmer, *Unwinding Sony*, *supra* note 8, at 943 ("The Supreme Court's recent unquestioning reliance on *Sony* in addressing the challenges of the digital age in *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.* reinforces the significance of *Sony*'s second holding.").

[176] *See, e.g.*, David Barnes, *What Is Torrenting and How Does It Work?*, BITTORRENTVPN, https://www.bittorrentvpn.com/what-is-torrenting (last visited Jan. 21, 2025) [https://perma.cc/H3ZH-RTXG] (describing BitTorrent).

[177] *See In re* Aimster Copyright Litig., 334 F.3d 643, 653 (7th Cir. 2003) ("Aimster has failed to produce any evidence that its service has ever been used for a noninfringing use . . . ."); Capitol Recs., LLC v. Escape Media Grp., No. 12-cv-6646, 2015 WL 1402049, at *43 (S.D.N.Y. Mar. 25, 2015) ("Escape provided all the mechanisms to allow for infringing activity, including the servers to host and the software to submit the infringing content, the tools for organizing the submitted files and facilitating their access and searchability, and the interface for users to select and stream infringing content to their devices."); Arista Recs. LLC v. Lime Grp. LLC, 784 F. Supp. 2d 398, 431 (S.D.N.Y. 2011) ("LW distributes LimeWire, and (1) is aware that LimeWire's users commit a substantial amount of copyright infringement; (2) markets LimeWire to users predisposed to committing infringement; (3) ensures that LimeWire enables infringement and assists users committing infringement; (4) relies on the fact that LimeWire enables infringement for the success of its business; and (5) has not taken meaningful steps to mitigate infringement."); Arista Recs. LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 154 (S.D.N.Y. 2009) ("Accordingly, based on the undisputed facts, I find that the Defendants' intent to induce or foster infringement by its users on its services was unmistakable, and no reasonable factfinder could conclude otherwise.").

although there are examples.[178] Nonetheless, *Grokster* established intent-driven parameters for lawful peer-to-peer file sharing to continue while protecting rights owners against the widespread infringement actively facilitated by Grokster and its ilk.

III. THE BENEFITS OF INTENT

As shown in Part II, and summarized in Figure 1 below, courts and Congress responded to historical architectural infringement claims by refining secondary liability doctrine with an eye to intent. The use of intent as a guiding polestar facilitated the growth of information architectures while maintaining copyright's incentives-access balance. If *Sony* had not endorsed the staple article of commerce doctrine, copyright law's high statutory damages would strongly discourage any product that could be used for infringement — regardless of intent. Yet if intent was entirely ignored, parties that clearly intended to encourage or facilitate infringement (and even based their businesses on infringement) would be allowed to escape liability through legal technicalities. By adopting inducement, the Supreme Court prevented Grokster from doing this and preserved copyright owners' rights by effectively imposing constructive knowledge on Grokster due to its unmistakable intent to encourage infringement.[179] The Internet posed perhaps the greatest challenge for the incentives-access balance. Yet *Netcom*, the DMCA, and later cases sought to maintain balance by imposing intent-based obligations on both the rights owner and service providers.[180]

[178] *See, e.g.*, Columbia Pictures Indus. v. Fung, 710 F.3d 1020, 1035-36 (9th Cir. 2013) (finding that Fung had actively encouraged the uploading of infringing copies to his system).

[179] *See* Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 941 (2005).

[180] *See* Athos Overseas Ltd. v. YouTube, Inc., No. 21-21698-Civ-GAYLES/TORRES, 2023 WL 5607936, at *9 (S.D. Fla. 2023) ("[C]harging YouTube with the affirmative obligation of going beyond the specific URLs identified in Plaintiff's DMCA takedown requests would in effect shift from the copyright owner to the ISP the burdens of policing and identifying infringement on its systems. This burden shift would contravene Congress' calculated choices and the DMCA's enacted text.").

FIGURE 1

Intent in Secondary Liability Refinements	
Sony	Staple article of commerce doctrine (i.e., *Sony* rule)
AHRA (§ 1002(a))	Second generation copying prohibited
Netcom, DMCA (§ 512(a))	No liability for merely providing Internet network
DMCA (§ 512(i))	Repeat infringer policy
DMCA (§ 512(c))	Takedown obligations (when know, should know, or upon receiving a report that it is infringing)
DMCA (§ 512(c))	No direct financial benefit and right and ability to control (i.e., prescreening content)
Viacom, *MP3tunes*	Willful blindness prohibited
Perfect 10	Knowing failure to prevent infringement; actual ability to terminate
Cox	Choosing to continue providing services despite believing infringement would continue
Grokster	Inducement

In the platform context, Felix Wu previously suggested that intent is a core requirement of contributory liability.[181] But the role of intent in copyright's secondary liability doctrine is broader than a mere requirement for one type of liability. Intent has also served as a guide for refining the vicarious liability doctrine in response to architectural infringement claims against Internet service providers and platforms, and for adopting the *Sony* rule and inducement.[182] Intent was also a guide for the AHRA's prohibition on second generation copying and for the DMCA, not only in the contributory liability parallels, but also for other aspects of that law such as the repeat infringer policy requirement.[183] This more holistic understanding of intent's role is not inconsistent with Wu's ultimate conclusion, that "if the misconduct and harm do occur, liability is based on the entity's own acts or omissions rather than

[181] Wu, *supra* note 69, at 389.

[182] *See supra* Part II.

[183] *See supra* Parts II.A–B.

on the entity taking responsibility for the other party's misconduct."[184] But recognizing intent as an overall refinement polestar for secondary liability rather than just an element for contributory liability provides a more precise understanding of the evolution of copyright doctrine and a guide for refining the doctrine in the future in response to new architectural infringement claims.

Beyond helping guide courts and Congress to the outcomes listed in Figure 1, it is also a promising normative framework for addressing future architectural infringement claims. In particular, (1) it is transparent for courts, Congress, and would-be market entrants; (2) it offers a dividing line to avoid a dragnet effect for liability; (3) its broad definition allows flexibility to respond to unforeseeable future technological developments; (4) it allows for the use of different doctrinal approaches; (5) it need not be an exclusive polestar; and (6) it helps achieve the more nebulous goals of secondary liability under tort.

First, being transparent about the role of intent for future architectural infringement cases is beneficial for the law and would-be market entrants. Without intent (or an alternative framework), the outcomes of future architectural infringement cases are more uncertain. Indeed, the historical architectural infringement decisions were often the result of years-long legal battles, appeals overturning lower court decisions, and the narrowest of victories. An intent-based outcome was not guaranteed. For example, *Sony* was a 5–4 decision reversing the Ninth Circuit after two oral arguments before the Supreme Court.[185] Judge Whyte diverged from prior judges' opinions in deciding *Netcom*.[186] The DMCA was a sui generis law reached only after significant compromise.[187] The Supreme Court decided *Grokster* by reversing the Ninth Circuit.[188]

[184] Wu, *supra* note 69, at 401.

[185] *See* Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 457 (1984) (Blackmun, J., dissenting); *see also* Sony Corp. v. Universal City Studios, Inc., 463 U.S. 1226, 1226 (1983) (restoring the case to the calendar for re-argument).

[186] Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1372-73 (1995).

[187] The House introduced the DMCA in H.R. 2281, 105th Cong. (1997), and it was enacted in Pub. L. No. 105-304, 112 Stat. 2860 (1998).

[188] Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 545 U.S. 913, 938-40 (2005).

By uncovering the latent intent framework animating those decisions and laws, courts can affirmatively use it as a dividing line rather than trying to divine a way to maintain the incentives-access balance from scratch each time an architectural infringement claim is brought. If intent had been surfaced earlier, courts could have more affirmatively relied on it to reach better outcomes in some cases involving new information architectures. For example, the Supreme Court's criticized decision in *American Broadcasting Cos. v. Aereo, Inc.* turned exclusively on direct liability.[189] The Court held that the provider of a remote antennae system for streaming local broadcasts was directly liable for copyright infringement, even though the users selected what to stream.[190] But, as Justice Antonin Scalia noted in his dissent, if copyright law's volition requirement were correctly applied, *Aereo* should have been a secondary liability case.[191] The users were causing the public performances to occur; Aereo merely provided the antennae that could rebroadcast, not a preselected assortment of content.[192] Under Scalia's approach, the provider could potentially still have been held liable under a secondary liability theory.[193] The Court could have applied prior intent-based refinements to still hold Aereo (not unlike Grokster) liable for providing a product with few if any noninfringing uses or possibly inducing infringement. If some broadcasts were licensed or another exception applied that would create substantial noninfringing uses, the Court could then turn to vicarious and contributory liability tests to determine (and potentially refine) the bounds of, respectively, the right and ability to control and the material contribution requirements.

---

[189] *See* ABC, Inc. v. Aereo, Inc., 573 U.S. 431, 453 (2014) (Scalia, J., dissenting); *see also, e.g.*, Mala Chatterjee & Jeanne C. Fromer, *Minds, Machines, and the Law: The Case of Volition in Copyright Law*, 119 COLUM. L. REV. 1887, 1900 (2019) (noting that the majority in *Aereo* failed to consider volition); Mark P. McKenna, *The Limits of the Supreme Court's Technological Analogies*, SLATE (June 26, 2014, 12:07 PM), https://slate.com/technology/2014/06/abc-v-aereo-ruling-the-supreme-courts-terrible-technological-analogies.html [https://perma.cc/3AJT-W9E9] (criticizing *Aereo* for drawing illogical and harmful comparisons between Aereo's streaming system and cable).

[190] *See Aereo*, 573 U.S. at 451.

[191] *See id.* at 455-56, 461 (Scalia, J., dissenting).

[192] *Id.* at 456.

[193] *Id.* at 462.

Relying on an explicit framework such as intent could help would-be information architecture market entrants, who may hesitate because of the uncertainty about how secondary liability will apply to them, at least prior to a court decision on the prospective architectural infringement claim. The deterrence of would-be innovators may have the undesirable effect of limiting competition to only the largest, most sophisticated technology companies rather than true competition amongst dominant players and mavericks.[194] New startups cannot compare in financial terms, making copyright infringement liability a proportionally greater risk to those companies if they are expected to bear the litigation costs and damages. This seems to have occurred with VCRs, where Sony and VHS dominated the market.[195] Overall, this legal uncertainty could have the effect of significantly chilling innovation in information technologies. Acknowledging the role of intent could potentially provide more confidence to well-intentioned market entrants that courts or Congress will not punish them merely due to a novel aspect of a new technology.

Second, intent provides a powerful and useful dividing line that considers motivation rather than relying on static tests, allowing more flexibility in responding to future architectural infringement claims. As Judge Learned Hand acknowledged, albeit in the criminal law context, there is a concern about a liability "drag net" effect capturing within its confines "all those who have been associated in any degree whatever with the main offenders."[196] Some sort of line is needed to counter this broad liability net. As prior literature has recognized, distinguishing between accidental and deliberate conduct can be a useful tool to achieve this positive legal outcome because it signals a party's motivations; mere accidents are not likely to be repeated intrusions

[194] *See* Ben DePoorter, *Technology and Uncertainty: The Shaping Effect on Copyright Law*, 157 U. PA. L. REV. 1831, 1859 (2009) ("Some individuals may overestimate the legal constraints and forego activities that the state seeks to encourage . . . ."); Uri Weiss, *The Regressive Effect of Legal Uncertainty*, 2019 J. DISPUTE RESOL. 149, 151 (positing that "a shift from a more certain legal regime to a less certain one transfers wealth from risk-averse parties to risk-neutral parties").

[195] *See Sony Goes to Battle*, *supra* note 81.

[196] United States v. Falcone, 109 F.2d 579, 581 (2d Cir. 1940).

upon one's rights.[197] While some have eschewed the value of intent in torts in favor of, say, cost-benefit analyses,[198] the legislature and courts have found these sort of intent-based distinctions necessary to avoid unjust results in both the criminal and tort context.[199] As legal philosopher John Finnis has explained, intent is not just about creating a risk of a particular outcome occurring, but actually trying to bring it about.[200] Finnis's explanation matches the logic of the *Sony* and *Grokster* courts, as well as several parts of the DMCA. But intent, at least as used by the courts and Congress in Part II, can also take the form of a spectrum where infringements being highly likely to occur can suggest enough of an indicia of intent to result in liability, such as with the AHRA's prohibition on second generation copying, the DMCA's repeat infringer policies, or willful blindness.

This is not to say that intent is a perfect line, as legal tools are almost necessarily imperfect. For example, the repeat infringer policy and its implementation are requirements of all DMCA safe harbors, including those for digital network communications (i.e., Internet access).[201] In practice, this intent-based requirement means that repeat infringers would lose access to the Internet (at least from that particular provider), despite Internet access being a fundamental requirement for daily life in the twenty-first century.[202] Another example is § 512(m), which says service providers do not need to take proactive measures to limit infringement.[203] Taken together with requiring takedowns

[197] Neil M. Gorsuch, *Intention and the Allocation of Risk*, *in* REASON, MORALITY, & LAW: THE PHILOSOPHY OF JOHN FINNIS 413, 419-20 (John Keown & Robert P. George eds., 2013); Richard A. Epstein, *A Clear View of* The Cathedral*: The Dominance of Property Rules*, 106 YALE L.J. 2091, 2100 (1997).

[198] *See, e.g.*, RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 260-65 (2011) (advocating for a law and economics approach to torts).

[199] *See* Gorsuch, *supra* note 197, at 420-21.

[200] John M. Finnis, *Allocating Risks and Suffering: Some Hidden Traps*, 38 CLEV. ST. L. REV. 193, 201 (1990).

[201] *See* 17 U.S.C. §§ 512(a), 512(i).

[202] *See* BMG Rts. Mgmt. (US) LLC v. Cox Commc'ns, Inc., 881 F.3d 293, 304-05 (4th Cir. 2018) (finding that Cox failed to implement its repeat infringer policy because it did not terminate Internet access for any repeat infringers); *see also* Wu, *supra* note 69, at 400 (criticizing blocking Internet access as extreme because it would prevent the subscriber's infringing and noninfringing activities).

[203] *See* 17 U.S.C. § 512(m).

whenever knowledge is required, this could disincentivize platforms — beyond the wealthiest, such as YouTube and Facebook — from taking any proactive actions against infringement.[204] As another example, service providers must accept rights owners' infringement notices at face value and remove the reported content to maintain the DMCA safe harbor, even if they are reporting (suspected) non-infringing content.[205] Despite these and other imperfections, intent can nonetheless be a useful framework for the incentives-access balance and achieving related goals such as innovation and free speech, as shown by its success in past architectural infringement cases.

Third, intent is a broad category that provides necessary flexibility for responding to new information architectures. The second definition of intent under the *Restatement (Third) of Torts* is more expansive than the first. While the first definition of intent is where one intends a particular result, the second definition is where one acts knowing that a result is substantially certain to occur if an action is or is not taken.[206] This broader second definition can capture the first definition, acting with the purpose of achieving a consequence.[207] Yet courts and Congress can distinguish between purpose and knowledge-based intent.[208] For example, the inducement doctrine adopted in *Grokster* imposes categorical secondary liability for purposefully inducing user infringement.[209] This broader framework gives courts and Congress more flexibility to adapt copyright law to future information architectures while maintaining copyright's incentives-access balance. New technologies can contain unexpected features that the law has not yet addressed. The breadth of intent makes it an attractive polestar for copyright's secondary liability doctrine because it provides courts and Congress with the necessary room to maneuver and still be able to address whatever new technologies may emerge.

---

[204] *See id.* § 512(c)(1)(A) (requiring takedowns once knowledge of infringement is acquired).

[205] *See id.* § 512(c)(1)(C).

[206] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL AND EMOTIONAL HARM § 1 (AM. L. INST. 2010).

[207] *See id.*

[208] *See id.* § 1 cmt. a.

[209] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 933-35 (2005).

Fourth, a somewhat related benefit of intent as a framework is that it can accommodate different doctrinal approaches. Intent's fluidity allows refinements to secondary liability to follow different doctrinal approaches, which is further facilitated by the flexibility of common law-derived secondary liability itself. For example, intent allows courts and Congress to draw from existing doctrine, as was the case in *Sony* and *Grokster*, or create sui generis approaches, like with the DMCA.[210]

Fifth, intent is not an exclusionary polestar. As a framework, it does not bar other additional considerations from emerging, such as consumer welfare or free speech, that are, at present, less obvious in the historical cases but could nonetheless have important ramifications for future cases.[211] These aspects allow courts and Congress to adapt the analytical framework as new work or technologies emerge that necessitate such a shift.

Finally, intent can also help actualize the traditionally invoked goals of secondary liability in tort, at least under the utilitarian approach of the *Restatement*.[212] The two common law tort secondary liability theories

[210] *See id.* at 936 (adopting inducement from patent law); 17 U.S.C. § 512 (adopting a new safe harbor structure); Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 441-42 (1984) (incorporating the staple article of commerce doctrine from patent law); *see also* Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 672-73 (9th Cir. 2017) (providing developed versions of contributory and vicarious liability tests).

[211] *See* Tim Wu, *The Copyright Paradox*, 2005 SUP. CT. REV. 229, 249-51 (2006) (arguing that social welfare costs and benefits, not intent (at least as understood by the inducement doctrine in *Grokster*), should be the focus for third-party copyright infringement liability, but advocating for the role of Congress rather than the courts in making these technology-type judgments).

[212] Intent could also be consistent with other tort theories, including corrective justice, civil recourse, and law and economics (cheapest cost avoider), but this is for future scholarship. *See generally* GUIDO CALABRESI, THE COST OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 24-29 (1970) (describing cheapest cost avoider theory); JOHN C. P. GOLDBERG & BENJAMIN C. ZIPURSKY, RECOGNIZING WRONGS 3, 263 (2020) (describing civil recourse theory and the authors' reframing of it as "redress-for-wrongs"); ARTHUR RIPSTEIN, PRIVATE WRONGS 4-6 (2016) (describing corrective justice); ERNEST J. WEINRIB, THE IDEA OF PRIVATE LAW 56-83 (2012) (describing corrective justice); Guido Calabresi & Spencer Smith, *On Tort Law's Dualisms*, 135 HARV. L. REV. F. 184, 184 (2022) (explaining that "[i]f you fixate only on one side or the other [of this debate between wrongs and redress and preventing harms], you fail to appreciate the whole of tort law"); Catherine M. Sharkey, *Modern Tort Law: Preventing Harms, Not Recognizing Wrongs*, 134 HARV. L. REV. 1423, 1424-25 (2021) (reviewing JOHN C. P. GOLDBERG & BENJAMIN C. ZIPURSKY,

that are most relevant to copyright infringement are aiding and abetting (contributory infringement's corollary) and vicarious liability.[213] Aiding and abetting is a fault-based form of liability that requires knowledge and substantial assistance.[214] The *Restatement* (*Second*) *of Torts* justified aiding and abetting liability because "[a]dvice or encouragement to act operates as a moral support to a tortfeasor."[215] The knowledge requirement allows courts to make nuanced inquiries into culpability (i.e., bad intent) based on how much the actor knew to punish the most blameworthy.[216] This makes intuitive sense given the moral justification: if aiding and abetting liability was available for *any* party who unknowingly aided a tortious act, a range of otherwise innocent parties would be liable.[217] An overbroad knowledge requirement would not only be unjust, but unworkable.

The substantial assistance requirement, meanwhile, cabins liability to those who were involved enough to merit moral condemnation. The *Restatement* (*Third*) explains that substantial assistance means "active participation," as determined by a holistic analysis of the circumstances.[218] This definition is nebulous, but courts have further elucidated the meaning. For example, the Supreme Court in *Twitter, Inc. v. Taamneh* relied upon the D.C. Circuit's decision in *Halberstam v. Welch*, a "leading case on civil aiding-and-abetting."[219] In *Halberstam*, the

RECOGNIZING WRONGS (2020)) (critiquing Goldberg and Zipursky's wrongs-based theory of tort law in favor of "cheapest cost avoider" tort theory).

[213] *See* Bartholomew & McArdle, *supra* note 16, at 694-96 (explaining that aiding and abetting liability is the main source of courts' commentary about contributory liability).

[214] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR ECON. HARM § 28 (AM. L. INST. 2020).

[215] RESTATEMENT (SECOND) OF TORTS § 876 cmt. d (AM. L. INST. 1979).

[216] *See* Charles W. Adams, *Indirect Infringement from a Tort Law Perspective*, 42 U. RICH. L. REV. 635, 639-40 (2008); Yen, *Torts and the Construction of Inducement*, *supra* note 16, at 530.

[217] *See, e.g.*, David S. Ruder, *Multiple Defendants in Securities Law Fraud Cases: Aiding and Abetting, Conspiracy,* In Pari Delicto*, Indemnification, and Contribution*, 120 U. PA. L. REV. 597, 630-31 (1972) (describing how such an all-encompassing theory of liability would, for example, hold banks liable merely for loaning money).

[218] *See* RESTATEMENT (THIRD) OF TORTS: LIAB. FOR ECON. HARM § 28 cmt. d (AM. L. INST. 2020).

[219] Twitter, Inc. v. Taamneh, 598 U.S. 471, 485 (2023); *see also* Cent. Bank, N.A. v. First Interstate, N.A., 511 U.S. 164, 181 (1994) (describing *Halberstam* as a "comprehensive opinion on the subject").

court had to decide whether a serial burglar's live-in partner aided and abetted a murder that occurred during one of the break-ins.[220] Based on an extensive survey of state law, federal law, the *Restatement* (*Second*), and leading treatises, the *Halberstam* court articulated six factors to determine when assistance was "substantial": (1) the nature of the tort; (2) the amount and type of assistance; (3) the defendant's presence during the commission of the tort; (4) the third party's relationship with the tortfeasor; (5) the third party's state of mind (which could include intent); and (6) the duration of the assistance.[221] The court determined that the burglar's partner was liable for aiding and abetting the murder because she continuously assisted him in laundering his pilfered gains, showing her desire for the thievery to succeed, and the victim's death was a foreseeable result of these crimes.[222] While the six factors formed the basis of the aiding and abetting finding in that case, the court recognized that these factors could, and even should, be modified in different circumstances.[223] Other courts have invoked *Halberstam* and applied similar factors to the aiding and abetting claims before them.[224] In the *Taamneh* case, the Supreme Court especially relied on the lack of intent of the defendant platforms to facilitate terrorism to find that they had not aided and abetted a terrorist attack in Istanbul.[225] In a recent bankruptcy court case, the court applied *Taamneh* to contributory copyright liability, noting that "culpability is the same core trunk from which contributory copyright infringement jurisprudence grows."[226] Taking it a step further, in *Cox*, the Fourth Circuit highlighted the connection between culpability and intent, noting that a defendant

[220] Halberstam v. Welch, 705 F.2d 472, 474-76 (D.C. Cir. 1983).

[221] *See id.* at 483-84.

[222] *See id.* at 488.

[223] *See id.* at 489.

[224] *See, e.g.*, Bernhardt v. Islamic Republic of Iran, 47 F.4th 856, 870 (D.C. Cir. 2022) (applying *Halberstam* to JASTA liability for terrorism); Honickman v. BLOM Bank SAL, 6 F.4th 487, 495-500 (2d Cir. 2021) (same); Fassett v. Delta Kappa Epsilon, 807 F.2d 1150, 1163 (3d Cir. 1986) (applying *Halberstam* in the context of an automobile accident stemming from intoxication of a minor at a fraternity party); Thompson v. Trump, 590 F. Supp. 3d 46, 122-24 (D.D.C. 2022) (applying *Halberstam* to the January 6, 2021 case involving President Trump).

[225] Twitter, Inc. v. Taamneh, 598 U.S. 471, 504-05 (2023).

[226] *In re* Frontier Commc'ns Corp., 658 B.R. 277, 299 (Bankr. S.D.N.Y. 2024).

"providing the means to infringe *is* culpable pursuant to the common law rule that a person is presumed to intend the substantially certain results of his acts."[227]

Vicarious liability, comparatively, stems from one's relationship with and control over the direct tortfeasor, irrespective of their own participation in or knowledge of the tort.[228] For example, the most well-known form of vicarious liability is respondeat superior, or holding an employer responsible for the torts of their employees.[229] There is no singular normative justification for vicarious liability.[230] Popular suggested rationales include (1) compensating the victim,[231] (2) imposing liability on who controlled the direct infringer,[232] (3) deterring unwanted conduct,[233] (4) allocating costs to an

[227] Sony Music Ent. v. Cox Commc'ns., Inc., 93 F.4th 222, 236 (4th Cir. 2024).

[228] *See* RESTATEMENT (THIRD) OF AGENCY § 7.03 cmt. b (AM. L. INST. 2006) (explaining that a principal may be held liable for its agent's torts if they were within the scope of the engagement); *see also* John Gardner, *Complicity and Causality*, 1 CRIM. L. & PHIL. 127, 130 n.2 (2007).

[229] *See* Daniela Glavaničová & Matteo Pascucci, *Making Sense of Vicarious Responsibility: Moral Philosophy Meets Legal Theory*, 89 ERKENNTNIS 107, 109 (2022).

[230] ANTHONY GRAY, VICARIOUS LIABILITY: CRITIQUE AND REFORM, at ix (2018) (noting that despite "a long case history reflecting such a doctrine, a satisfactory unifying rationale for the imposition of such liability remains elusive").

[231] *See* Alan O. Sykes, *The Economics of Vicarious Liability*, 93 YALE L.J. 1231, 1235-36 (1984) (arguing that it is Pareto optimal to hold wealthier principals liable).

Bartholomew, *supra* note 103, at 465 (explaining that vicarious liability is often justified as cost redistribution).

[232] *See* ERNEST W. HUFFCUT, ELEMENTS OF THE LAW OF AGENCY § 149(1) (1895) ("It is universally conceded that the principal is liable for all torts which he commands or ratifies."); Glavaničová & Pascucci, *supra* note 229, at 114 (explaining that control has been a common justification for vicarious liability). *But see* Sykes, *supra* note 231, at 1245-56, 1261-71 (explaining that efficiency depends not just on the principal's control, but on the *extent* of control).

[233] *See* ROBERT STEVENS, TORTS AND RIGHTS 258 (2007) (explaining how vicarious liability may encourage principals to take appropriate actions to prevent their agents from engaging in tortious conduct).

enterprise,[234] and (5) punishing voluntary involvement.[235] None of these theories are complete explanations, as they would all lead to overbroad liability, such as holding wealthy parties liable merely for purposes of compensating victims. Guido Calabresi's "cheapest cost avoider" theory reflects some of these justifications by holding liable the party most able to prevent tortious conduct in the future.[236] The second, third, and fifth rationales and Calabresi's theory suggest that vicarious liability should punish the party that was ultimately responsible for the tortious conduct or could have stopped it from occurring. This is reflected in the *Restatement (Third)*, which suggests that the vicarious party is financially *responsible* for the tort.[237]

Similar considerations to both forms of secondary liability have borne out in the intellectual property law literature. Stacey Dogan, for example, has noted that there is a difference between "the innocent intermediary and one whose technology and business model deliberately seek to confuse."[238] She posited that courts have relied upon three normative values in applying secondary liability to platforms: (i) balancing effective relief for rights owners with non-interference with legitimate commerce; (ii) culpability of the third party (which suggests bad intent); and (iii) reasonableness or feasibility in the third party's responses to notices of infringement.[239] Jane Ginsburg also evocatively

---

[234] *See* PETER CANE, RESPONSIBILITY IN LAW AND MORALITY 176 (2002) (describing vicarious liability as a "form of relational activity-based responsibility"); Glavaničová & Pascucci, *supra* note 229, at 118-19 (describing how employers voluntarily hire employees, lenders voluntarily lend their car to borrowers, and parents voluntarily become caregivers to children).

[235] *See* GRAY, *supra* note 230, at 111 ("[A] particular enterprise should have costs allocated to it that fairly reflect the cost of it doing business. . . . An enterprise should be liable for the costs it causes.").

[236] CALABRESI, *supra* note 212, at 155.

[237] RESTATEMENT (THIRD) OF TORTS: APPORTIONMENT LIAB. § 13 cmt. b (AM. L. INST. 2000).

[238] Dogan, "*We Know It When We See It*," *supra* note 64, ¶ 19 (describing the Second Circuit's decision in *Rescuecom*, which, while nominally a direct trademark infringement action, discussed Google's inducement and culpability).

[239] *See* Stacey L. Dogan, *Principled Standards vs. Boundless Discretion: A Tale of Two Approaches to Intermediary Trademark Liability Online*, 37 COLUM. J.L. & ARTS 502, 504-14 (2014) [hereinafter Dogan, *Principled Standards vs. Boundless Discretion*] (applying the approach to trademarks, but noting that it could apply to copyright too).

described secondary liability as a dividing line between Sony-like sheep (well-meaning actors) and Grokster-like goats (bad actors), also suggesting a role for intent.[240]

These goals and lines are beneficial, but they are difficult for courts to apply in the future due to the vast amount of space they do not cover.[241] For example, how do we determine wrongdoing or culpability? Balance and reasonability are laudable goals, but how do we achieve them? Even the ubiquitous "reasonable person" in tort law is "fluid and sponge-like," an "inherently definition-resistant standard."[242] As explained above, there must be limits to imposing secondary liability on the biggest pockets.[243] In short, these traditional normative purposes for secondary liability are helpful, but difficult to apply.[244]

Intent can help actualize these nebulous goals of common law tort and prior scholars' work — punishing wrongdoing, shifting damages to the cheapest cost avoider, culpability, reasonability, and balance. A wrongdoer or culpable actor would not merely exist in the ether but be one who acted in an intentional manner knowing that their action or lack thereof would facilitate a specific infringement. Intent can help craft the dividing line that allows for reasonability and balance by identifying those we would most wish to hold liable rather than relying on more amorphous concepts. It could also contribute to the cheapest cost avoider theory by looking more closely at what an actor could have done. While not coterminous with these broader goals of tort law, intent facilitates the introduction of these goals into copyright law refinements alongside more core copyright concerns.

---

[240] Ginsburg, *supra* note 64, at 608-09.

[241] *See id.* (emphasizing the importance of the dividing line between *Sony* and *Grokster*); Dogan, *Principled Standards vs. Boundless Discretion*, *supra* note 239, at 504-13 (identifying the goals of balance, culpability, and reasonability).

[242] Haim Abraham, *Queering the Reasonable Person*, *in* DIVERSE VOICES IN TORT LAW 1, 7-8 (Kirsty Horsey ed., 2023).

[243] *Supra* notes 228–237 and accompanying text.

[244] *See, e.g.*, Transcript of Oral Argument at 50, Nike v. Kasky, 539 U.S. 654 (2003) (Justice Breyer explaining that "[w]hat I'm really looking for is help in writing a hypothetical opinion. I have to write a standard, or a rule . . . .").

IV. APPLYING INTENT TO EMERGING INFORMATION ARCHITECTURES

To demonstrate how the surfaced intent framework could potentially animate innovation-promoting, copyright-respectful responses to future architectural infringement claims, consider two emerging information architectures. Generative AI and blockchain-based Web3 technologies may represent the next architectural infringement claims that could necessitate further refinements to secondary copyright infringement liability. Assuming infringements are perpetrated through these technologies, intellectual property law could stymie these emerging information architectures due to novel aspects that could lead to overbroad secondary liability, unbalancing copyright. Providers of generative AI cannot predict the expression in particular outputs, raising a novel question of who should be liable for AI-generated infringement.[245] In the case of Web3, blockchain's immutability (imperviousness to deletion) presents a novel aspect that does not comport with current notice-and-takedown structures under copyright law. Therefore, courts will have to refine secondary liability if these information architectures are to flourish but will need to do so in a copyright-respectful manner to avoid weakening copyright owners' rights. The following examines the architectural infringement conundrums posed by these new technologies and offers potential intent-driven responses.

[245] *See* Andres Guadamuz, *A Scanner Darkly: Copyright Liability and Exceptions in Artificial Intelligence Inputs and Outputs*, 73 GRUR INT'L 111, 111-12 (2024).

A. Generative AI

1. Generative AI Technology

Generative AI is the technology *du jour*.[246] Generative AI can create vivid award-winning art,[247] excel at the bar exam,[248] and write new songs in the style and voice of deceased stars.[249] Generative AI systems such as ChatGPT and Midjourney have become household names. This revolution in AI was made possible through machine learning. Machine learning is the process by which computers use algorithms to learn from (and improve through) data.[250] Developers provide the training data and model and users provide the prompts, but the system "learns" from the training material to best achieve its goal and create a responsive output.[251]

Yet the self-programming nature of machine learning means AI systems are becoming increasingly autonomous.[252] While machine learning has existed for decades, much faster computers and larger

[246] *See* Tal Elyashiv, *Winning Web3 Investment Strategies Must Combine Artificial Intelligence and Blockchain Technology*, NEWSWEEK (Aug. 14, 2023), https://www.newsweek.com/winning-web3-investment-strategies-must-combine-artificial-intelligence-blockchain-technology-1819218 [https://perma.cc/2JST-SQ6V] ("Artificial Intelligence (AI), specifically generative AI, is definitely having its 'moment' right now. . . . And to think, right before AI burst onto the scene, a different new technology was investors' darling, gaining momentum and increased attention. Remember blockchain?").

[247] Kevin Roose, *An A.I.-Generated Picture Won an Art Prize. Artists Aren't Happy.*, N.Y. TIMES (Sept. 2, 2022), https://www.nytimes.com/2022/09/02/technology/ai-artificial-intelligence-artists.html.

[248] Debra Cassens Weiss, *Latest Version of ChatGPT Aces Bar Exam with Score Nearing 90th Percentile*, ABA J. (Mar. 16, 2023, 1:59 PM), https://www.abajournal.com/web/article/latest-version-of-chatgpt-aces-the-bar-exam-with-score-in-90th-percentile [https://perma.cc/X39U-KK6F].

[249] Steve Brachmann, *Senate IP Subcommittee Mulls Federal Right of Publicity at AI and Copyright Hearing*, IPWATCHDOG (July 13, 2023, 3:15 PM), https://ipwatchdog.com/2023/07/13/senate-ip-subcommittee-mulls-federal-right-publicity-ai-copyright-hearing/id=163469 [https://perma.cc/D47N-65KP].

[250] Guadamuz, *supra* note 245, at 113; *see also* 15 U.S.C. § 9401(11) (defining machine learning).

[251] Mark A. Lemley & Bryan Casey, *Remedies for Robots*, 86 U. CHI. L. REV. 1311, 1324 (2019) [hereinafter Lemley & Casey, *Remedies for Robots*].

[252] Andrew Tutt, *An FDA for Algorithms*, 69 ADMIN. L. REV. 83, 100 (2017).

quantities of data facilitated its recent explosive growth.[253] AI's increasing complexity and reliance on machine learning means specific outputs are unpredictable.[254] The path the AI system follows can be complex, unexpected, and inexplainable.[255] Machine learning often incorporates randomness, which can help achieve the best outcome, but at the cost of accountability and reproducibility.[256] Continuous learning by AI systems exacerbates output unpredictability.[257] Together, this means that even developers may not be able to precisely know a generative AI system's outputs in advance.[258]

Yet the unpredictability of an AI system's outputs is what enables generative AI to go beyond human capabilities and offer novel outputs.[259] As Harry Surden has noted, older hand-coded AI systems struggled with more amorphous tasks such as image generation.[260] For these sorts of questions, there is not one right answer. For example, hard coding an understanding of "dog" as only German Shepherds or Poodles may miss other types of dogs, such as Scottish Terriers and

[253] Ryan Calo, *Artificial Intelligence Policy: A Primer and Roadmap*, 51 UC DAVIS L. REV. 399, 405 (2017).

[254] Samuel R. Bowman, *Eight Things to Know About Large Language Models*, ARXIV:2304.00612, at 2-4 (2023).

[255] Deven R. Desai & Joshua A. Kroll, *Trust but Verify: A Guide to Algorithms and the Law*, 31 HARV. J.L. & TECH. 1, 26 (2017).

[256] Kroll et al., *supra* note 23, at 653-56.

[257] Omri Rachum-Twaig, *Whose Robot Is It Anyway?: Liability for Artificial-Intelligence-Based Robots*, 2020 U. ILL. L. REV. 1141, 1148 (2020).

[258] *See* P. Bernt Hugenholtz & João Pedro Quintais, *Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?*, 52 IIC 1190, 1212 (2021) ("Due to the 'black box' nature of some AI systems, persons in charge of the conception phase will sometimes not be able to precisely predict or explain the outcome of the execution phase."); Anat Lior, *AI Entities as AI Agents: Artificial Intelligence Liability and the AI Respondeat Superior Analogy*, 46 MITCHELL HAMLINE L. REV. 1043, 1057 (2020) ("[T]he decision-making process[] itself takes place in a virtual 'black-box' and is unknown to the human creator or user.").

[259] *See* Mindy Nunez Duffourc, *Malpractice by the Autonomous AI Physician*, 2023 J.L., TECH. & POL'Y 1, 19 (2023) (discussing the benefits of unpredictable outputs in the health AI context).

[260] *Cf.* Harry Surden, *Artificial Intelligence and Law: An Overview*, 35 GA. ST. U. L. REV. 1305, 1324-25 (2019).

Shetland Sheepdogs, whereas an organic learning process can lead to an AI system recognizing dogs more holistically.[261]

Although the unpredictable nature of the AI systems' outputs brings benefits, some harms will be genuinely unforeseeable despite developers' best efforts.[262] This unpredictability would seem to create the very real risk of copyright infringement liability.[263]

2. Balancing Prospective Architectural Infringement Risks

Generative AI's use as a tool by users to create and disseminate content continues the long development of information architectures from the printing press. Like its predecessors that were the subject of architectural infringement claims, generative AI is a novel information technology, barriers to entry for users are relatively low, it has been adopted by a large population, and it has long-term potential. Generative AI is different from prior information architectures in that it does not just distribute copied information to users but produces "new" information itself. Nonetheless, like its predecessors, it is likely to face architectural infringement challenges stemming from its novel feature, in this case the semiautonomous creation of content. Indeed, such claims have already been alleged in some copyright infringement cases, including *Andersen v. Stability AI Ltd.*, where the plaintiffs allege a secondary liability theory premised on the argument that "Stable Diffusion *by operation* by end users creates copyright infringement and was created to facilitate that infringement by design."[264]

There is already a significant amount of literature on AI and copyright law. Much of this work has focused on the question of whether AI-generated outputs can be copyrightable.[265] At present, the literature and

[261] *See* Desai & Kroll, *supra* note 255, at 28 (explaining that adding randomness into an AI system can further help it gain a better understanding of the task and address any challenges it encounters).

[262] Lemley & Casey, *Remedies for Robots*, *supra* note 251, at 1334.

[263] *Id.* at 1335.

[264] Andersen v. Stability AI Ltd., No. 23-cv-00201-WHO, 2024 WL 3823234, at *6 (N.D. Cal. Aug. 12, 2024).

[265] *See, e.g.*, Ryan Abbott & Elizabeth Rothman, *Disrupting Creativity: Copyright Law in the Age of Generative Artificial Intelligence*, 75 FLA. L. REV. 1141, 1183 (2023) (arguing that AI-generated works should be copyrightable because they will encourage the creation

courts are focused on the question of whether training a generative AI system on copyrighted content is a permissible fair use.[266] If training is

and dissemination of AI-generated works); Annemarie Bridy, *Coding Creativity: Copyright and the Artificially Intelligent Author*, 2012 STAN. TECH. L. REV. 5, 27 (2012) (suggesting that the work for hire doctrine could be an appropriate structure for computer-generated works, but acknowledging that the current language in the Copyright Act would not permit it); Daniel J. Gervais, *The Machine as Author*, 105 IOWA L. REV. 2053, 2105-06 (2020) (providing normative and doctrinal arguments for and against protection, ultimately rejecting copyright protection for AI-generated outputs); Jane C. Ginsburg & Luke Ali Budiardjo, *Authors and Machines*, 34 BERKELEY TECH. L.J. 343, 446-47 (2019) (classifying four ways to allocate authorship with machine-generated works and determining that an output is "authorless" and not copyrightable where human authors are not sufficiently involved and could not be said to collaborate in the creation); James Grimmelmann, *There's No Such Thing as a Computer-Authored Work — And It's a Good Thing, Too*, 39 COLUM. J.L. & ARTS 403, 403 (2016) ("Copyright law doesn't recognize computer programs as authors, and it shouldn't."); Edward Lee, *Prompting Progress: Authorship in the Age of AI*, 76 FLA. L. REV. 1445, 1454-56 (2024) (arguing that restricting copyrights to human authors, not AI systems, is wrong); Pamela Samuelson, *Allocating Ownership Rights in Computer-Generated Works*, 47 U. PITT. L. REV. 1185, 1192 (1986) ("The Article concludes that, in general, the user of a computer generator program should be considered the author of a computer generated work, and should be free to exploit this product commercially."); Haochen Sun, *Redesigning Copyright Protection in the Era of Artificial Intelligence*, 107 IOWA L. REV. 1213, 1217 (2022) ("AI works generated with human contributions should be awarded *sui generis* rights designed specifically to protect this type of IP. However, AI works generated solely by autonomous AI systems should be placed in the public domain without copyright protection.").

[266] *See, e.g.*, Peter Henderson, Xuechen Li, Dan Jurafsky, Tatsunori Hashimoto, Mark A. Lemley & Percy Liang, *Foundation Models and Fair Use*, 23 J. MACH. LEARNING RSCH. 1, 6 (2023) ("For generative models like DALL-E or GPT that produce creative outputs, the situation is less likely to be problematic if the outputs do not copy a substantial portion of any existing work but instead transform the input into totally different outputs, in line with the fair use doctrine."); Katherine Lee, A. Feder Cooper & James Grimmelmann, *Talkin' 'Bout AI Generation: Copyright and the Generative-AI Supply Chain*, J. COPYRIGHT SOC'Y (forthcoming 2025) (manuscript at 98, 100), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4523551 [https://perma.cc/9TWV-6677] (concluding that training a generative AI system and AI-generated outputs could be fair uses, or not, depending on the nature of the generated outputs); Lemley & Casey, *Fair Learning*, *supra* note 23, at 770-79 (describing training an AI system on copyrighted data as relying on the unprotectable parts of copyrighted works); Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem*, 93 WASH. L. REV. 579, 619-29 (2018) (describing AI training as being highly transformative and only using the factual content of copyrighted works); Matthew Sag, *Copyright Safety for Generative AI*, 61 HOUS. L. REV. 295, 340-41 (2023) [hereinafter Sag, *Copyright Safety*] ("Using copyrighted works as training data for generative AI is likely to be fair use if appropriate

found to be a fair use — as is expected by most scholars — courts will then have to determine on a case-by-case basis whether a specific AI-generated output is a lawful fair use or infringement.[267] There is a growing consensus that at least some of these outputs will be infringing.[268] For example, Matthew Sag has been able to cause Midjourney and Stable Diffusion to reproduce images of the famous Peanuts' beagle, Snoopy.[269] Because AI systems are able "to accomplish both useful and unfortunate tasks in unexpected ways,"[270] it is likely inevitable that they will perpetrate infringements despite the best efforts of their developers.

The semiautonomous nature of generative AI is unprecedented, raising questions about who should be liable for resulting copyright infringements and under what circumstances.[271] The threshold consideration is who the direct infringer should be. While the answer to that question could have significant ramifications for generative AI, we only reach the unique risks of architectural infringement if there is an

precautions are taken."); Samuelson, *supra* note 23, at 1558 (concluding that "the AI training uses are likely to be considered transformative."). *But see* Benjamin L.W. Sobel, *Artificial Intelligence's Fair Use Crisis*, 41 COLUM. J.L. & ARTS 45, 65-66 (2017) (arguing that fair use may not apply).

[267] *See, e.g.*, Lemley & Casey, *Fair Learning*, *supra* note 23, at 770-79 (describing training an AI system on copyrighted data as relying on the unprotectable parts of copyrighted works); Levendowski, *supra* note 266, at 619-29 (describing AI training as being highly transformative and only using the factual content of copyrighted works); Sag, *Copyright Safety*, *supra* note 266, at 336 (noting that "LLMs are capable of memorizing aspects of their training data" and creating infringing outputs).

[268] *See, e.g.*, Henderson et al., *supra* note 266, at 2 ("[T]he risk of infringement is real, and fair use will not cover every scenario where a foundation model is created or used."); Lee et al., *supra* note 266, at 110 ("Some outputs from these models will incorporate copyrighted material that will be seen by humans — indeed, some generations will infringe."); Lemley & Casey, *Fair Learning*, *supra* note 23, at 766-67 (noting that machine learning systems are capable of replicating works); Sag, *Copyright Safety*, *supra* note 266, at 309 (concluding that "these machine learning models still qualify as nonexpressive use so long as the outputs are not substantially similar to any particular original expression in the training data"); Samuelson, *supra* note 23, at 1555 ("It is, of course, possible for outputs of generative AI to infringe derivative work rights.").

[269] Sag, *Copyright Safety*, *supra* note 266, at 330.

[270] Ryan Calo, *Robotics and the Lessons of Cyberlaw*, 103 CALIF. L. REV. 513, 515 (2015).

[271] *See* Lemley & Casey, *Remedies for Robots*, *supra* note 251, at 1353 ("[I]f the AI is self-learning, we may really never know who is to blame.").

accusation of systemic *secondary* liability.[272] Therefore, for purposes of this Article, the direct infringer is assumed to be the user or possibly the AI system itself.[273] The latter approach is not unprecedented; other scholars have suggested that the AI system should be directly liable.[274] And the ample literature on generative AI has not yet focused on secondary liability risks.

Finding the AI system to be the direct infringer likely does not allow the developer (or any entities involved in the system's creation upstream from the end-user) to avail itself of the DMCA safe harbor, since the content would not be user-created,[275] but it could allow courts to further refine secondary liability to maintain the incentives-access balance and not unreasonably endanger generative AI. Looking to intent suggests that vicarious liability alone could unsettle balanced copyright by either imposing de facto liability on generative AI systems' operators or completely excusing them from liability. While Congress could craft a bespoke solution like it did for the Internet with the DMCA, a sui generis refinement to the contributory liability test — this Article proposes "notice-and-revision" — could maintain the incentives-access balance by imposing obligations on operators consistent with the technology to avoid chilling innovation in the space.

[272] *See supra* Part I (defining architectural infringement).

[273] I examine the refinement of copyright direct liability and defend this proposal for generative AI in a separate article. *See* Goodyear, *supra* note 33, at pt. IV.A.

[274] *See, e.g.*, SAMIR CHOPRA & LAURENCE F. WHITE, A LEGAL THEORY FOR AUTONOMOUS ARTIFICIAL AGENTS 119, 121 (2011) (describing how an AI system could be thought of as an independent actor or agent); Jack B. Balkin, *The Path of Robotics Law*, 6 CALIF. L. REV. CIR. 45, 58 (2015) ("When we employ legal fictions of this kind, we substitute robot for human to allow the law to function effectively in the face of the legal enigmas posed by emergent behavior. Or we might adopt legal fictions to keep existing legal doctrines working provisionally until we can produce more thorough and coherent reforms."); Chatterjee & Fromer, *supra* note 189, at 1910-11 (hypothesizing that an AI system could be considered to "choose" whether to make a copy).

[275] *See* Henderson et al., *supra* note 266, at 18 ("But it is not obvious that the DMCA safe harbors apply to *generated* content."); Lee et al., *supra* note 266, at 101 ("Although these safe harbors have been significant for technology platforms and for Internet law, none of them are likely to apply to generative AI in most cases.").

a. Unbalanced vicarious liability

At first glance, vicarious liability may seem an appropriate framework for holding developers[276] liable. Some non-copyright scholars have advocated for vicarious liability or agency law as the proper framework because AI systems are not able to compensate injured parties.[277]

But this proposal suffers from two issues: it is unclear whether vicarious liability could even apply under current copyright law and, if it could, it would overly constrain AI companies without considering intent. First, one must both have the right and ability to control the infringement and financially benefit from it to be vicariously liable.[278] The lack of predictability for the outputs would suggest the developer does not have control over the AI system. As Daniel Gervais has noted (albeit in the context of copyrightability), "[T]he AI machine uses its own insights to create."[279] Katherine Lee, A. Feder Cooper, and James Grimmelmann have posited that AI system operators would have the right and ability to control because they could disable the entire system and could filter the outputs.[280] But requiring the developer to delete the entire product goes much further than prior cases have held.[281] Online

[276] I use the term developer to refer to any upstream entity involved in the AI system's creation before the end-user.

[277] *See, e.g.*, Lior, *supra* note 258, at 1071 (advocating "employing an analogy that treats AI entities as agents, as if they were 'servants' of their owners, operators, designers, trainers, or programmers"); Nunez Duffourc, *supra* note 259, at 28 ("Recognizing the Autonomous AI Physician as a legal person for the limited purposes of assigning liability for its malpractice allows it to both be directly liable under a theory of medical malpractice and serve as an agent under a theory of vicarious liability.").

[278] Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 673 (9th Cir. 2017).

[279] Gervais, *supra* note 265, at 2059 (emphasis omitted).

[280] Lee et al., *supra* note 266, at 97.

[281] *See, e.g.*, A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1020-22 (9th Cir. 2001) (imposing liability when, upon receiving knowledge, a platform fails to purge the infringing content); Dunham v. Lei, No. CV 20-3716-DMG (MAAx), 2021 WL 4595808, at *7 (C.D. Cal. June 7, 2021) (removing a storefront selling infringing products); Sony Music Ent. v. Cox Commc'ns, Inc., 464 F. Supp. 3d 795, 813-14 (E.D. Va. 2020), *overturned on other grounds by* 93 F.4th 222 (4th Cir. 2024) (having the "actual ability to stop or limit ongoing infringement by modifying or terminating an account"); Oppenheimer v. Allvoices, Inc., No. C 14-00499 LB, 2014 WL 2604033, at *7 (N.D. Cal. June 10, 2014) (content removal and disabling access to sites with infringing content); Agence France

platforms who cannot prevent infringing content from appearing are typically not held to have the requisite control for vicarious liability.[282] Likewise, here, a finding of control would seem uncertain at best. If control can never exist in the AI context, vicarious liability could never apply to AI developers.

If a court did find control, that would spark the second issue: vicarious infringement is a strict liability offense.[283] A finding of control would lead the court to hold the developer liable for any resulting infringements if there is also a direct financial benefit, which seems likely since generative AI is often producing outputs as part of a subscription service, even if the infringement not necessarily being a draw could weaken that argument.[284] This de facto — and potentially widespread — liability could discourage generative AI innovation and make copyright more rights owner-friendly. The mismatch between strict liability and generative AI has led some scholars to conclude that generative AI requires a paradigm shift away from strict liability altogether.[285]

Presse v. Morel, 934 F. Supp. 2d 547, 575 (S.D.N.Y. 2013) (having the right and ability to control because it could remove allegedly infringing photos and block accounts).

[282] *See, e.g.*, Routt v. Amazon.com, Inc., 584 F. App'x 713, 714-15 (9th Cir. 2014) (finding that plaintiff insufficiently alleged that Amazon could monitor the websites of participants in its affiliate-marketing program and potentially influence the participants' actions and did not allege that Amazon could control or terminate those websites); Luvdarts, LLC v. AT&T Mobility, LLC, 710 F.3d 1068, 1072 (9th Cir. 2013) (AT&T could not supervise its networks for infringing activity).

[283] Yen, *Third Party Copyright Liability*, *supra* note 9, at 214.

[284] *See* Lee et al., *supra* note 266, at 97 ("In many cases, they will not have a direct financial interest in infringing use of the service — but they might if the plaintiff could show that the service's ability to create infringing generations was a major part of its competitive appeal as compared with other generative-AI services."); Pedro Palandrani, *Generating Content and Profits: Examining the Potential Business Models of Generative AI*, NASDAQ (May 9, 2023, 3:40 PM), https://www.nasdaq.com/articles/generating-content-and-profits%3A-examining-the-potential-business-models-of-generative-ai [https://perma.cc/8VB5-DYCX] (describing the different models through which generative AI can profit).

[285] *See, e.g.*, Anna Beckers & Gunther Teubner, *Responsibility for Algorithmic Misconduct: Unity or Fragmentation of Liability Regimes?*, 25 YALE J.L. & TECH. (SPECIAL ISSUE) 76, 80-81, 83-85, 94-95 (2023) (rejecting one-size-fits all approaches to AI liability and proposing looking at the specific use of the AI system and the involvement of the human); Emiliano Marchisio, *In Support of "No-Fault" Civil Liability Rules for Artificial Intelligence*, 1 SN SOC. SCI. 1, 13 (2021) (noting the need to shift the discussion about

Intent also suggests that vicarious liability would be a poor fit for maintaining the incentives-access balance with generative AI. If we are refining secondary liability to maintain the incentives-access balance, applying only de facto vicarious liability would upset that balance one way or another. To avoid this conundrum, courts should hold that the operators of AI systems do *not* have the right and ability to control. This avoids the de facto liability scenario and allows courts to instead turn to inducement and contributory liability to craft a more balanced framework for AI-generated infringement liability.

b. The promise of inducement and contributory liability

Inducement and contributory liability are fault-based standards that allow more flexibility and consideration of intent.[286] While inducement can remain unaltered, refinements to contributory liability for AI-generated outputs will likely turn on the material contribution requirement. This subsection offers notice-and-revision as a potential permutation of how contributory liability could be refined in an intent-conscious manner in response to architectural infringement claims involving generative AI.

The Supreme Court's decisions in *Sony* and *Grokster* provide a powerful threshold dividing line for contributory liability between platforms that are intentionally furthering or forbearing from preventing infringement and those that are not. Generative AI does not pose any novel issues for *Sony* and *Grokster*. The two decisions help separate innocent and intentionally infringing parties.[287] Generative AI technologies seem well-suited to the *Sony* safe harbor for substantial noninfringing uses.[288] Almost undoubtedly some content connected to them will be infringing, but many (if not most) of the uses appear

obligations away from producers and programmers when robots can act autonomously from their original design); Rachum-Twaig, *supra* note 257, at 1153 (examining how the unpredictability of AI raises material normative problems for applying direct or vicarious liability).

[286] *See* Yen, *Third Party Copyright Liability*, *supra* note 9, at 214-15.

[287] *See* Ginsburg, *supra* note 64, at 585.

[288] *See* Sony Corp. v. Universal City Studios, Inc., 464 U.S. 417, 442 (1984).

legitimate, such as original works of art or fair uses.[289] But *Grokster* offers an important corollary that imposes liability on system providers that induced infringement through "purposeful, culpable expression and conduct."[290] A developer that encourages the use of their AI system to create harmful, substantially similar copies, or a user who actively seeks to have the AI system create such outputs, could be held liable for inducement.

After the court passes the *Sony-Grokster* threshold, the intent framework suggests that the material contribution requirement for contributory liability should be refined for generative AI in a manner that obliges generative AI developers to act once they know of specific infringements. The DMCA's notice-and-takedown structure could provide a useful corollary. The DMCA would almost certainly not apply to generative AI if the user is not the direct infringer. However, a parallel notice-and-takedown structure has emerged in contributory liability doctrine, where material contribution requires content removal (i.e., the "takedown").[291] As explained above, notice-and-takedown puts the onus on the rights owner to report instances of infringement to the service provider, and then the service provider must remove the reported content to maintain its safe harbor.[292] This prevents the platform from being held liable merely because infringement happens to occur on its platform, instead only requiring action once the specific

[289] *See, e.g.*, Sag, *Copyright Safety*, *supra* note 266, at 336 (noting that infringing outputs are likely relatively rare, although they will occur sometimes).

[290] Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 937 (2005).

[291] *See, e.g.*, Bus. Casual Holdings, LLC v. YouTube, LLC, No. 22-3007-cv, 2023 WL 6842449, at *2 (2d Cir. Oct. 17, 2023) (per curiam) (declining to find material contribution when YouTube "acted to remedy, TV-Novosti's infringement" by removing the infringing content); A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1020-22 (9th Cir. 2001) (imposing liability when, upon receiving knowledge of infringement, a platform "fails to purge such material from the system"); Spy Phone Labs LLC. v. Google Inc., No. 15-CV-03756-KAW, 2016 WL 6025469, at *5 (N.D. Cal. Oct. 14, 2016) (discussing removal of infringing material for contributory infringement); Arista Recs. LLC v. Lime Grp. LLC, 784 F. Supp. 2d 398, 432 (S.D.N.Y. 2011) (quoting the "fails to purge" language from *Napster*). *But see* Greer v. Moon, 83 F.4th 1283, 1294-95 (10th Cir. 2023) ("We discern no error in the district court's explanation that contributory liability requires more than 'merely "permitting" the infringing material to remain on the website.'").

[292] *See supra* Part II.B.

infringement is known. Intent to act or not in response to knowledge of infringement is at the core of this bargain.

While notice-and-takedown could be a promising idea, takedowns are not a technologically viable option for generative AI. The developer cannot simply remove the infringing output once it has been reported since it has already been created and possibly downloaded by the user, putting it out of reach of the developer (much like the uses of the Betamax once Sony sold it to consumers). Alternatively, a service provider could engage in so-called instance unlearning, or the removal of a datapoint from consideration by the AI system in the future.[293] But instance unlearning is a nascent approach and, although it could be promising long-term, it currently incurs high computational costs and inaccuracies that make it impractical.[294]

Another possible approach could be a mechanism that filters outputs that are too similar to a particular copyrighted work or are unlikely to be fair use.[295] However, as prior scholarship has shown, mechanical determinations of fair use are far from perfect and can block free speech.[296] It is quite difficult to devise filters that are robust enough to capture more than mere surface-level matches but not so broad as to be proscriptively overinclusive of fair uses or other noninfringing outputs.[297] Indeed, in devising the DMCA system, Congress expressly did not require service providers to engage in proactive activities such as filtering.[298]

An alternative that builds upon notice-and-takedown while considering intent would potentially provide a more promising vehicle

---

[293] *See* Henderson et al., *supra* note 266, at 19 (explaining instance unlearning).

[294] *See id.*; *see also* Lee et al., *supra* note 266, at 98 ("But the technology to make a generative model avoid generating specific concepts is an active area of research, and modifying a model to remove a concept can compromise its performance in other ways.").

[295] *See* Henderson et al., *supra* note 266, at 17 (explaining the viability of filters in AI systems).

[296] *See* Ard, *supra* note 10, at 34; Dan L. Burk, *Algorithmic Fair Use*, 86 U. CHI. L. REV. 283, 285 (2019) (concluding that algorithmic determination of fair use embeds biases and will not be completely accurate).

[297] *See* Henderson et al., *supra* note 266, at 21-22 (describing the technical limitations of filtering).

[298] *See* 17 U.S.C. § 512(m).

for maintaining copyright's balance between incentives and access. Eugene Volokh proposed a similar notice-and-blocking structure for AI-generated defamation.[299] Peter Henderson, Tatsunori Hashimoto, and Mark Lemley also noted the potential parallel with the DMCA's actual or red flag knowledge requirements for defamation liability for AI-generated libel against public figures and the potential viability of a regime like notice-and-takedown in that context.[300]

An adaptation of notice-and-takedown is viable in the copyright context in part because courts have adopted a variety of tests for the material contribution requirement. The Ninth Circuit has referred to material contribution as either providing the "site and facilities" for the infringement or failing to take "simple measures" to prevent the infringement.[301] Courts in the Southern District of New York have instead referred to material contribution as "author[ing], or play[ing] [a] part" or involving "substantial participation" in the infringement.[302] Other courts in the Southern District have also endorsed the Ninth Circuit's "site and facilities" test.[303] Courts in both Circuits have applied a notice-and-takedown test, with emphasis on the "takedown," akin to the DMCA.[304] This allows some flexibility to build from these tests and

[299] *See* Eugene Volokh, *Large Libel Models? Liability for AI Output*, 3 J. FREE SPEECH L. 489, 514-15 (2023).

[300] *See* Peter Henderson, Tatsunori Hashimoto & Mark Lemley, *Where's the Liability in Harmful AI Speech?*, 3 J. FREE SPEECH L. 589, 641-42, 649 (2023).

[301] *See* Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 671 (9th Cir. 2017) (finding that failing to implement a "simple measure" to prevent infringement would qualify as a material contribution, but that there were no simple measures that Giganews could have taken to remove infringing works from its servers under the circumstances); A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001) (finding that Napster had materially contributed to the infringing activity by providing the site and facilities for the direct infringement).

[302] *See, e.g.*, Lopez v. Bonanza.com, Inc., No. 17 Civ. 8493 (LAP), 2019 WL 5199431, at *24 (S.D.N.Y. Sept. 30, 2019) (quoting Warren v. John Wiley & Sons, Inc., 952 F. Supp. 2d 610, 619 (S.D.N.Y. 2013); Wolk v. Kodak Imaging Network, Inc., 840 F. Supp. 2d 724, 750 (S.D.N.Y. 2012)).

[303] Capitol Recs., LLC v. ReDigi Inc., 934 F. Supp. 2d 640, 658 (S.D.N.Y. 2013); Arista Recs. LLC v. Usenet.com, Inc., 633 F. Supp. 2d 124, 155 (S.D.N.Y. 2009) (quoting Fonovisa v. Cherry Auction, Inc., 76 F.3d 259, 264 (9th Cir. 1996)).

[304] *See supra* note 291.

create a sui generis refinement rather than merely adopting one of the existing options.

This sui generis refinement could be a "notice-and-revision" structure. Instead of requiring takedowns, this approach would require expeditious *revision* of the AI system to address the learned-of infringement. While the revision will not necessarily prevent all future infringement, even of the same copyrighted work, it puts the onus on the developer to improve the AI system to limit infringements once it is aware of its specific infringement capabilities. As Volokh noted in the defamation liability context, once the company is on notice, "[p]resumably the company could then add [post-processing content filtering] code that would prevent these particular allegations [or, in this case, infringements] . . . from being output."[305] The provider could also revise the underlying model to prevent the infringement from reoccurring. This approach may not be perfect, but it offers a reasonably protective solution.[306] Thus, notice-and-revision offers a balanced approach that places certain reasonable obligations on the developer only once they are aware of the problem — holding the developer liable where they have intentionally acted or not acted in response to knowledge of specific infringements.

Beyond considering intent, notice-and-revision also provides three benefits that help maintain the incentives-access balance. First, it provides a more balanced approach than direct or vicarious liability, which would impose categorical ex ante restrictions on AI systems that strongly favor rights over access. Second, it accommodates the unpredictability of AI-generated outputs — which, as one of the core features of increasingly autonomous AI, we must accept if we wish to maximize the technology's capabilities. Third, by imposing shared obligations on rights owners and AI system providers (similarly to the DMCA), it does not unduly favor incentives or access over the other. Therefore, notice-and-revision could be a viable refinement to secondary liability to facilitate the emerging information architecture of generative AI and maintain the incentives-access balance.

[305] Volokh, *supra* note 299, at 514-15.

[306] *See id.* at 518.

B. Web3

1. Blockchain Technology

Another emerging information architecture that could raise architectural infringement claims is blockchain and, more broadly, Web3 technologies that rely on blockchain. A blockchain is an immutable digital ledger operating on a decentralized network consisting of a number of computers called "nodes," not unlike decentralized peer-to-peer systems like Napster and Grokster.[307] As a ledger, the purpose of the blockchain is to record transactions and track assets.[308] These transactions are communicated by a sequence of blocks forming a chain (hence "blockchain").[309] Each block represents a unique transaction.[310] When a transaction is requested, a new block is created.[311] That block is sent to every node in the network to validate the transaction — confirming the owner is not trying to sell the same digital asset twice.[312] The block is then added to the existing blockchain and the transaction is complete.[313]

Blockchain is also immutable; it cannot be changed.[314] Once the transaction is recorded, it is imprinted on the blockchain ledger

---

[307] *See* Georgios Dimitropoulos, *The Law of Blockchain*, 95 WASH. L. REV. 1117, 1127 (2020).

[308] *What Is Blockchain?*, IBM, https://www.ibm.com/topics/what-is-blockchain (last visited Jan. 21, 2025) [https://perma.cc/3RMM-S7RH] (noting that blockchain "facilitates the process of recording transactions and tracking assets in a business network"); *see* Samuel N. Weinstein, *Blockchain Neutrality*, 55 GA. L. REV. 499, 501 (2021).

[309] *See* Dimitropoulos, *supra* note 307, at 1129.

[310] *See id.* (explaining that "[a]fter a successful transfer . . . a new block is created as part of the ledger").

[311] *See What Is Blockchain Technology?*, *supra* note 308.

[312] *See How Blockchain Architecture Works? Basic Understanding of Blockchain and Its Architecture*, ZIGNUTS TECHNOLAB (May 23, 2018), https://www.zignuts.com/blogs/how-blockchain-architecture-works-basic-understanding-of-blockchain-and-its-architecture [https://perma.cc/4F5S-ATGQ].

[313] *Id.*

[314] *See* DELOITTE LEGAL, BLOCKCHAIN: LEGAL IMPLICATIONS, QUESTIONS, OPPORTUNITIES AND RISKS 3 (2022) ("Once stored on the blockchain, participants are incentivized to not manipulate or change the data . . . ."); Usha R. Rodrigues, *Law and the Blockchain*, 104 IOWA L. REV. 679, 682 (2019) ("Because of the decentralized,

forever.[315] This does not necessarily mean that the information in the blockchain is infallible, as incorrect information could have been added.[316] But it is permanent.[317]

One of the most prominent uses of blockchain (and a useful example for architectural infringement claims) is for non-fungible tokens ("NFTs").[318] While some commentators and the public have — mostly incorrectly — referred to NFTs as digital art,[319] they are actually just tokens stored on a blockchain.[320] NFTs themselves are unique, non-interchangeable units of data that are created, or "minted," on a blockchain and that can represent possession or other rights in associated assets, be they art, music, electronic files, or anything else.[321] This uniqueness of the NFT (although not necessarily the underlying

distributed nature of the blockchain ledger, changes in the code will be rejected unless the code itself contemplates subsequent modifications.").

[315] *See* Michele Benedetto Neitz, *How to Regulate Blockchain's Real-Life Applications: Lessons from the California Blockchain Working Group*, 61 JURIMETRICS 185, 186 (2021) ("A blockchain ledger is practically immutable, meaning that once a transaction is written into the blockchain, it is computationally impractical to reverse that record."); *see also How Blockchain Architecture Works*, *supra* note 312.

[316] *See* DELOITTE LEGAL, *supra* note 314, at 3 ("The garbage-in, garbage-out principle is as applicable here as with any other process, the difference being that we cannot go back and correct the mistake.").

[317] *See id.*

[318] *See* James Grimmelmann & A. Jason Windawi, *Blockchains as Infrastructure and Semicommons*, 64 WM. & MARY L. REV. 1097, 1109-10 (2023).

[319] *See, e.g.*, Franky Aguilar, *NFTs Aren't Just Assets. They're Art.*, BUILT IN (Sept. 7, 2022), https://builtin.com/blockchain/nfts-are-art [https://perma.cc/T9Y3-SE46] (describing NFTs as a "digital art form"); Elena Fitzsimons, *NFT Art: What Is It, How It Works and What It Means for the Creative Industry*, 99DESIGNS, https://99designs.com/blog/web-digital/nft-art (last visited Jan. 21, 2025) [https://perma.cc/5W6E-K37U] ("An NFT can be any type of digital file: an artwork, an article, music or even a meme . . . .").

[320] *See* Edward Lee, *NFTs as Decentralized Intellectual Property*, 2023 U. ILL. L. REV. 1049, 1054-55 (noting that "the sale [of an NFT] involves a purchase of the *virtual token*, a new type of property, stored on blockchain, *plus* a content license, granted by the creator, that allows the NFT owner to make certain uses of the associated copyrighted work, such as commercial uses and the making of derivative works"); Robyn Conti & Michael Adams, *What Is an NFT? Non-Fungible Tokens Explained*, FORBES https://www.forbes.com/advisor/investing/cryptocurrency/nft-non-fungible-token (last updated Mar. 10, 2024, 3:41 PM) [https://perma.cc/3UXY-4EUS] ("NFTs are typically held on the Ethereum blockchain, although other blockchains support them as well.").

[321] *See* KRISTEN E. BUSCH, CONG. RSCH. SERV., NON-FUNGIBLE TOKENS (NFTS) 1 (2022).

asset) is what makes it non-fungible.[322] An NFT is more akin to an original piece of art or a signed baseball — objects for which there is no true replacement — than U.S. dollars or apples, for which any dollar or apple would do.[323] This is unlike cryptocurrency, which is fungible because each individual bitcoin, for example, has the same value as all others.[324]

There are two types of NFTs: "off-chain" and "on-chain." An off-chain NFT is somewhat like a receipt. The underlying content in an off-chain NFT is stored outside of the blockchain.[325] An NFT could even link to someone else's online content.[326] Comparatively, an on-chain NFT is where the underlying asset is uploaded directly onto the blockchain.[327] This is more akin to possessing the work than the receipt.[328] Until recently, these on-chain NFTs were fairly rare, as it was prohibitively expensive to write such large amounts of data onto the blockchain.[329]

---

[322] *See* Juliet M. Moringiello & Christopher K. Odinet, *The Property Law of Tokens*, 74 FLA. L. REV. 607, 609 (2022) (describing NFTs as "just the latest in the tokenization craze — the idea of creating a unique digital representation (a token) of a particular asset").

[323] *See* Joshua A.T. Fairfield, *Tokenized: The Law of Non-Fungible Tokens and Unique Digital Property*, 97 IND. L.J. 1261, 1266 (2022) (describing how NFTs are "unique digital assets that can be bought and sold like real-world objects").

[324] *See id.* at 1265 (noting that "there is nothing to emotionally attach to in a bitcoin, no difference in characteristics and meaning").

[325] *On-Chain NFTs and Why They're Better*, GNARS (Jan. 11, 2022), https://art.haus/on-chain-nfts-and-why-theyre-better/#:~:text=While%20on%2Dchain%20NFTs%20have, smart%20contract%20will%20be%20useless [https://perma.cc/7WPV-5PY8].

[326] *See* Andres Guadamuz, *Perspectives on NFTs from the EU and UK*, 45 COLUM. J.L. & ARTS 361, 363 (2022).

[327] *See* Pınar Çağlayan Aksoy & Zehra Özkan Üner, *NFTs and Copyright: Challenges and Opportunities*, 16 J. INTELL. PROP. L. & PRAC. 1115, 1120 (2021) ("The underlying content and the metadata are uploaded directly into the blockchain in on-chain NFTs.").

[328] *See id.*

[329] *See* Andres Guadamuz, *The Treachery of Images: Non-Fungible Tokens and Copyright*, 16 J. INTELL. PROP. L. & PRAC. 1367, 1371-72 (2021) (explaining the high cost of uploading kilobytes onto the Ethereum blockchain and why this means, in practice, that NFTs are typically small metadata files); Andres Guadamuz, *Non-Fungible Tokens (NFTs) and Copyright*, WIPO MAG. (Dec. 10, 2021), https://www.wipo.int/wipo_magazine/en/2021/04/article_0007.html [https://perma.cc/9EQ5-DH6H] ("There are various types of NFTs, but the most common is a metadata file containing information encoded with a digital version of the work that is being tokenized. The other type is where the entire

However, there is growing interest in increasing the use of on-chain NFTs as this obviates the risk of link rot (hyperlinks breaking) and content drift (the off-chain content being removed or modified).[330] In January 2023, for example, Bitcoin introduced on-chain NFTs called Ordinals that can hold up to 4MB of data.[331] Major NFT projects, such as CryptoPunks, are now on-chain too.[332]

As shown in Figure 2, there are three NFT permutations relevant for copyright infringement: off-chain direct links, off-chain copies, and on-chain. To demonstrate, take Chris Torres' Pumpkin Spice Nyan Cat NFT — a festive Halloween-themed version of the famous Internet meme Nyan Cat, a flying Pop-Tart shaped cat emitting a rainbow trail in its wake. As of March 2025, the Pumpkin Spice Nyan Cat NFT is available on NFT marketplace OpenSea.[333] If I wanted to create my own Pumpkin Spice Nyan Cat NFT, I could either directly link to Torres' original image of the cat, or I could make another copy of the cat and link to it. In the first case (direct link), I would not create a copy, so the potential copyright infringement claim is negligible.[334] But in the second

work is uploaded to the blockchain; these are less common as it is expensive to upload information to the blockchain.").Megan E. Noh, Sarah C. Odenkirk & Yayoi Shionoiri, *GM! Time to Wake Up and Address Copyright and Other Legal Issues Impacting Visual Art NFTs*, 45 COLUM. J.L. & ARTS 315, 317 (2022) (noting that an NFT typically "does *not* contain the media file for the associated asset").

330 *See On-Chain NFTs and Why They're Better*, *supra* note 325 (describing projects attempting to utilize on-chain NFTs and the benefits of on-chain NFTs over off-chain ones); *see also* Jonathan Zittrain, *The Internet Is Rotting*, ATLANTIC (June 30, 2021), https://www.theatlantic.com/technology/archive/2021/06/the-internet-is-a-collective-hallucination/619320 [https://perma.cc/PL7M-79TK] (describing the issues of link rot and content drift on the Internet).

331 Murtuza Merchant, *Bitcoin's On-Chain NFTs Spark Controversy, Censorship Calls Among Developers*, BENZINGA (Jan. 30, 2023, 12:55 PM), https://www.benzinga.com/markets/cryptocurrency/23/01/30623341/bitcoins-on-chain-nfts-spark-controversy-censorship-calls-among-developers [https://perma.cc/46L2-JN22].

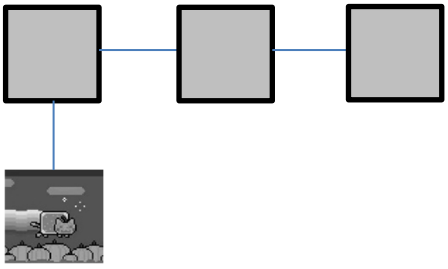
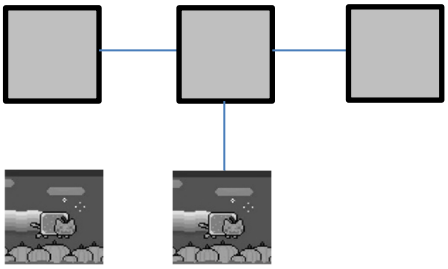
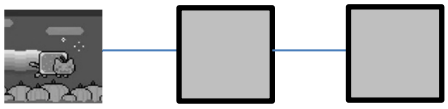
332 *On-Chain Cryptopunks*, LARVA LABS, https://www.larvalabs.com/blog/2021-8-18-18-0/on-chain-cryptopunks (last visited Jan. 21, 2025) [https://perma.cc/84R9-GK2R].

333 *Pumpkin Spice Nyan Cat*, OPENSEA, https://opensea.io/assets/ethereum/0xb32979486938aa9694bfc898f35dbed459f44424/10056 (last visited Mar. 20, 2025).

334 *See* Emily Behzadi, *The Fiction of NFTs and Copyright Infringement*, U. PA. L. REV. ONLINE (Apr. 12, 2022), https://www.pennlawreview.com/2022/04/12/the-fiction-of-nfts-and-copyright-infringement [https://perma.cc/X8H2-6HAG]. There is an argument that the display right could be infringed. *See* Guadamuz, *supra* note 329, at 1377-83

case (copy), I would be creating a new, infringing copy and linking to it, which could form the basis for a copyright infringement claim. Third, I could upload an (infringing) copy of Pumpkin Spice Nyan Cat to make an on-chain NFT, which would be direct copying.[335]

FIGURE 2

NFT Permutations for Copyright Infringement	
1. Off-Chain Direct Links	 Original
2. Off-Chain Copies	 Original Copy
3. On-Chain	

(concluding that unauthorized minting of an NFT does not necessarily copy a copyrighted work, but it may impermissibly share it). However, this argument is likely inapplicable in districts that apply the server test, which holds that a person only displays a work when he or she hosts and serves it, not embeds it. *See generally* Michael P. Goodyear, *The Server Test Quandary and Embedding Permission Culture*, 75 OKLA. L. REV. 263, 268-283 (2023) (discussing the server test and which courts have endorsed or rejected it).

[335] *See* Guadamuz, *supra* note 329, at 1378.

Blockchain and NFTs have fallen considerably from their height of over $17.6 billion in NFT sales in 2021.[336] Nonetheless, blockchain and NFTs have potential future value. Despite environmental concerns about the significant amount of energy they (and AI) consume,[337] blockchain and NFTs are expected to be important building blocks for future advances in information technology and the Internet. [338]

Until now, the literature has almost completely ignored Web3 secondary liability risks for nodes and platforms with blockchain and NFTs, let alone connected them to the broader concerns of architectural infringement claims. The vast majority of NFT- and blockchain-related legal scholarship has focused on securities, regulatory law, or general legal surveys.[339] The intellectual property literature has focused on the relationship between copyright and NFTs, but rarely infringement.[340]

[336] Steve Kaaru, *NFT Volume Hits 6-Month High, But Still 90% Down from 2021*, COINGEEK (Dec. 9, 2024), https://coingeek.com/nft-volume-hits-6-month-high-but-still-90-down-from-2021 [https://perma.cc/F525-4PH6].

[337] *The Latest Hype in NFTs is a Climate Disaster: On-Chain Bitcoin NFTs*, DIGICONOMIST (Feb. 2, 2023), https://digiconomist.net/the-latest-hype-in-nfts-is-a-climate-disaster-on-chain-bitcoin-nfts [https://perma.cc/S8PV-YE79].

[338] *See* Jacquelyn Melinek, *Bitcoin NFTs Are Growing Quickly as Community Sees Long-Term Potential*, TECHCRUNCH (Feb. 14, 2023, 1:30 PM), https://techcrunch.com/2023/02/14/bitcoin-nfts-are-growing-quickly-as-community-sees-long-term-potential [https://perma.cc/X3FW-BL49] (quoting industry figures such as Nick Hansen, CEO and co-founder of Luxor, who described Bitcoin NFTs as an "impactful revelation" and that "we're definitely headed to more Bitcoin NFT inscriptions now than fewer").

[339] *See, e.g.*, Jon M. Garon, *Legal Implications of a Ubiquitous Metaverse and a Web3 Future*, 106 MARQ. L. REV. 164, 185-206 (2022) (reviewing the Web3 regulatory environment); Kimberly A. Houser & John T. Holden, *Navigating the Non-Fungible Token*, 2022 UTAH L. REV. 891 (2022) (analyzing NFTs under gambling, copyright, securities, finance, tax, and property law); Steven L. Schwarcz, *Next-Generation Securitization: NFTs, Tokenization, and the Monetization of 'Things,'* 103 B.U. L. REV. 967, 984-98 (2023) (describing non-cash-flow monetization transactions such as NFTs and positing how they should be regulated).

[340] *See, e.g.*, Adler, *supra* note 23, at 760 (examining the norm of artificial authenticity in the art market and NFTs); Aksoy & Üner, *supra* note 327, at 1124-25 (examining which rights are granted to an NFT buyer); Brian L. Frye, *Are CryptoPunks Copyrightable?*, 2021 PEPP. L. REV. 1 (2022) (explaining why the CryptoPunk NFT content may not be copyrightable); Brian L. Frye, *After Copyright: Pwning NFTs in a Clout Economy*, 45 COLUM. J.L. & ARTS 341, 342 (2022) (describing how NFTs, unlike copyright, may promote public access to goods); Houser & Holden, *supra* note 339, at 910-12 (discussing what rights a purchaser of an NFT gains and the inapplicability of the first sale doctrine); Lee, *supra*

Commentators such as Emily Behzadi and Megan Noh have highlighted the risk of direct infringement by NFT users but have not addressed the consequential architectural infringement concerns of secondary liability.[341] While Behzadi explains that the mere creation of an (off-chain) NFT by itself is not an infringing act, Andres Guadamuz correctly notes that the underlying content in an NFT itself may be (directly) infringing.[342] This analysis also excludes on-chain NFTs, where the content is directly uploaded to the blockchain. There is therefore a significant gap in the literature when it comes to NFT-related (and, more broadly, blockchain-based) secondary infringement liability.

2. Architectural Infringement Risks and Refinements

As with their predecessors, blockchain-based information architectures are likely to face significant architectural infringement challenges stemming from users' infringements and the architecture's novel aspect (in this case, immutability). With standard user-generated content on the Internet, a platform can easily remove infringing content once it learns of it, thus meeting its obligations under the DMCA safe harbor and avoiding contributory liability.[343] But with blockchain, the

note 320, at 1053-54 (describing NFTs as "De-IP," an alternative way for creators to directly market their works rather than rely on copyright, which is largely dominated by corporate intermediaries); Brian L. Frye, *NFTs & the Death of Art* 5 (Apr. 19, 2021) (unpublished article), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3829399 [https://perma.cc/W2KJ-2KVB] (describing how NFTs may allow artists to monetize non-copyrightable works); Michael D. Murray, *NFT Ownership and Copyrights: A Brief and Pleasant Guide to NFTs and Copyright Law, Part 1*, at 1 (July 2, 2022) (unpublished article), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4152468 [https://perma.cc/HF5B-5ZEX] (discussing the relationship between NFT ownership and copyrights, and transfers and licensing of copyrights to NFT purchasers).

[341] *See* Noh et al., *supra* note 329, at 324-25 (describing the issues with copyright owners enforcing their copyrights against alleged direct infringers, i.e., sellers of NFTs); Behzadi, *supra* note 334 (explaining why (off-chain) NFTs cannot constitute direct copyright infringement).

[342] *See* Guadamuz, *supra* note 329, at 1377-83 (concluding that unauthorized minting of an NFT does not necessarily copy a copyrighted work, but it may impermissibly share it).

[343] *See, e.g.*, 17 U.S.C. § 512(c)(1) (providing for a safe harbor against secondary copyright infringement claims for platforms that, inter alia, remove content once they learn it is infringing); Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 670 (9th Cir. 2017)

infringing content or link to the infringing content would be written into the blockchain itself and become a permanent part of content that is distributed to other servers.[344] Depending on how the content is structured, a platform may host infringing user-created content but be powerless to remove it due to blockchain's immutability. While novel risks may exist for other actors too, including NFT owners and network service providers, architectural infringement claims strike at the operation of the information architecture itself, implicating the operating (or hosting) platform.

Blockchain (and NFTs) share strong similarities with the historic information architectures discussed in Part II. They are novel systems of communicating information, sizeable populations adopted them, and they have long-term potential for future uses. NFTs — like their information architecture predecessors — already have a sizeable infringement problem.[345] In part, this is because, like with the historical information architectures, the barriers to entry for users are also remarkably low. For example, anyone can create an NFT on a third-party platform, making it easy to mint NFTs that either refer to or contain directly infringing content.[346]

Most importantly, blockchain's novel aspect of immutability poses conundrums under existing copyright law, as will be discussed in the rest of this Part. The U.S. Copyright Office and Patent and Trademark Office's 2024 report on NFTs and intellectual property recognized that immutability could cause an enforcement problem with copyright

(noting that contributory copyright infringement liability requires that a platform have "knowledge of another's infringement" and "materially contributes to . . . that infringement").

344 *See* Guadamuz, *supra* note 329, at 1375 ("This means that one can make any sort of erroneous ownership claims, and then this is written into the blockchain.").

345 *See* Jonathan Schmalfeld, *Copyright Violations Could Crash the NFT Party*, FORTUNE (Aug. 4, 2021), https://fortune.com/2021/08/04/nfts-copyright-violations-penalties-non-fungible-tokens-collectibles-nfttorney-jonathan-schmalfeld [https://perma.cc/VW2T-AV3L].

346 *See* BUSCH, *supra* note 321, at 14 ("In many NFT marketplaces, scammers can easily 'tokenize' art they did not create, as proof of legal ownership of the underlying artwork is often not required to mint a token."); Guadamuz, *supra* note 329, at 1374 ("Moreover, one could even generate a token made from works that one does not own.").

infringement, but it did not offer any solutions.[347] Taken to its furthest extent, this uncertain architectural infringement risk from NFTs could jeopardize platforms' DMCA safe harbors and potentially expose them to contributory infringement liability. This liability risk could stifle promising Web3 developments and distort the incentives-access balance in copyright law. This necessitates further refinement of copyright secondary liability. By using intent, one potential solution is to refine contributory liability's material contribution requirement to focus exclusively on the ability to take simple measures in response to specific infringements rather than rely on rigid, incompatible tests.

a. The vulnerable DMCA

For online platforms, the DMCA safe harbors serve as the first line of defense against secondary copyright infringement claims yet, due to immutability, they are likely unavailable for blockchain-based platforms. Two of these safe harbors are particularly salient for emerging information architectures like NFTs: 17 U.S.C. § 512(c) and § 512(d). Section 512(c) provides a safe harbor for user-generated content stored on one's platform.[348] As discussed above, the § 512(c) safe harbor is premised on, inter alia, a notice-and-takedown structure where a platform expeditiously removes infringing content once it is reported or the platform otherwise learns the content is infringing.[349] Section 512(d) provides a safe harbor for providing links to a webpage containing infringing content.[350] Most of the same § 512(c) requirements also apply to § 512(d).[351]

Whether NFTs are on-chain or an off-chain copy dictates the applicable safe harbor. If the underlying content is located on-chain, the platform hosting the NFT would need to avail itself of the § 512(c) safe harbor. However, if the content is an off-chain copy, either safe harbor

[347] *See* USPTO & U.S. COPYRIGHT OFF., NON-FUNGIBLE TOKENS AND INTELLECTUAL PROPERTY: A REPORT TO CONGRESS 32-33 (2024), https://www.uspto.gov/sites/default/files/documents/Joint-USPTO-USCO-Report-on-NFTs-and-Intellectual-Property.pdf [https://perma.cc/GN7H-UCRM].

[348] *See* 17 U.S.C. § 512(c).

[349] *Id.* § 512(c)(1)(C).

[350] *Id.* § 512(d).

[351] *See id.* § 512(d)(1), (3).

could apply. If the linked-to copy is located on the service provider's own service, it would need to remove that content under § 512(c). But if the content is stored on an external service, it would instead need to sever the link from the NFT to the infringing content to avail itself of the § 512(d) safe harbor.

NFTs' immutability could undermine both safe harbors. Under either safe harbor, the platform would have takedown obligations. But as NFTs and other blockchain-based tokens are immutable, this raises a significant practical concern. Infringing content or links to infringing content cannot simply be removed from the blockchain like traditional takedowns.[352] The exact risks for NFTs are dependent on whether the underlying content is (1) an off-chain copy on the same platform, (2) an off-chain copy on another platform, or (3) on-chain.

First, the easy case. If a platform were to host both the off-chain NFT and the underlying copy, it would simply have to expeditiously remove the content. The NFT would now contain a dead link, and the platform would no longer link to or host the infringing content. To meet its notice-and-takedown obligations under § 512(d), a platform need only disable access, but to meet the § 512(c) safe harbor a platform typically needs to remove the underlying content from its service.[353]

But if the underlying copy is located off-chain on another platform, the platform would not be able to disable the content, and it would also likely not be able to modify the link in the NFT due to its immutability. Yet the platform would need to disable the link to avail itself of the § 512(d) safe harbor.[354] On NFT marketplaces such as OpenSea, the platform may be able to mitigate the infringement risk by removing the listing and any linked-to depiction of the infringing content on the platform.[355] Indeed, OpenSea has a standard DMCA takedown notice

[352] *See* Houser & Holden, *supra* note 339, at 915.

[353] *See* 17 U.S.C. § 512(c)(1)(C), (d)(1)(C).

[354] *Id.* § 512(d)(3).

[355] *See* BUSCH, *supra* note 321, at 14 (noting that OpenSea delists NFTs in response to receiving takedown requests that fulfill the requirements of the DMCA); Peter Cramer & David Munkittrick, *Will NFT Piracy Compel Changes to the Digital Millennium Copyright Act?*, BLOCKCHAIN & THE L. (Mar. 16, 2022), https://www.blockchainandthelaw.com/2022/03/will-nft-piracy-compel-changes-to-the-digital-millennium-copyright-act [https://perma.cc/3C4V-NQ3J] (noting that NFT marketplaces can generally remove the listing and prevent the underlying content in an NFT from being displayed in users' virtual wallets).

portal and processes takedown notices from copyright owners.[356] However, if the platform hosts the NFT and knows that it links to infringing off-chain content, the platform may not be able to avail itself of the § 512(d) safe harbor unless that link in the NFT is somehow severed or the content is removed. Removing the link is seemingly impossible for immutable NFTs and service providers would have no control over infringing content on other platforms, as they did in the first scenario. Given this scenario, partnerships could develop where the NFT-hosting platform forwards the infringement notice to the content-hosting platform so it can remove the infringing content associated with the NFT. The content-hosting platform would have to remove the content if it wanted to maintain its § 512(c) safe harbor.[357] But such partnerships are not guaranteed.

Third, similarly, if the infringing content is located on-chain, a platform would not be able to avail itself of the § 512(c) safe harbor unless it takes down the NFT (and the infringing content embedded within).[358] Yet the NFT and its embedded content should be immutable, preventing a takedown.

NFTs' immutability thus poses a serious problem for service providers' DMCA safe harbors. At present, it is unclear how courts will apply the DMCA's requirements to NFTs. One possibility is that platforms may be required to burn infringing NFTs on their platforms. Burning is the process by which an NFT is rendered unusable in the future.[359] For example, one can burn an NFT by sending the NFT to a null address, effectively a "digital rubbish bin."[360] But burning NFTs can

[356] *See* Nilay Patel, *Can the Law Keep Up with Crypto?*, VERGE (Feb. 22, 2022, 7:54 AM), https://www.theverge.com/22944579/crypto-bitcoin-internet-law-nft-tiktok-dances-tonya-evans-interview (quoting Tonya Evans that OpenSea has a DMCA portal "the same as any other social platform").

[357] 17 U.S.C. § 512(c)(1)(A).

[358] *See id.* § 512(c)(3) (requiring that upon gaining knowledge or red flag knowledge of infringing user-generated content, the service provider expeditiously remove or disable it).

[359] *See* Alex Gomez, *Burn an NFT: What it Means, How to Burn, and Why it Matters*, CYBER SCRILLA (Apr. 19, 2023), https://cyberscrilla.com/burning-your-nft-how-to-cost-and-purpose [https://perma.cc/B233-ZEXG].

[360] *See* Maghan McDowell, *Why Brands Are Burning NFTs*, VOGUE BUS. (Feb. 8, 2022), https://www.voguebusiness.com/technology/why-brands-are-burning-nfts [https://perma.

be quite expensive compared to merely removing content from an interactive webpage like Amazon or TikTok. The blockchain requires gas fees to burn an NFT, which some estimate to cost up to $100 per NFT, or even higher if there is a surge in gas fees.[361] In addition, platforms may not have the ability to burn infringing NFTs; those rights may be limited to the NFT owner or the original creator under its smart contract.[362] So while it is possible that platforms may be obligated to burn NFTs once they know they are infringing, questions remain, especially where the platforms lack that ability.

Losing the DMCA safe harbor does not automatically make a platform secondarily liable for copyright infringement.[363] However, a platform's obligations under the DMCA have parallels in contributory and vicarious copyright infringement that may make them liable nonetheless.[364] Therefore, if a platform loses its safe harbor vis-à-vis

cc/J2M9-WABX] (describing the various meanings of the term "burn" and how to burn an NFT); CCI, *What Is NFT Burning?*, CRYPTO COUNCIL FOR INNOVATION (Jan. 19, 2024), https://cryptoforinnovation.org/what-is-nft-burning [https://perma.cc/7WKL-4KJY] (explaining that burning "is achieved by sending the NFT to a burn address, which correlates to a crypto wallet that cannot be controlled or accessed by anyone, meaning the NFT can never again be transferred, bought, or sold and therefore can never again be owned by an individual").

[361] *See* LEE, *supra* note 23, at 177 (explaining that a surge caused gas fees at one time to be between $6,500 and $14,000); Gomez, *supra* note 359.

[362] *See How Does OpenSea Handle NFTs with a Burn Mechanism*, OPENSEA, https://support.opensea.io/en/articles/8867074-how-does-opensea-handle-nfts-with-a-burn-mechanism (last visited Jan. 21, 2025) [https://perma.cc/4UDV-EGSV] ("A smart contract with a burn mechanism might be authorized to burn your NFT, or even authorize others to burn your NFT."); McDowell, *supra* note 360 (explaining that the owner is generally the party that can burn the NFT, although the original creator may have reserved rights to the NFT such that it can effectively burn it by revoking the rights to the NFT).

[363] *See* 17 U.S.C. § 512(l) ("The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense."); Finley v. YouTube, LLC, No. 20-cv-04888-RS, 2022 WL 704835, at *1 (N.D. Cal. Mar. 9, 2022) ("[T]he DMCA provides a series of statutory safe harbors, not a cause of action.").

[364] Although there are slight differences, the notice-and-takedown obligation aligns with contributory liability, and the right and ability to control and a direct financial benefit align with vicarious liability. *Compare* 17 U.S.C. § 512(c)(1)(A) (stating that in order to avail itself of the safe harbor, a service provider must "not have actual

NFTs, it could potentially be held contributorily or vicariously liable for that infringement because it hosts or links to the underlying content.[365] Those two claims are examined below.

knowledge that the material or an activity using the material on the system or network is infringing [and] upon obtaining such knowledge or awareness, act[] expeditiously to remove, or disable access to, the material"), *with* A&M Recs., Inc. v. Napster, Inc., 239 F.3d 1004, 1019 (9th Cir. 2001) (noting that contributory liability applies when one "with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another"); *compare* 17 U.S.C. § 512(c)(1)(B) (stating that in order to avail itself of the safe harbor, a service provider must not "receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity"), *with* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1173 (9th Cir. 2007) (noting that vicarious liability lies where a defendant "exercises the requisite control over the direct infringer and . . . derives a direct financial benefit from the direct infringement.").

[365] There is some debate about whether providing hyperlinks to infringing content can be the basis for a contributory infringement claim. Some early Internet cases suggested hyperlinking should lead to contributory liability when they enjoined third parties from providing links to infringing content or circumvention software. *See, e.g.*, Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 346 (S.D.N.Y. 2000) (enjoining Defendants from linking to other websites that make circumvention software available under the DMCA); Intell. Rrsv., Inc. v. Utah Lighthouse Ministry, Inc., 75 F. Supp. 2d 1290, 1295 (D. Utah 1999) (enjoining Defendants from posting addresses of websites that Defendants knew or had reason to know contained allegedly infringing content). The Ninth Circuit seemed to agree with these earlier cases in *Perfect 10, Inc. v. Amazon.com, Inc.*, where it held that "facilitat[ing] access to websites throughout the world can significantly magnify the effects of otherwise immaterial infringing activities" and remanded on whether Google had knowledge of the infringement for purposes of contributory liability. 508 F.3d at 1172-73. But in *Flava Works, Inc. v. Gunter*, the Seventh Circuit, albeit in dicta, noted that holding parties contributorily liable for the mere provision of a link to infringing content — without inducement — would be implausible, although it reserved the possibility that the plaintiff could show that the defendant's service "really does contribute significantly to infringement." *See* 689 F.3d 754, 758-59, 763 (7th Cir. 2012). Some scholars have written that hyperlinks can clearly fit within the existing secondary liability framework (even if the desirability of this outcome is debatable). *See, e.g.*, Dogan, *Infringement Once Removed*, *supra* note 16, at 884 ("Clearly, links to infringement can fit into existing standards for indirect liability under United States law."); Jane C. Ginsburg & Luke Ali Budiardjo, *Liability for Providing Hyperlinks to Copyright-Infringing Content: International and Comparative Law Perspectives*, 41 COLUM. J.L. & ARTS 153, 195-96 (2018) (explaining that providing a link to an infringing work may constitute contributory copyright infringement or inducement).

b. Vicarious liability mismatch

Like with generative AI, it is unclear whether vicarious liability could apply to blockchain. A platform is vicariously liable for copyright infringement where it has both the right and ability to supervise or control the infringing content and receives a direct financial benefit from the infringing content.[366] For purposes of vicarious copyright infringement liability, courts have adopted a lower threshold for the right and ability to control than in other contexts, including the DMCA: the ability to delete or remove content — or even the responsible user's account (as harsh and potentially undesirable as that is) — is enough.[367] Courts have been reluctant to impose vicarious liability where a platform's control over the infringing content is lower.[368]

Based on this standard, blockchain's immutability should reduce the risk of vicarious liability because it undermines a platform having the right and ability to control. For example, if a platform could delete the underlying content of an NFT (e.g., an off-chain NFT with the content located on the platform's servers), it would undoubtedly have the right

[366] Luvdarts, LLC v. AT & T Mobility, LLC, 710 F.3d 1068, 1071 (9th Cir. 2013) (quoting *Napster*, 239 F.3d at 1022-23).

[367] *See, e.g.*, Bus. Casual Holdings, LLC v. YouTube, LLC, No. 22-3007-cv, 2023 WL 6842449, at *3 (2d Cir. Oct. 17, 2023) (per curiam) ("YouTube did not decline to exercise its right to stop TV-Novosti's alleged infringement, and instead removed the three videos shortly after learning about their alleged infringement."); *Napster*, 239 F.3d at 1022 (finding that a service provider had the right and ability to supervise the infringing activity where it could terminate users' access to the system); Sony Music Ent. v. Cox Commc'ns, Inc., 464 F. Supp. 3d 795, 813-14 (E.D. Va. 2020), *overturned on other grounds by* 93 F. 4th 222 (4th Cir. 2024) (Cox had the right and ability to control because it had the "actual ability to stop or limit ongoing infringement by modifying or terminating an account"); Agence France Presse v. Morel, 934 F. Supp. 2d 547, 575 (S.D.N.Y. 2013) (holding that Getty Images could have the right and ability to control because it could remove allegedly infringing photos and block subscribers).

[368] *See, e.g.*, Routt v. Amazon.com, Inc., 584 F. App'x 713, 714-15 (9th Cir. 2014) (Amazon could only monitor the websites of participants in its affiliate-marketing program, not terminate the websites); *Luvdarts*, 710 F.3d at 1072 (holding that AT&T was not vicariously liable because it could not supervise its networks for infringing activity at that time).

and ability to control as it could disable the infringing content.[369] However, the right and ability to control is much less likely in the case of on-chain NFTs and off-chain NFTs whose underlying content is stored off the platform's servers and cannot be easily removed. Even if the platform could remove the infringing account, the infringing content would likely remain on its platform, undermining the benefit to the rights owner of deleting the account. Therefore, immutability could provide a potential defense for platforms against claims of vicarious liability, although the ability to delete a user's account could be sufficient for control.

The other prong of the vicarious liability test, a direct financial benefit, would appear to be readily met in the NFT context as NFTs are bought and sold. One of the primary uses of NFTs has been to generate considerable profits for sellers and marketplace intermediaries such as OpenSea.[370] But hosting providers may also monetize NFTs or NFT-related services.[371] This may take the form of charging a transaction fee for hosting the NFT on a platform or taking a cut from subscriptions for accessing the NFT.[372] Post-DMCA courts have held that financial benefits flowing from specific infringing content are sufficient.[373] It is also enough

[369] *See Napster*, 239 F.3d at 1023 (the right and ability to supervise the infringing activity exists where a service provider can terminate the infringing content or users' access to the system).

[370] *See* Ryan Browne, *Trading in NFTs Spiked 21,000% to More than $17 Billion in 2021, Report Says*, CNBC (Mar. 10, 2022, 1:00 AM), https://www.cnbc.com/2022/03/10/trading-in-nfts-spiked-21000percent-to-top-17-billion-in-2021-report.html [https://perma.cc/ZEH7-B4RQ] (describing the profits stemming from NFTs); Natasha Dailey, *NFT Exchange OpenSea Made Just $28,000 a Month When it Launched 4 Years Ago. Now Its Founders Are About to Be Crypto Billionaires.*, BUS. INSIDER (Nov. 28, 2021, 3:41 AM), https://markets.businessinsider.com/news/currencies/nft-exchange-opensea-founders-billionaires-sales-transaction-surge-2021-11 [https://perma.cc/Y3KR-JSLY] (describing how OpenSea has profited from NFT sales).

[371] *See* Oppenheimer v. Allvoices, Inc., No. C 14-00499 LB, 2014 WL 2604033, at *8 (N.D. Cal. June 10, 2014) (holding that a direct financial benefit exists where there is a causal relationship between the infringing content and a financial benefit to the service provider, regardless of the substantiality of the benefit).

[372] *See* Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 674 (9th Cir. 2017) (holding that "Perfect 10 was required to provide evidence that customers were drawn to Giganews's services because of the infringing Perfect 10 material at issue").

[373] *See, e.g.*, Ventura Content, Ltd. v. Motherless, Inc., 885 F.3d 597, 613 (9th Cir. 2018) ("The words 'the' and 'directly' in the statute, though, must mean that some revenue has

if the specific infringing NFT was a draw to the platform.[374] But if the platform is agnostic as to the presence of the infringing NFT (i.e., it does not charge for that NFT) and consumers are not attracted by the infringing NFT, the platform may have a sound basis to push back against the vicarious infringement claim on the direct financial prong too.

Regardless, the right and ability to control prong would likely bar successful vicarious infringement claims. Therefore, a refinement to secondary liability is seemingly not needed for vicarious liability to maintain the current balance between copyright owners' incentives and access, or to avoid stymying Web3 technologies.

c. Contributory liability refinements

Unlike vicarious liability, contributory liability poses a significant architectural infringement claim risk that could upset copyright's incentives-access balance. A platform is liable for contributory copyright infringement when it "(1) has knowledge of another's infringement and (2) . . . materially contributes to . . . that infringement."[375] This largely parallels the notice-and-takedown requirement under the DMCA. But an intent-consistent refinement to the material contribution requirement, such as exclusively adopting the nuanced simple measures test, could nullify this risk by accommodating immutability.

As a threshold matter, like with the intent-guided refinement for generative AI, Web3-based refinements can maintain the inducement doctrine from *Grokster* to capture actors whose clear intent is to

to be distinctly attributable to the infringing material at issue. There is no evidence that Motherless made any money directly from the [plaintiff] Ventura clips."); Downs v. Oath, 385 F. Supp. 3d 298, 307 (S.D.N.Y. 2019) ("[I]t is not enough for [plaintiff] Downs to show that [defendant] HuffPost ran commercial advertisements on its website. . . . Instead, Downs must put forth evidence of a connection between the allegedly infringing activity and the financial benefit that HuffPost received.").

[374] *See Giganews*, 847 F.3d at 674 (holding that the infringing content had to draw customers to Giganews' services); Ellison v. Robertson, 357 F.3d 1072, 1078-79 (9th Cir. 2004) (holding that a financial benefit exists where the availability of infringing materials "acts as a draw" for users, not just an "added benefit" (quoting A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1023 (9th Cir. 2001))).

[375] *Giganews*, 847 F.3d at 670 (quoting Perfect 10, Inc. v. Visa Int'l Serv., Ass'n, 494 F.3d 788, 795 (9th Cir. 2007)).

encourage infringement. *Grokster* makes platforms that encourage infringing content liable for inducement, notwithstanding the *Sony* safe harbor.[376] For example, encouraging users to mint NFTs with infringing content (e.g., encouraging users to upload Banksy and Pokémon NFTs) would likely fall afoul of the inducement doctrine. But merely offering Web3 technologies, which can have significant non-infringing uses, would not result in contributory liability based on mere constructive knowledge of infringement under *Sony*.

But *Sony* and *Grokster* only provide a threshold inquiry — the platform could still have *specific* knowledge of infringements, potentially resulting in contributory liability if it materially contributes to the infringement.[377] Like with generative AI, the material contribution requirement is the problem for blockchain and NFTs. The requirement therefore needs to be refined to not unduly stymie innovation in Web3 technologies and maintain copyright's incentives-access balance.

The plethora of material contribution tests described previously (including notice-and-takedown, site and facilities, and simple measures) could pose a significant deterrent to would-be Web3 entrants.[378] If some tests apply, platforms would be de facto liable due to blockchain's immutability, while others allow a more nuanced examination that could accommodate Web3 technologies. This uncertainty — and potential architectural infringement — could restrain all but the largest technology companies from entering the space and reduce the number of platforms contributing to future innovations. If the wrong test is selected, it could undesirably chill innovation or impinge upon rights owners' copyrights. As with prior architectural infringement claims, courts or Congress should refine the secondary liability framework to accommodate for these new information architectures. Intent provides a more predictable path for refining the material contribution test that maintains balance between the dual goals of incentives and access. In this case, the architectural infringement challenge raised by Web3 does not necessarily require a sui generis refinement like the DMCA or notice-and-revision. Instead,

[376] *See* Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd., 545 U.S. 913, 936-37 (2005).

[377] *See* Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1172 (9th Cir. 2007).

[378] *See supra* notes 301–304 and accompanying text.

the refinement could be selecting the existing material contribution test that is most consistent with intent and technological change.

If we consider intent, one possible result is that static material contribution tests such as notice-and-takedown and "site and facilities" are poor matches for new information architectures because they cannot adjust to changes in technological capabilities. As explained above with the DMCA safe harbors, for immutable content — such as on-chain NFTs and off-chain NFTs whose underlying content is stored elsewhere — it may not be possible for platforms to remove the content, which would seem to make them de facto liable under the notice-and-takedown test. They would presumably be held liable under the "site and facilities" test too because they are providing the information architecture, even if they are powerless to prevent the use after it has occurred due to blockchain's immutability.[379] These outcomes would skew the balance of copyright by creating de facto infringement based solely on the technology.

Even more flexible tests could pose problems. The "substantial participation" test could cause liability risks because it is unclear what the test requires. It is possible that substantial participation could align with intent if it seeks to hold only the most culpable liable. One court, for example, interpreted the substantial participation test as a high bar requiring that "the contributory infringer must have acted in concert with the direct infringer."[380] But courts could also interpret it to mean that merely providing the platform is enough. Another court suggested that merely "play[ing] any part at all" was sufficient.[381] It could also be coterminous with the site and facilities test.[382]

The most fluid test, the "simple measures" test, is a promising alternative under intent. This is a flexible standard that looks to awareness of one's role in the infringement rather than the more static, limited understandings of notice-and-takedown and site and facilities.

---

[379] *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1022 (9th Cir. 2001); *supra* Part IV.B.2.

[380] Marvullo v. Gruner & Jahr, 105 F. Supp. 2d 225, 230 (S.D.N.Y. 2000).

[381] Warren v. John Wiley & Sons, Inc., 952 F. Supp. 2d 610, 619 (S.D.N.Y. 2013).

[382] *See, e.g.*, Demetriades v. Kaufmann, 690 F. Supp. 289, 293-94 (S.D.N.Y. 1988) (declining to find material contribution where the defendant did not "provide[] the means or facilities for the admitted copying").

Following *Grokster*, the Ninth Circuit applied the simple measures test in *Perfect 10 v. Amazon* and other cases, requiring the platform to take "simple measures to prevent further damage to copyrighted works, [while not] continu[ing] to provide access to infringing works."[383] Courts outside of the Ninth Circuit have also looked to simple measures or adopted a similar test.[384] For example, the Fourth Circuit has noted that "the proper standard requires a defendant to have specific enough knowledge of infringement that the defendant *could do something about it*."[385] Scholars such as Fred Yen have similarly argued that there should be a stronger case for liability where a service provider can take simple measures to prevent infringement but does not, than where the precaution is difficult or impossible without also suppressing legitimate conduct.[386]

As a flexible framework, the simple measures test requires what a contributory infringement defendant is reasonably capable of doing. Forwarding notices of infringement to website operators was an appropriate simple measure in one case.[387] Disabling or removing content or even a storefront, where possible, could also be a simple

[383] Perfect 10, Inc. v. Amazon.com, Inc., 487 F.3d 701, 729 (9th Cir. 2007) (quoting Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc., 907 F. Supp. 1361, 1375 (N.D. Cal. 1995)); *see also* VHT, Inc. v. Zillow Grp., Inc., 918 F.3d 723, 745 (9th Cir. 2019); Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 671 (9th Cir. 2017).

[384] *See, e.g.*, Millennium Funding, Inc. v. 1701 Mgmt. LLC, No. 21-cv-20862-BLOOM/Otazo-Reyes, 2022 WL 901745, at *5 (S.D. Fla. Mar. 28, 2022) (finding that defendant could have implemented "simple measures such as null-routing and/or logging IP addresses to stop unauthorized distribution of Plaintiffs' Works"); Sony Music Ent. v. Cox Commc'ns, Inc., 464 F. Supp. 3d 795, 816 (E.D. Va. 2020), *overturned on other grounds by* 93 F. 4th 222 (4th Cir. 2024) (noting that Cox took "simple measures to prevent infringement through its graduated response system"); UMG Recordings, Inc. v. Grande Commc'ns Networks, LLC, 384 F. Supp. 3d 743, 768 (W.D. Tex. 2019) (applying the simple measures test); Tomelleri v. Zazzle, Inc., No. 13-CV-02576-EFM-TJJ, 2015 WL 8375083, at *14 (D. Kan. Dec. 9, 2015) (applying the Ninth Circuit's contributory liability test).

[385] BMG Rts. Mgmt. (US) LLC v. Cox Commc'ns, Inc., 881 F.3d 293, 311-12 (4th Cir. 2018) (emphasis added).

[386] *See* Yen, *Torts and the Construction of Inducement*, *supra* note 16, at 522.

[387] ALS Scan, Inc. v. Steadfast Networks, LLC, 819 F. App'x 522, 523 (9th Cir. 2020). However, the court did not address whether this would be sufficient if the website operator did not remove the infringing content. *See id.* at 523-24 (noting that "every infringing work was taken down" by the operator).

measure.[388] But the Ninth Circuit rejected watermarking technology as a simple measure.[389] It also rejected manually running search terms against messages to proactively locate infringement.[390]

In the case of blockchain, the content is immutable, so the simple measures test should only require what action platforms *could* take to limit the infringement. For example, if a platform can remove infringing NFTs under the applicable smart contract, it would likely be required to do so under the simple measures test. Even if it cannot delete the content due to the NFT's immutability, it may have other obligations to reduce infringement on its platform. It should perhaps have to stop the display of the infringing NFT content (if possible).[391] For example, OpenSea, in response to notice-and-takedown notices, will delist the reported NFT from being displayed on its platform so the public cannot see it.[392] But OpenSea notes that "[t]he item or collection will still exist on the blockchain (we don't have the power to change that!)."[393] This would reduce some of the effects of infringement, even if it would not stop the infringement entirely. The platform may even be required to burn the content if it is not unduly burdensome, although the high costs may weigh against this approach.[394]

However, the simple measures test would not impose liability for platforms' own innate traits such as immutability. Such an outcome would seem contrary to the rule in *Sony* that merely providing a product that has infringing capabilities should not be sufficient for liability and would be unmoored from intent animating secondary liability

---

[388] *See, e.g.*, Dunham v. Lei, No. CV 20-3716-DMG (MAAx), 2021 WL 4595808, at *7 (C.D. Cal. June 7, 2021) (considering the removal of a storefront selling infringing products to be a simple measure); Oppenheimer v. Allvoices, Inc., No. C 14-00499 LB, 2014 WL 2604033, at *7 (N.D. Cal. June 10, 2014) (considering content removal and disabling access between Allvoices' system and other websites containing infringing content to be simple measures).

[389] *See* VHT, Inc. v. Zillow Grp., Inc., 918 F.3d 723, 745 (9th Cir. 2019).

[390] *See* Perfect 10, Inc. v. Giganews, Inc., 847 F.3d 657, 671 (9th Cir. 2017).

[391] *See supra* notes 359–362 and accompanying text.

[392] *See Why Are My Items and Collections Delisted?*, OPENSEA, https://support.opensea.io/en/articles/8867135-why-are-my-items-and-collections-delisted (last visited Jan. 21, 2025) [https://perma.cc/3C8X-FM2R].

[393] *Id.*

[394] *See supra* notes 359–362 and accompanying text.

refinements. The inducement theory can capture true malefactors that would not otherwise be captured by the simple measures test.

Intent could help guide courts to the simple measures test as a balance-promoting refinement for secondary liability in response to Web3 architectural infringement claims. The simple measures test — unlike its fellow material contribution tests — is attuned to the capabilities of parties and their choice to take or forgo an action within those capabilities. Since it is not a static test, the flexibility of the simple measures test could accommodate not just blockchain but other future information architectures too, including generative AI and the notice-and-revision structure I proposed in Part IV.A.

CONCLUSION

If history is any lesson, generative AI and blockchain will not be the final information architectures. They, like their predecessors from the printing press to peer-to-peer file exchanges, are merely stages in the evolution of information technology. As new information architectures arise, they too will likely face architectural infringement claims and the accompanying significant liability risks and challenges to copyright's incentives-access balance. Almost by definition, information architectures contain novel features that create scenarios that copyright law has not yet addressed. As explained in this Article, architectural infringement claims against new information architectures can therefore pose serious risks to balancing copyright law's goals. However, the uncovered polestar of intent for secondary liability refinements can assist courts and Congress in maintaining balance between incentives and access in the face of technological progress while furthering competition and promoting free speech. Intent was not just the solution to past crossroads of copyright law, information, and innovation, but also a valuable tool for future intersections we have not yet reached.