SURVEY OF ADDITIONAL IP AND TECHNOLOGY LAW DEVELOPMENTS

Berkeley Technology Law Journal†

TABLE OF CONTENTS

I. PATENT DEVELOPMENTS 1050

A. SNAPRAYS, LLC V. LIGHTING DEFENSE GROUP, LLC 1050
B. REGENTS OF THE UNIVERSITY OF CALIFORNIA V. BROAD INSTITUTE 1051

II. COPYRIGHT DEVELOPMENTS 1053

A. WARNER CHAPPELL MUSIC, INC. V. NEALY 1053
B. APPLE INC. V. CORELLIUM, INC. 1055

III. TRADE SECRET DEVELOPMENTS 1056

A. PEGASYSTEMS INC. V. APPIAN CORP. 1056
1. Motion to Strike and Set Aside the Verdict 1057
2. Jury Instructions 1058
3. Exclusion of Evidence 1059

IV. PRIVACY AND CYBERLAW DEVELOPMENTS 1060

A. MURTHY V. MISSOURI 1060
B. NATIONAL RIFLE ASSOCIATION OF AMERICA V. VULLO 1062
C. GEOFENCE WARRANTS & REVERSE KEYWORD WARRANTS 1063
D. MEDICAL IMAGING & TECHNOLOGY ALLIANCE V. LIBRARY OF CONGRESS 1065
E. ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT 1067
F. EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT 1068
1. What AI Systems Are Prohibited? 1068
2. Risk Categories 1069
3. Extraterritoriality and Enforcement 1069
4. Sandboxes 1070
5. Noncompliance and Enforcement 1070
G. ARTIFICIAL INTELLIGENCE, INVENTORSHIP, AND AUTHORSHIP 1070
1. USPTO Guidelines on AI Inventorship 1070

DOI: https://doi.org/10.15779/Z38X921M6T
© 2025 Berkeley Technology Law Journal.
† Editors of the Berkeley Technology Law Journal.

2. USCO Guidelines on AI Authorship 1071
3. Conclusion 1072
4. Doe v. Github 1072

V. ANTITRUST DEVELOPMENTS 1073

A. EPIC GAMES INC. V. APPLE, INC. 1073
B. UNITED STATES V. GOOGLE, LLC 1074

I. PATENT DEVELOPMENTS

A. SNAPRAYS, LLC V. LIGHTING DEFENSE GROUP, LLC

SnapRays v. Lighting Defense Group presents a novel way to find personal jurisdiction over a defendant outside of their home state by using Amazon.com's procedure to remove patent-infringing product listings.[1] The Amazon Patent Evaluation Express (APEX) is a low-cost procedure "to efficiently resolve claims that third-party product listings infringe utility patents."[2] To initiate an APEX proceeding, a patent owner submits an APEX agreement identifying a patent claim and up to twenty allegedly infringing listings to Amazon.[3] When Amazon sends the APEX Agreement, it send it to all sellers who have three options to avoid automatic removal: (1) opt into the APEX program and its subsequent third-party evaluation, (2) resolve the claim directly with the patent owner, or (3) file a lawsuit for declaratory judgement of noninfringement.[4] If the alleged infringer takes no action after three weeks, Amazon removes the accused listings.[5]

In *SnapRays*, the appellee, Lighting Defense Group (LDG), was a Delaware limited liability company with its principal place of business in Arizona.[6] Appellant and patent owner, SnapPower (SP), is a Utah company with its principal place of business in Utah.[7] Both LDG and SP sell products on Amazon.com.[8]

LDG submitted an APEX Agreement, which notified SP as a potential infringer.[9] In response, SP filed a motion for declaratory judgement of

1. *See* SnapRays v. Lighting Def. Grp., 100 F.4th 1371, 1378 (Fed. Cir. 2024).
2. *Id.* at 1373.
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.* at 1374.

noninfringement in Utah.[10] LDG then filed a motion to dismiss for a lack of personal jurisdiction, which the district court granted, citing a lack of sufficient contacts in Utah.[11] The district court found that "SnapPower did not demonstrate LDG purposefully directed activities at SnapPower in Utah, or that the action arose out of or related to any LDG activities in Utah" and instead found that "LDG's allegations of infringement were directed toward Amazon in Washington, where the APEX Agreement was sent."[12] SP appealed.[13]

Personal jurisdiction has three factors: "(1) whether the defendant 'purposefully directed' its activities at residents of the forum; (2) whether the claim 'arises out of or relates to' the defendant's activities with the forum; and (3) whether assertion of personal jurisdiction is 'reasonable and fair."[14] If (1) and (2) are met, jurisdiction is "presumptively reasonable" unless defendant presents a compelling case that makes it otherwise.[15]

Here, the Federal Circuit held that specific jurisdiction over LDG in Utah was proper.[16] On factor (1), the court held that LDG, by intentionally submitting the APEX Agreement to Amazon, purposefully directed activities in Utah, knowing that Amazon would notify SP and potential inaction from SP would automatically affect activities in Utah by delisting SP's products.[17] Submitting the APEX Agreement was also sufficient to meet factor (2); this action "arose out of" LDG's activities with the forum because the APEX Agreement was directed towards SP in Utah, aimed to affect "marketing, sales, and other activities."[18] On factor (3), the court held that LDG failed to present a compelling case as the floodgates concern was limited to only APEX and its subsequent allegedly infringing states.[19] Taken together, the court found that LDG's action satisfied the test for specific personal jurisdiction.[20]

B. REGENTS OF THE UNIVERSITY OF CALIFORNIA V. BROAD INSTITUTE

In *Regents of the University of California v. Broad Institute*, researchers from the University of California and the Broad Institute each alleged that they were the

10. *Id.*
11. *Id.*
12. *Id.*
13. *Id.*
14. *Id.* (citing Xilinx, Inc. v. Papst Licensing GmbH & Co. KG, 848 F.3d 1346, 1353 (Fed. Cir. 2017) (internal citations omitted)).
15. *Id.* at 1375 (citing *Xilinx*, 848 F.3d at 1356 (internal citations omitted)).
16. *Id.* at 1378.
17. *Id.* at 1375.
18. *Id.* at 1377.
19. *Id.* at 1378.
20. *Id.*

first to invent a "CRISPR-Cas9 system that contains a 'single-guide' RNA that edits or cleaves DNA in eukaryotic cells."[21] CRISPR-Cas9, or more colloquially, CRISPR, is a novel method by which researchers can edit cellular DNA.[22] Bioengineering labs around the world using CRISPR have had "a revolutionary impact on the life sciences" and have "contribut[ed] to new cancer therapies and may make the dream of curing inherited diseases come true."[23] For their work on this technology, Jennifer A. Doudna from the University of California, Berkeley and Emmanuelle Charpentier from Max Planck Unit for the Science of Pathogens received the Nobel Prize in Chemistry.[24]

As a result of both The Regents of the University of California ("Regents") and Broad Institute ("Broad") both claiming to be the inventor of CRISPR in various patent applications, the Patent Trial and Appeal Board (PTAB) instituted an interference—an administrative procedure in which the Patent Office determines "which party first invented the commonly claimed invention."[25] In this context, invention is defined by conception or "the formation in the mind of the inventor, of a definite and permanent idea of the complete and operative invention, as it is hereafter to be applied in practice."[26] In the interference proceeding, the PTAB determined that Regents had not proved that they had conceived of CRISPR before Broad because "Regents' scientists did not know their CRISPR-Cas9 system would produce the effects on genes in a eukaryotic cell."[27]

Regents argued that the PTAB erred by "requiring Regents' scientists to know that their invention would work."[28] The Federal Circuit agreed, holding that "[a]t the conception stage, it is well-established that an inventor need not know that his invention will work for conception to be complete."[29] In the PTAB proceeding, the PTAB relied on "Regents' scientists' statements expressing uncertainty about whether the experiments had succeeded" to conclude that the Regents had not conceived of the invention when they

21. Regents of the Univ. of Cal. v. Broad Inst., Inc., 136 F.4th 1367, 1371 (Fed. Cir. 2025).

22. *See id.*

23. Press Release, *Nobel Prize Outreach 2025*, NOBEL PRIZE (Oct. 7, 2020), https://www.nobelprize.org/prizes/chemistry/2020/press-release/.

24. *Id.*

25. *Regents*, 136 F.4th at 1375; MPEP § 2301 (9th ed. Rev. 1, 2024).

26. *Regents*, 136 F.4th at 1378 (quoting Burroughs Wellcome Co. v. Barr Lab'ys, Inc., 40 F.3d 1223, 1228 (Fed. Cir. 1994)).

27. *Id.*

28. *Id.*

29. *Id.* (quoting *Burroughs*, 40 F.3d at 1228 (internal citations omitted)).

claimed.[30] The Federal Circuit distinguished "factual uncertainty that bears on the problem of conception and general uncertainty surrounding experimental sciences" by stating that "[f]actual uncertainty is when the subsequent course of experimentation, especially experimental failures, reveals uncertainty that so undermines the specificity of the inventor's idea that it is not yet a definite and permanent reflection of the complete invention as it will be used in practice."[31] The court found that the PTAB erred by "focusing on Regents' scientists' statements of uncertainty, without considering whether those statements led to modifications in their experiments that substantively changed their original idea, when determining whether they had a 'definite and permanent idea.'"[32]

The Federal Circuit found that the PTAB had not used the proper framework for determining conception, vacated the previous decision, and remanded for proper application of the legal framework.[33]

II. COPYRIGHT DEVELOPMENTS

A. WARNER CHAPPELL MUSIC, INC. V. NEALY

In *Warner Chappell Music, Inc. v. Nealy*, the Supreme Court held that a plaintiff who files a timely copyright infringement claim is entitled to damages and not restricted by when the infringement occurred.[34] This decision overrules the previous interpretation of the Copyright Act, which had previously applied the three-year time limit for discovering the infringement to the time period a plaintiff could also collect damages.[35]

In 1983, Sherman Nealy and Tony Butler formed a short-lived musical collaboration, Music Specialist, Inc., which created the copyrighted works at issue in this case.[36] After the collaboration dissolved, Butler licensed the work of Music Specialist, Inc. to Warner Chappell Music, Inc. without Nealy's knowledge.[37] This license resulted in the songs being interpolated and used in many other songs, including one in the popular show "So You Think You Can Dance" (Flo Rida's "In the Ayer").[38]

30. *Id.*
31. *Id.* at 1379 (quoting *Burroughs*, 40 F.3d at 1229 (internal citations omitted)).
32. *Id.* (quoting *Burroughs*, 40 F.3d at 1230).
33. *Id.* at 1382.
34. Warner Chappell Music, Inc. v. Nealy, 601 U.S. 366, 374 (2024).
35. *See* 17 U.S.C. § 507(b); Petrella v. Metro-Goldwyn-Mayer, Inc., 572 U.S. 663, 685 (2014).
36. *Warner Chappell Music*, 601 U.S. at 368.
37. *Id.* at 368–69.
38. *Id.* at 369.

In 2018, after discovering Warner Chappell's use of the songs in 2016, Nealy sued Warner Chappell for copyright infringement dating back to 2008.[39] Warner argued that even though Nealy's claims were within the three-year discovery period, he could only recover damages from infringing activity that occurred within the last three years.[40] The District Court for the Southern District of Florida relied on a decision from the Second Circuit[41] and agreed with Warner Chappell that Nealy could not recover money from infringing acts beyond the three years prior to filing the claim.[42] The Court of Appeals for the Eleventh Circuit reversed, stating Nealy's claims were timely under the discovery rule and there is no time limitation for the recovery of damages.[43]

Many circuits had used the previous Supreme Court decision, *Petrella v. Metro-Goldwyn-Mayer, Inc.*, to argue in favor of the three-year restriction on damages.[44] The language in that case, taken out of context, could support the time limit on relief, but the Court clarified that the limitations in *Petrella* on relief were discussed when the plaintiff did not file a timely claim.[45] In *Petrella*, the plaintiff had known of the defendant's infringement longer than three years and could only file for the infringements that occurred in the three years before her claim.[46] The Court determined that that is not the situation at issue in this case because the plaintiff filed within three years of discovering the infringement and therefore the claim was timely.[47]

The Supreme Court ultimately concluded that there was no time limit on damages in the Copyright Act or its remedial sections.[48] Judge Gorsuch's dissenting opinion argued that because the infringement acts took place so long before Nealy's discovery that his claims were untimely, and therefore, he should not be able to recover damages.[49] The Court's five-three decision affirmed the Eleventh Circuit's opinion that Nealy should be able to recover all damages.[50]

39. *Id.* at 369–70.
40. *Id.* at 370.
41. *See* Sohm v. Scholastic Inc., 959 F.3d 39, 51–52 (2d Cir. 2020).
42. *Warner Chappell Music*, 601 U.S. at 370.
43. *Id.* at 374.
44. *See id.* at 373.
45. *Id.* at 372.
46. *Petrella*, 572 U.S. at 670.
47. *Warner Chappell Music*, 601 U.S. at 374.
48. *See id.*
49. *Id.* at 375 (Gorsuch, J., dissenting).
50. *Id.* at 366.

B. APPLE INC. V. CORELLIUM, INC.

Apple Inc. sued Corellium, Inc. in 2019, alleging copyright infringement in Corellium's virtualization software, CORSEC, that could run iOS on non-Apple hardware.[51] Apple brought three specific claims: (1) direct copyright infringement of iOS, (2) direct copyright infringement of Apple's icons and wallpapers, and (3) contributory copyright infringement of the aforementioned icons and wallpapers.[52] The district court granted summary judgment for Corellium on all three claims, finding that fair use protected Corellium's use.[53] After the district court's summary judgment for Corellium, Apple appealed to the Eleventh Circuit.[54]

In 2023, the Eleventh Circuit affirmed the district court's finding that Corellium's use of iOS was protected by fair use but vacated and remanded counts two and three because the district court had not independently analyzed those claims.[55] Apple's subsequent petition for rehearing was denied.[56]

In its opinion, the Eleventh Circuit thoroughly analyzed the four statutory fair use factors. First, the court found that CORSEC was "moderately transformative" because it added features not available on iOS that serve security research purposes, including the ability to see and halt running processes, modify the kernel, and take live snapshots.[57] While acknowledging that Corellium's use was commercial, the court noted that "many fair uses are commercial" and that "Corellium's commercial use does little to change [the] analysis" within the first factor.[58]

Second, the court recognized that while iOS's nature embodies some creativity, it is a "primarily functional" software that falls "'further . . . from the core of copyright' than protected works like paintings, movies, and books."[59] Third, the court found that Corellium's copying was "reasonable in relation to the purpose of the copying" and "proportional and necessary to achieve Corellium's transformative purpose."[60] Fourth, the court found "no evidence that [CORSEC] had affected, let alone materially affected, Apple's

51. Apple Inc. v. Corellium, Inc., No. 21-1283, 2023 WL 3295671 (11th Cir. 2023).
52. *Id.* at *3.
53. *Id.* at *4.
54. *Id.*
55. *Id.* at *1.
56. *Id.*
57. *Id.* at *6.
58. *Id.* at *9.
59. *Id.* at *10 (quoting Google LLC v. Oracle Am., Inc., 593 U.S. 1, 29 (2021)).
60. *Id.* at *13.

market or the market value for iOS."[61] The court specifically noted that CORSEC is "a poor substitute for iOS on a real iPhone."[62]

Corellium establishes an important precedent for security research and the fair use of software. The ruling recognizes that creating virtualization software enabling security researchers to study operating systems constitutes fair use, even when that use is commercial in nature.[63] This decision reinforces the notion that copyright law's fair use doctrine provides important protections for security research that ultimately serves the public interest by improving the security and functionality of widely used software.[64] The Eleventh Circuit's reasoning aligns with copyright's constitutional purpose "to promote the progress of science and useful arts" by allowing transformative uses that advance scientific progress without superseding an original work's market.[65]

III. TRADE SECRET DEVELOPMENTS

A. PEGASYSTEMS INC. V. APPIAN CORP.

In *Pegasystems Inc. v. Appian Corp.*, the Virginia Court of Appeals reversed a jury verdict with a damage award exceeding $2 billion, remanding the case for a new trial due to erroneous jury instructions and improper exclusion of evidence.[66] Appian and Pegasystems are competitors within the business process management (BPM) industry, offering platforms where third-party business customers can build complex software applications to automate their own business functions.[67] While Pegasystems focused primarily on serving larger companies by offering reliability and scalability, Appian's platform emphasized a user-friendly experience through ease-of-use and simplicity.[68] Here, Appian alleged Pegasystems misappropriated trade secrets to imitate Appian's user-friendly features.[69] Pegasystems did not have direct access to Appian's platform because it was not made publicly available without license terms.[70] To bypass this control and maintain secrecy, Pegasystems's head of intelligence, John Petronio, hired consultant Youyong Zou, who had access to Appian's platform through his job and provided 200 hours of consultation,

61. *Id.* at *12.
62. *Id.*
63. *See id.* at *9–10.
64. *See id.* at *10.
65. U.S. CONST. art. I, § 8, cl. 8; *see Apple v. Corellium*, 2023 WL 3295671, at *12.
66. Pegasystems Inc. v. Appian Corp., 81 Va. App. 433, 448, 508 (2024).
67. *Id.* at 449.
68. *Id.* at 449–50.
69. *Id.* at 450.
70. *Id.* at 450.

including nearly 100 videos demonstrating the platform's features and analyzing their strengths and weaknesses.[71] In 2015, Petronio left Pegasystems and was later hired by Appian as a consultant, eventually revealing the illicit activities he undertook at Pegasystems, leading to the dispute at issue.[72]

Appian sued under the Virginia Uniform Trade Secrets Act (VUTSA)[73] and the Virginia Computer Crimes Act,[74] claiming Pegasystems misappropriated trade secrets and confidential documentation.[75] Key points of dispute between the parties included whether the information constituted a trade secret, as determined by whether adequate secrecy was maintained; whether Pegasystems's improvements were the result of corporate espionage or independently developed; admissibility of evidence; and the method of determining damages.[76] At trial, the jury returned a verdict for Appian, finding Pegasystems and Zou misappropriated trade secrets in violation of VUTSA and awarded $2,036,860,045 in damages—the largest damage award in Virginia's history—plus attorney fees, costs, and interest.[77] The trial court denied Pegasystems's motions to strike the evidence and set aside the verdict, as well as Pegasystems's request for a new trial subject to remittitur.[78] Pegasystems subsequently appealed.[79]

1. Motion to Strike and Set Aside the Verdict

First, the Court of Appeals affirmed the trial court's denial of Pegasystems's motions to strike and set aside the verdict.[80] The court rejected Pegasystems's arguments that (1) "none of Appian's purported secrets were trade secrets as a matter of law because they exposed them without requiring confidentiality" and (2) "Appian did not identify key trade secrets with requisite particularity," instead asserting these issues were "questions for the factfinder."[81] When addressing the first argument, the court emphasized that Virginia does not require "absolute secrecy," but rather permits licensing and disclosures "made in confidence."[82] Furthermore, the court noted that there

71. *Id.* at 449–51.
72. *Id.* at 452.
73. VA. STAT. § 59.1-336–343.
74. VA. CODE § 18.2–152.1.
75. *Pegasystems*, 81 Va. App. at 452, 454–55.
76. *Id.* at 455–62.
77. *Id.* at 448, 463.
78. *Id.* at 463.
79. *Id.* at 463.
80. *Id.* at 476.
81. *Id.* at 464–65.
82. *Id.* at 466 (quoting Dionne v. SE Foam Converting & Packaging, Inc., 240 Va. 297, 302 (1990)).

was "considerable evidence that [Appian] took careful steps to safeguard its secrets," including the use of license agreements, restricted access to documentation, firewalls, multifactor authentication, encryption, user authentication, and password change requirements.[83] In response to the particularity argument, the court noted Appian's expert witness provided testimony for almost three days, which resulted in over 800 transcript pages, providing sufficient detail about the trade secrets Pegasystems was accused of misappropriating.[84] Consequently, the court found the cause of action was sufficient to survive a motion for judgment as a matter of law, drawing all reasonable inferences in favor of Appian, the non-moving party, thus, the trial court did not err in its denial.[85]

2. Jury Instructions

Second, the Court of Appeals rejected the trial court's instructions to the jury regarding the burden of proving proximate causation, thus leading to a reversal and remand for a new trial.[86] The instruction in question shifted the burden of proof such that Appian was only required to prove misappropriation of a trade secret and Pegasystems's total sales revenue rather than proving the misappropriation of trade secrets was the proximate, or "but-for," cause of Pegasystems's sales.[87] As a result of the erroneous jury instruction, the burden shifted to Pegasystems to prove what portion of the sales were not attributable to the allegedly misappropriated trade secrets.[88] In other words, Appian only had to establish Pegasystems was enriched rather than the higher burden of proving "unjust enrichment."[89] The burden-shifting approach utilized by the trial court contravened both the statute and Virginia's jurisprudence.[90] The court emphasized that even under the Restatement, only after the plaintiff has established sales causation does the burden shift to the defendant to raise other considerations, such as expenses to be deducted from revenues and the apportionment of sales resulting from misappropriated information relative to "just" profits.[91]

83. *Id.* at 469.
84. *Id.* at 475.
85. *Id.* at 466–67, 472, 476.
86. *Id.* at 476.
87. *Id.* at 477, 479.
88. *Id.* at 477.
89. *Id.* at 479.
90. *Id.* at 479–81; VA. CODE § 59.1-338(A); *see* Hale v. Fawcett, 214 Va. 583, 585–86 (1974).
91. *Pegasystems*, 81 Va. App. at 483–84.

3. Exclusion of Evidence

Finally, the Court of Appeals ruled that the trial court abused its discretion in excluding evidence relevant to damages and causation as well as Pegasystems's software evidence.[92] The exclusion of evidence that would have aided Pegasystems in demonstrating that over 50% of its sales revenue was attributable to unrelated products was excluded by the trial court due to an incorrect interpretation of an interrogatory, in which the court conflated "products" and "versions" of the same product rather than distinguishing them.[93] As a result, Pegasystems was essentially prohibited from providing a breakdown of its revenue by product line.[94] This led to a much higher damage award than appropriate, particularly when combined with the erroneous burden-shifting instruction provided by the trial court.[95] During the trial, Pegasystems also sought to introduce a copy of the software at issue to demonstrate versions of the software to the jury.[96] The court denied this request, stating the laptop Pegasystems proposed to use was not the same laptop that had been provided to Appian during discovery.[97] In assessing whether the trial court abused its discretion, the Court of Appeals emphasized that Appian had been allowed to show the software on a different laptop, Pegasystems had exhibited the ability to authenticate the software, and Appian attacked Pegasystems during closing arguments for not presenting software evidence while arguing to the jury.[98] The Court of Appeals found no justification for the exclusion of the evidence in question, thus necessitating a new trial.[99]

Although not at issue on appeal, the court also provided direction regarding the trial court's instruction to the jury that the number of people with access to Appian's platform was not relevant.[100] The court emphasized that while user numbers alone are not determinative, it is relevant, being emphasized in both prior jurisprudence and the Restatement of Torts.[101] Consequently, the court directed that Appian's requested jury instruction

92. *Id.* at 491–92, 495.
93. *Id.* at 488–89.
94. *Id.* at 489.
95. *Id.* at 492.
96. *Id.* at 500.
97. *Id.* at 494–95.
98. *Id.* at 494–95, 501.
99. *Id.* at 491.
100. *Id.* at 501.
101. *Id.* at 504–05; *see* SI Handling Sys., Inc. v. Heisley, 753 F.2d 1244, 1256 (3d Cir. 1985); Restatement (First) of Torts § 757 cmt. b (1939).

regarding the irrelevance of evidence about the number of users should not be granted.[102]

IV. PRIVACY AND CYBERLAW DEVELOPMENTS

A. MURTHY V. MISSOURI

In *Murthy v. Missouri*, the Supreme Court reversed a Fifth Circuit decision regarding First Amendment rights and the misinformation on social media, holding that "neither the individual nor the state plaintiffs have established standing to seek an injunction against any defendant."[103]

Social media platforms like Meta have long been targeting harmful speech and misinformation, and they continued during the COVID-19 pandemic and the 2020 Presidential Election.[104] The White House publicly asked the platforms to work to address COVID-19 misinformation and brought up the possibility of making legal reforms aimed at the platforms.[105] The CDC worked with these platforms by sending reports alerting them to misinformation and providing fact checks to the platforms on claims about the pandemic.[106] Similarly, the FBI and Cybersecurity and Infrastructure Security Agency (CISA) communicated with the platforms about misinformation relating to the 2020 election, warning of potential Russian interference.[107]

The States of Missouri and Louisiana alleged that the platforms suppressed the speech of state entities, officials, and citizens.[108] The individual plaintiffs included doctors who questioned COVID-19 policies and received restrictions in 2020 on social media prior to the White House and CDC entering discussions with those platforms.[109] An individual, Jim Hoft, joined the suit because he claimed the CISA was tracking and restricting his content through X.[110] However, X suspended his brother's account, not his own.[111] Jill Heins hosted Heath Freedom groups on Facebook, which were demoted and deleted, allegedly in connection with the suggestions given to Meta by the White House.[112]

102. *Pegasystems*, 81 Va. App. at 507.
103. Murthy v. Missouri, 603 U.S. 43, 56 (2024).
104. *Id.* at 50–51.
105. *Id.* at 52.
106. *Id.* at 53.
107. *Id.*
108. *Id.*
109. *Id.* at 63.
110. *Id.* at 64.
111. *Id.*
112. *Id.* at 65.

When plaintiffs filed suit, the district court issued a preliminary injunction, holding that the government agencies likely "coerced" or "significantly encouraged" the platforms to make the moderation decisions that harmed the plaintiffs.[113] The Fifth Circuit agreed, reviewing the defendants' alleged coercive behavior and the district court's standing analysis.[114] The Fifth Circuit determined that all the government agencies at issue significantly encouraged or exercised "active, meaningful control" in the moderation, while only the White House officials, Surgeon General's office, and FBI coerced by implying "some form of punishment" would follow noncompliance.[115]

On review, the Supreme Court rejected that any plaintiffs had established standing to seek an injunction against any defendant.[116] The Court noted that Article III standing requires that a plaintiff show "that she has suffered, or will suffer, an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[117] The plaintiffs' claims related to the censorship of their speech or, in the case of the states, their "right to listen" to their citizens.[118] However, the plaintiffs were not seeking relief from the platforms that censored them—rather they were seeking an injunction against the government.[119] The Court analyzed each plaintiff's claims and found that none had standing because of a lack of "any concrete link between their injuries and the defendants' conduct" and because the plaintiffs sought "only forward-looking relief" and provided only evidence of past injuries.[120] The Court reversed and remanded the decision.[121]

The dissent sees this case as a crucial free speech case being wrongly decided because the coercion from the government was sophisticated.[122] The plaintiffs provided many instances where Meta was pressured by the Surgeon General's Office and other government entities.[123] The communications from the government could be seen as containing "thinly veiled threats" to Meta if they were not compliant.[124] The dissent disagreed that no plaintiffs had

113. Missouri v. Biden, 680 F. Supp. 3d 630, 694, 729 (W.D. La. 2023).
114. *See generally* Missouri v. Biden, 83 F.4th 350 (5th Cir. 2023).
115. *Id.* at 377, 380, 388, 389, 391.
116. *Murthy*, 603 U.S. at 56.
117. *Id.* at 57 (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (internal citations omitted)).
118. *Id.*
119. *Id.*
120. *Id.* at 58–59, 76.
121. *Id.* at 76.
122. *Id.* at 80 (Alito, J., dissenting).
123. *Id.* at 79–88 (Alito, J., dissenting).
124. *Id.* at 102–03 (Alito, J., dissenting) (citing Bantam Books, Inc. v. Sullivan, 372 U.S. 58, 68 (1963)).

standing, believing that Jill Hines did.[125] Hines demonstrated that the conduct of the officials in question was a factor leading to her censoring and the dissent saw this relationship as likely casual unlike the majority.[126] The dissent also believed that because Hines' censorship continued after suing, it passes the test of assuming future injury.[127]

B. NATIONAL RIFLE ASSOCIATION OF AMERICA V. VULLO

The National Rifle Association (NRA) sued Maria Vullo, former superintendent of the New York Department of Financial Services (DFS), alleging that Vullo violated the First Amendment rights of NRA by coercing DFS-regulated parties to punish or suppress the NRA's gun-promotion advocacy.[128] Vullo then filed a motion to dismiss, which was denied.[129] The Court of Appeals for the Second Circuit then reversed and remanded.[130] NRA then appealed the Supreme Court, which granted Certiorari.[131]

The NRA, as a benefit of membership, offered insurance policies such as "Carry Guard," which insured gun owners against from intentional criminal acts.[132] NRA promoted Carry Guard without the required insurance producer license.[133] Chubb Limited ("Chubb") and Lloyd's of London ("Lloyd's") underwrote this policy.[134] In the context of the Parkland shooting, DFS issued guidance letters to evaluate insurance companies' risks dealing with NRA, review any relationships with the NRA, and take prompt actions to manage these risks and promote public health and safety.[135] DFS then entered consent decrees and enforced insurance law violations against Chubb and Lloyd's, in which they admitted to violations of law, agreed to pay fines, and agreed not to provide any NRA-endorsed insurance programs.[136]

The Supreme Court on appeal sought to answer whether the factual allegations of the NRA complaint, if true, constructed a plausible scenario that Vullo engaged in conduct that could be "reasonably understood to convey a

125. *Id.* at 98 (Alito, J., dissenting).
126. *Id.* (Alito, J., dissenting).
127. *Id.* at 92. (Alito, J., dissenting).
128. Nat'l Rifle Ass'n of Am. v. Vullo, 602 U.S. 175, 180–81 (2024).
129. *Id.* at 181.
130. *Id.* at 186.
131. *Id.*
132. *Id.* at 181.
133. *Id.* at 181–82.
134. *Id.* at 182.
135. *Id.* at 176, 182.
136. *Id.* at 176.

threat of adverse government action in order to punish or suppress the plaintiff's speech."[137]

The alleged facts are as follows: Vullo conducted private meetings with DFS regulated entities, particularly with Lloyd's.[138] Vullo cited insurance-law violations of Lloyd's and said that if they were to cease in providing insurance to pro-gun groups such as the NRA, DFS would be "less interested in pursuing the infractions" and Vullo would focus her enforcement actions "solely" on the syndicates with ties to the NRA.[139] Lloyd's then instructed its syndicates to terminate existing agreements with the NRA and publicly announced its decision to cut ties with the NRA.[140]

Here, the Court held that the alleged facts were sufficient to demonstrate Vullo's violation of the First Amendment rights of NRA.[141] Under *Bantam Books*, a government official may not indirectly do what she could not directly do—using governmental powers to coerce insurance companies and effectively suppress NRA activity in this case.[142] Three contextual factors constituted coercion: (1) Vullo's authority and power to enforce and regulate insurance companies in New York, (2) Vullo's alleged communications with DFS-regulated entities, and (3) the reaction of Lloyd's to cease underwriting firearm-related policies, scale back its NRA related business, and terminate all insurance policies related to the NRA.[143] Taken together, the Court held that Vullo's communications with Lloyd's can be "reasonably understood as . . . coercive."[144] The complaint, when "assessed as a whole" plausibly alleged that Vullo violated the First Amendment by threatening to use her power against those refusing to aid in her push to punish NRA's advocacy.[145] The Court vacated the Second Circuit's opinion and remanded for further proceedings.[146]

C. GEOFENCE WARRANTS & REVERSE KEYWORD WARRANTS

The increasing use and people's diverging opinions about geofence warrants sparked a split between the Fourth and Fifth Circuits over their constitutionality under the Fourth Amendment. Geofence warrants compel information about anyone whose mobile device located them within a

137. *Id.* at 191.
138. *Id.* at 192.
139. *Id.*
140. *Id.* at 193.
141. *Id.* at 198.
142. *Id.* at 190 (citing *Bantam Books*, 372 U.S. at 67–69).
143. *Id.* at 189–91.
144. *Id.* at 193.
145. *Id.* at 194.
146. *Id.* at 199.

geographic area during a specific time.[147] Unlike traditional warrants, geofence warrants seek to identify suspects based on geographic and temporal circumstances, rather than requesting information about known suspects.[148]

In *United States v. Chatrie*, the Fourth Circuit held that geofence warrants do not constitute a Fourth Amendment search under the third-party doctrine.[149] The Court reasoned that since users must opt-in to Location History collection,[150] maintain some control over the data,[151] and voluntarily provide the data to Google,[152] the defendant therefore lacked a reasonable expectation of privacy.[153]

Conversely, in *United States v. Smith*, the Fifth Circuit ruled that geofence warrants are unconstitutional modern-day general warrants, but applied the good-faith exception to allow the warrant in this instance.[154] The court criticized geofence warrants as "general, exploratory rummaging" prohibited by the Fourth Amendment, because they target "anything or everyone in sight" and not a specific individual.[155] Moreover, the court found that the defendant had an expectation of privacy in just a few hours of location data, given the data's intrusive nature and that cell phones which collect location data are essential in modern life.[156] The Court rejected the third-party doctrine because users are "hardly informed" about forfeiting their Fourth Amendment rights when opting-in to Location History, especially when encouraged to do so across multiple apps.[157]

In November 2024, *Chatrie* was granted a rehearing,[158] potentially leading to a ruling more aligned with *Smith*. The new ruling may also consider Google's policy change to store location data on users' devices instead of Google data centers, making this data unavailable for Google to comply with geofence warrants.[159]

147. *Reverse Search Warrants*, NAT'L ASS'N OF CRIM. DEF. LAWS., https://www.nacdl.org/Landing/Reverse-Search-Warrants (last visited Apr. 19, 2025).

148. *Id.*

149. United States v. Chatrie, 107 F.4th 319, 339 (4th Cir. 2024).

150. *Id.* at 322.

151. *Id.* at 323.

152. *Id.* at 322, 325–26.

153. *Id.* at 330.

154. United States v. Smith, 110 F.4th 817, 820, 840 (5th Cir. 2024).

155. *Id.* at 836–37.

156. *Id.* at 827, 832–33.

157. *Id.* at 823, 835–36.

158. United States v. Chatrie, No. 22-4489, 2024 WL 4648102 (4th Cir. Nov. 1, 2024).

159. Mario McGriff, *Updates to Location History and New Controls Coming Soon to Maps*, GOOGLE BLOG (Dec. 12, 2023), https://blog.google/products/maps/updates-to-location-history-and-new-controls-coming-soon-to-maps/.

Similarly, reverse keyword warrants raise constitutional questions regarding users' search histories. Like geofence warrants, reverse keyword warrants compel search histories from all users who searched specific terms within a defined timeframe, before suspects are identified.[160]

Only the Colorado Supreme Court has ruled on reverse keyword warrants. In *People v. Seymour*, Colorado held that the defendant had a reasonable expectation of privacy in his searches, but found the warrant sufficiently particularized based on narrow search terms, time frame constraints, and initial anonymization of results.[161] The Court also applied the good-faith exception given the search's unprecedented nature.[162] The Court did not apply the third-party doctrine because the Colorado Constitution provides stronger privacy protections.[163] *Seymour* thus echoes aspects of both *Chatrie* and *Smith*. Like location data in *Chatrie*, the *Seymour* Court suggests that the third-party doctrine may apply to search history data since users voluntarily submit queries to third-party search engines.[164] Like *Smith*, *Seymour* found both an expectation of privacy in the data and applied the good-faith exception to a novel law enforcement practice.[165]

Ultimately, considerable uncertainty remains for the constitutionality of both geofence and reverse keyword warrants, given the circuit split on geofence warrants, and that reverse keyword warrants have yet to be examined in federal court.

D. MEDICAL IMAGING & TECHNOLOGY ALLIANCE V. LIBRARY OF CONGRESS

The United States Court of Appeals for the District of Columbia Circuit vacated and remanded a motion to dismiss in the District Court for the District of Columbia.[166] The Court of Appeals considered the question: Are rules for copyright under the Digital Millennium Copyright Act (DMCA) reviewable under the Administrative Procedure Act (APA)?[167] The Court said yes.[168]

The DMCA anti-circumvention laws protect digital media from infringement.[169] At the same time, these laws make non-infringing uses harder

160. *Reverse Search Warrants*, *supra* note 147.
161. People v. Seymour, 536 P.3d 1260, 1267, 1270 (Colo. 2023).
162. *Id.* at 1278–79.
163. *Id.* at 1272.
164. *Id.*
165. *Id.* at 1272.
166. Med. Imaging & Tech. All. v. Libr. of Cong., 103 F.4th 830, 841 (D.C. Cir. 2024).
167. *Id.* at 833.
168. *Id.*
169. *Id.*

through the prevention of access.[170] The Library of Congress has a process for addressing copyright issues that involves submitting applications to the Register of the Copyright Office.[171] The Register evaluates several factors, including the proposed use, its impact on fair use, and its effect on the market, before making a recommendation to the Librarian of the Library of Congress.[172] The plaintiffs are trade associations representing medical device manufacturers for devices such as MRI machines and surgery-assisting robots.[173] These companies have previously pushed against access to their software by third parties.[174] Independent service operations petitioned the Copyright Office for an exemption to the DMCA's anti-circumvention provision, claiming it was fair use to access information on repairs because, without them, they couldn't do their necessary duties during the pandemic.[175] The Register recommended the Library grant this exemption because they were fair uses that the provision was negatively impacting, such as the diagnosis and maintenance of medical devices and systems.[176]

The District Court held that APA claims were barred by the Library of Congress's sovereign immunity.[177] However, the Court determined DMCA rules, like any copyright rules, are subject to the APA.[178] The APA governs copyright decisions meaning the DMCA rules are subject to the APA and should be seen *in pari materia*, or "as if they were one law."[179] Because the APA applies, there is, therefore, no sovereign immunity barring the claims.[180] Courts have the power to provide judicial review on administrative actions.[181] While Congress could withhold that review, that is not the case here because there is no indication Congress would want the Librarian and Register to not have their power checked by judicial review.[182] While the defense argues that the Library of Congress is free from judicial review, Title 17 specifies that the APA applies to "all actions taken by the Register of Copyrights."[183] The defense's argument that the Register's analysis isn't final was seen as too extreme a statutory

170. *Id.* at 834.
171. *Id.*
172. *Id.*
173. *Id.*
174. *Id.* at 835.
175. *Id.*
176. *Id.*
177. *Id.* at 833.
178. *Id.*
179. *Id.* at 837; United States v. Freeman, 44 U.S. 556, 564 (1845).
180. *Med. Imaging*, 103 F.4th at 838.
181. *Id.* at 839.
182. *Id.*
183. *Id.*; 17 U.S.C. § 701(e).

interpretation because it could make all copyright regulations free from judicial review, as the Registers tend to just make recommendations.[184]

The Court vacated the judgment and remanded the case "to consider the merits of the APA claims in the first instance."[185]

E. ILLINOIS BIOMETRIC INFORMATION PRIVACY ACT

In August 2024, Illinois Governor Pritzker signed amendments to sections 15(b) and 15(d) of the Illinois Biometric Information Privacy Act to prohibit companies from collecting a person's biometric information multiple times in the same manner.[186] However, the Act also prohibits plaintiffs from receiving damages for each individual violation.[187] The amendments specifically came about from the dispute in *Cothron v. White Castle System, Inc.*, where the Illinois Supreme Court found that using the same collection method for biometric collection data, even multiple times, is considered multiple violations.[188]

The question certified to the court in *Cothron* was whether section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission.[189] To answer this question, the court assumed that the defendant, White Castle System, had violated the rights of the plaintiff, a manager of a White Castle restaurant in Illinois, under the Illinois Biometric Information Privacy Act.[190] The alleged violation resulted from not explicitly obtaining the Plaintiff's consent to a biometric-collection system.[191] Specifically, White Castle required its employees to scan their fingerprints to access their pay stubs and computers, leading to the cause of action.[192]

Cothron argued that the "plain meaning of the statutory language" demonstrated that claims under sections 15(b) and 15(d) accrue every time a private entity collects or disseminates biometrics without prior informed consent.[193] In particular, the plaintiff asserted that the use of the word "first"

184. *Med. Imaging*, 103 F.4th at 841.

185. *Id.* at 841–42.

186. Ian Fisher, Gillian Lindsay & Elizabeth Babbitt, *Illinois BIPA Reform Offers Welcome Relief to Businesses*, LAW360 (Aug. 12, 2024), https://www.law360.com/articles/1868530/illinois-bipa-reform-offers-welcome-relief-to-businesses.

187. *Id.*

188. Cothron v. White Castle Sys., Inc., 2023 IL 128004, at 918, 920 (Ill. 2023).

189. *Id.* at 922.

190. I*d.* at 920.

191. *Id.*

192. *Id.*

193. *Id.* at 923.

in section 15(b) modifies the words "informs" and "receives."[194] White Castle argued that the sections focused on the consent, which would only pertain to the "first instance" of disclosure or dissemination.[195]

The Illinois Supreme Court sided with Cothron, holding that the plain language of sections 15(b) and 15(d) demonstrates that violations occur with every scan or transmission, instead of just at the first instance.[196] However, the court limited the damages plaintiffs can receive to the first violation to prevent "the financial destruction of a business."[197]

In the context of the holding of Cothron, the amendments to the Illinois Biometric Information Privacy Act recognize individual privacy protection but also incorporate protections for businesses. These amendments are important because Illinois is the first state to have a biometric data privacy law. Many other states have and will continue to look to Illinois as an example of how to implement privacy laws as new developments arise to better protect their constituents' data while balancing the needs of corporations.

F. EUROPEAN UNION ARTIFICIAL INTELLIGENCE ACT

Some believe the EU's regulation of artificial intelligence at the initial level in accordance with the *precautionary principle* will prevent further development of AI systems in the EU marketplace.[198] This blurb will discuss the relevant articles of the Act in the context of the ultimate spirit of the EU legislation.

1. What AI Systems Are Prohibited?

To show that it prioritizes the safety of its own citizens, the EU has banned some AI models.[199] Some of the banned AI practices include "deploying subliminal, manipulative, or deceptive techniques to distort behavior and impair informed decision-making, causing significant harm, . . . evaluating or classifying individuals/groups based on social behavior or personal traits, causing detrimental or unfavorable treatment of those people ("social

194. *Id.*
195. *Id.*
196. *Id.* at 926.
197. *Id.* at 929.
198. *The Precautionary Principle: Definitions, Applications and Governance*, EUR. PARLIAMENT THINK TANK (Sep. 12, 2015), https://www.europarl.europa.eu/thinktank/en/document/EPRS_IDA(2015)573876.
199. *EU AI Act, Article 5: Prohibited AI Practices*, FUTURE OF LIFE INST. (Feb. 2, 2025), https://artificialintelligenceact.eu/article/5/.

scoring"), . . . and inferring emotions in workplaces or educational institutions, except for medical or safety reasons."[200]

2. Risk Categories

The AI Act mentions three categories of risks associated with AI systems: (1) unacceptable,[201] (2) high,[202] (3) limited. AI systems that compromise basic rights or safety will be categorized as high risk and fall into one of two groups: "1) AI systems that are used in products falling under the EU's product safety legislation. This includes toys, aviation, cars, medical devices and lifts,"[203] and "2) AI systems falling into specific areas that will have to be registered in an EU database, such as law enforcement, and assistance in legal interpretation and application of the law."[204]

To regulate high-risk AI systems, the AI Act determines standards such as establishing risk management systems,[205] conducting data governance,[206] record keeping,[207] human oversight,[208] and implementing cybersecurity measures throughout the lifecycle of the AI system.[209]

3. Extraterritoriality and Enforcement

Despite not being enshrined in a single article, General Protection Data Regulation-style extraterritoriality gives the AI Act worldwide impact.[210] The Act is essentially a global standard because non-EU suppliers are required to abide by the standard if their products are used inside the Union.[211] Moreover,

200. *High-Level Summary of the AI Act*, FUTURE OF LIFE INST. (Feb. 27, 2024), https://artificialintelligenceact.eu/high-level-summary/.

201. Regulation (EU) 2024/1689, of the European Parliament and of the Council of 13 June 2024 on Laying Down Harmonised Rules on Artificial Intelligence and Amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act), 2024 O.J. (L) Preamble ¶¶ 26, 31, 46, 179 [hereinafter EU AI Act]. The examples of the unacceptable risk AI models are also mentioned as prohibited AI models.

202. EU AI Act, art. 6, 2024 O.J. (L) 53–54.

203. *EU AI Act: First Regulation on Artificial Intelligence*, EUR. PARLIAMENT: TOPICS (Feb. 19, 2025), https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence#ai-act-different-rules-for-different-risk-levels-6.

204. *Id.*

205. EU AI Act, art. 9, 2024 O.J. (L) 56–57.

206. EU AI Act, art. 10, 2024 O.J. (L) 57–58.

207. EU AI Act, art. 12, 2024 O.J. (L) 59.

208. EU AI Act, art. 14, 2024 O.J. (L) 60–61.

209. EU AI Act, art. 15, 2024 O.J. (L) 61.

210. EU AI Act, art. 2, 2024 O.J. (L) 45–46; *see* General Data Protection Regulation, INTERSOFT CONSULTING, https://gdpr-info.eu/ (last visited May 14, 2025).

211. EU AI Act, art. 2, 2024 O.J. (L) 45–46.

the enforcement of the Act is based on a decentralized model: The EU AI Office[212] handles cross-border cases, while notifying authorities[213] oversee compliance.[214]

4. Sandboxes

The most innovative element of the Act, Article 57, creates pan-EU regulatory sandboxes that enable startups to trial AI systems with supervisory oversight.[215] In contrast to fintech sandboxes aimed at market entry, these prioritize ethical experimentation; participants are required to show compliance with basic rights, even though they are exempt from certain technical standards.

5. Noncompliance and Enforcement

Finally, the EU AI Act creates strict compliance standards and costly consequences for noncompliance.[216] Depending on the type of noncompliance or violation, penalties can range from EUR 7.5 million, or 1.5 percent of global annual sales, to EUR 35 million, or 7 percent of global annual turnover.[217]

G. ARTIFICIAL INTELLIGENCE, INVENTORSHIP, AND AUTHORSHIP

Over the last year, both the U.S. Patent and Trade Office (USPTO) and U.S. Copyright Office (USCO) have issued memoranda regarding the use of artificial intelligence in patented and copyrighted works in response to the growing use of artificial intelligence.

1. USPTO Guidelines on AI Inventorship

On February 13, 2024, in response to the rise of artificial intelligence (AI) aided inventions, the USPTO published guidelines on AI-related inventorship.[218] Citing *Thaler v. Vidal*, where the court held that only a natural person can be an inventor, the USPTO reiterated that AI alone does not qualify as an inventor.[219] The guidelines addressed whether inventions developed with AI assistance are eligible for patent protection when listed as joint inventors.[220]

212. EU AI Act, art. 3, 2024 O.J. (L) 46–50.
213. *Id.*
214. EU AI Act, art. 55, 2024 O.J. (L) 86.
215. EU AI Act, art. 57, 2024 O.J. (L) 88–89.
216. EU AI Act, art. 99, 2024 O.J. (L) 115–16.
217. *Id.* ¶ 3.
218. 2024 Guidance Update on Patent Subject Matter Eligibility, Including on Artificial Intelligence, 89 Fed. Reg. 58128 (Jul. 17, 2024) [hereinafter USPTO AI Guidance].
219. *Id.*; *see* Thaler v. Vidal, 43 F.4th 1207, 1213 (Fed. Cir. 2022).
220. *See generally* USPTO AI Guidance.

The USPTO stated that if one or more natural—meaning human—persons "significantly contributed" to the invention, the invention can be patentable, even if AI was instrumental in the creation of such, with one caveat.[221] A human must have contributed significantly to every claim on the patent.[222]

The USPTO guidelines established several specific criteria: (1) Recognizing a problem and having a general goal or research plan is not sufficient conception; not a significant contribution.[223] However, if prompting particularly for a specific solution for a specific problem, it may be considered more significant.[224] (2) Appreciating an inventive property of an AI output is not as significant if it is apparent to a person having ordinary skill in the art (PHOSITA).[225] However, if one applies the output to significantly contribute to an invention, it may be proper.[226] (3) While merely overseeing the AI system is not an invention, if the AI system is built, designed, or trained in view of a specific problem and solution, it could be considered a significant contribution.[227]

2. USCO Guidelines on AI Authorship

Similarly to USPTO, the United States Copyright Office (USCO) issued guidance on AI-generated material reiterating the human authorship requirement.[228] The USCO cites both *Thaler v. Perlmutter*, as well as the 1973 Compendium of Copyright Office Practices, both of which indicate that the term "author" excludes nonhumans.[229] Consequently, a work produced solely by AI cannot be copyrighted.[230]

The USCO also states that if the work's traditional elements were produced by machine, it lacks human authorship; if the machine determines how instructions are carried out, it would not be protected.[231] However, if a work has sufficient human authorship, only the human authored aspects,

221. *Id.*
222. *Id.*
223. *Id.*
224. *Id.*
225. *Id.*
226. *Id.*
227. *Id.*
228. Copyright Registration Guidance: Works Containing Material Generated by Artificial Intelligence, 88 Fed. Reg. 16190–94 (Mar. 16, 2023) (to be codified at 37 C.F.R. pt. 202).
229. *Id.* (citing Thaler v. Perlmutter, No. 1:22-cv-01564 (D.D.C.), currently Thaler v. Perlmutter, 130 F.4th 1039 (D.D.C. 2025)).
230. *Id.*
231. *Id.*

independent of the whole work, are protected and the AI-generated material itself is still unprotected.[232]

The USCO recommends that for submitting registration, indicate which parts of works are created by the author and which are generated by AI, without necessarily specifying the particular AI program used.[233]

3. Conclusion

Taken together, the general trend in AI and its usage-legality seems positive based on form; as long as there is some significant contribution or at least human authorship in the work's traditional elements, AI usage has potential pathways to be protected works of both inventors and artists in the near future.

4. Doe v. Github

Here, various software developers who submitted their code to GitHub publicly sued GitHub and OpenAI regarding the development of Codex and Copilot programs, alleging breaches of contract, fraud, torts, and statutory violations.[234] Codex and Copilot programs were developed by OpenAI using machine learning from data scraped from various public sites, including GitHub, to come up with the best code solution to a prompted problem.[235] However, when producing the solution, the resulting output misattributed copyrights, notices, and license terms, violating the open-source licenses of possibly millions of software developers who have published their code on GitHub.[236]

As for claims of privacy and property right violations, the court held that while the alleged harms were not particularized enough to the plaintiffs to award the plaintiffs' damages, they still have standing to pursue injunctive relief.[237] For many allegations, the court granted leave to amend due to insufficient specific facts in the pleadings, while dismissing claims for civil conspiracy and declaratory relief as they were not independent causes of action.[238]

While inconclusive at this time, this case represents an important overarching problem in the development of AI: When data is trained upon licensed data, what is to be made of the licenses and their subsequent violations? How do we legally gather and train data?

232. *Id.*
233. *Id.*
234. Doe 1 v. GitHub, Inc., 672 F. Supp. 3d 837, 847 (N.D. Cal. 2023).
235. *Id.* at 845.
236. *Id.* at 846.
237. *Id.* at 850.
238. *Id.* at 861–62.

V. ANTITRUST DEVELOPMENTS

A. EPIC GAMES INC. V. APPLE, INC.

The dispute in *Epic Games Inc. v. Apple, Inc.* focused on whether Apple's App Store policies violated federal antitrust laws under the Sherman Act and California's Unfair Competition Law.[239] Epic Games brought legal action against Apple in 2020 after Apple removed Fortnite from the App Store as a response to Epic's attempt to bypass Apple's in-app purchase system and its 30 percent commission.[240]

Epic Games Inc. v. Apple, Inc. was initially heard in the District Court for the Northern District of California, which ruled in favor of Epic Games on one count, finding that Apple violated California's Unfair Competition Law, but ruled in favor of Apple on all other counts.[241] The Ninth Circuit affirmed the district court's conclusion that Apple's App Store anti-steering rules violated California's Unfair Competition Law and upheld the nationwide injunction against those rules.[242]

However, the district court rejected Epic's Sherman Act claim, acknowledging that although Apple has significant market power, it did not achieve or maintain it through anticompetitive conduct.[243] The court acknowledged that Apple did not create a completely open ecosystem where developers and users could "transact freely without any mediation."[244] However, the Ninth Circuit affirmed the district court's denial of antitrust liability alleging that Epic Games failed to establish a market definition of how Apple violated the Sherman Act.[245]

The Ninth Circuit also concluded that Epic Games failed to meet its burden under the "rule of reason" framework required in antitrust claims.[246] The court found that although Apple's restrictions on app distribution and in-app purchases limited competition, Epic did not provide sufficient evidence that these limitations were unreasonable when weighed against Apple's justifications related to security, privacy, and payment processing.[247] The Ninth

239. Epic Games, Inc. v. Apple, Inc., 67 F.4th 946, 966 (9th Cir. 2023).
240. *Id.* at 966–67.
241. *Id.* at 966.
242. *Id.*
243. *Id.* at 972.
244. *Id.* at 967.
245. *Id.* at 970–71.
246. *Id.* at 966.
247. *Id.* at 996.

Circuit ultimately concluded by emphasizing that they are not able to resolve the relationship between online transaction platforms with market power.[248]

The Ninth Circuit's decision reinforced the narrow path for successful antitrust claims in digital platform markets, while still recognizing the importance of consumer choice and fair business practices under state law. Although Epic failed to dismantle Apple's App Store model entirely, questions about the scope of platform power, the role of privacy and security justifications, and how future cases might challenge similar ecosystems under both federal and state law remain.

B. UNITED STATES V. GOOGLE, LLC

The U.S. District Court for the District of Columbia held that Google LLC violated § 2 of the Sherman Act by illegally maintaining a monopoly over general search services and general search text ads.[249]

Section 2 of the Sherman Act makes it a crime for a person to "monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of the trade or commerce among the several States, or with foreign nations."[250] Violation of § 2 can result in fines up to $100 million for corporations or fines up to $1 million or imprisonment not exceeding ten years for any other person.[251]

In October 2020, the DOJ and attorneys general of eleven states sued Google for § 2 illegal monopolization violations of the Sherman Act.[252] The plaintiffs alleged that Google formed exclusive agreements in order to secure the default distribution of its search and advertising services to maintain monopolies in three online markets.[253] In December 2020, thirty-eight other states sued Google for violations of the Clayton Act.[254]

Google took some anticompetitive steps, such as acquiring competitors, forcing adoption of Google's tools, distorting auction competition, and auction manipulation.[255] Therefore, Judge Mehta found Google in violation of § 2 and stated the following relevant reasons for the judgment:

248. *Id.* at 1004.
249. United States v. Google LLC, 747 F. Supp. 3d 1, 187 (D.D.C. 2024).
250. 15 U.S.C. § 2 (2018).
251. *Id.*
252. *Google*, 747 F. Supp. 3d at 33.
253. *Id.*
254. *Id.*
255. Press Release, *Justice Department Sues Google for Monopolizing Digital Advertising Technologies*, U.S. DEP'T OF JUST. (Jan. 24, 2023), https://www.justice.gov/archives/opa/pr/justice-department-sues-google-monopolizing-digital-advertising-technologies.

- There are relevant product markets for general search services and general search text ads;
- Google has monopoly power in (a) general search services and (b) general search text ads markets; and
- Google's distribution agreements are exclusive and have anticompetitive effects.[256]

Google did not offer valid pro-competitive justifications for those agreements.[257]

256. *See generally Google*, 747 F. Supp. 3d.
257. *Id.* at 171.