SURVEY OF ADDITIONAL IP AND TECHNOLOGY LAW DEVELOPMENTS

I. PATENT DEVELOPMENTS

A. HELSINN HEALTHCARE S.A. V. TEVA PHARMS. USA, INC., 855 F.3D 1356 (FED. CIR. 2017)

The United States Court of Appeals for the Federal Circuit held (1) that the asserted claims of the patents-in-suit were subject to an invalidating contract for sale prior to the critical date, (2) that the Leahy-Smith America Invents Act (AIA) did not change the statutory meaning of "on-sale" of the on-sale bar provision of 35 U.S.C. § 102 of the Patent Act, and (3) that public disclosure of the existence of the sale of a patented item may suffice to invalidate a patent under the on-sale bar, even if "the details of the invention" are not "publicly disclosed in the terms of sale."[1]

In 2011, Teva Pharmaceuticals USA, Inc. and Teva Pharmaceutical Industries, Ltd. (collectively, "Teva") filed an Abbreviated New Drug Application (ANDA) seeking FDA approval to market a generic 0.25 mg palonosetron product. Teva's ANDA filing included a Paragraph IV certification that the claims of the patents-in-suit were invalid and/or not infringed. Helsinn Healthcare S.A. ("Helsinn") then brought suit under the Hatch-Waxman Act, 35 U.S.C. § 271(e)(2)(A), alleging infringement of the patents-in-suit by the ANDA filing. The four patents-in-suit are directed to intravenous formulations of palonosetron for reducing or reducing the likelihood of chemotherapy-induced nausea and vomiting (CINV), a serious side effect of chemotherapy treatment.[2]

At trial, Teva argued, *inter alia*, that the asserted claims were invalid under the on-sale bar provision of 35 U.S.C. § 102.[3] The district court found that the patents-in-suit were not invalid.[4] With respect to three of the patents, which are governed by the pre-AIA version of § 102, the district court concluded that there was a commercial offer for sale before the critical date, but that the

DOI: https://doi.org/10.15779/Z38QB9V571

1. Helsinn Healthcare S.A. v. Teva Pharms. USA, Inc., 855 F.3d 1356, 1360, 1375 (Fed. Cir. 2017).
2. *Id.* at 1360, 1363.
3. *Id.* at 1360.
4. *Id.*

invention was not ready for patenting before the critical date.[5] With respect to the fourth patent, which is governed by the AIA version of § 102, the district court concluded that there was no commercial offer for sale because the AIA changed the relevant standard and that the invention was not ready for patenting before the critical date.[6] The district court found that the patents-in-suit were not invalid.[7]

The Federal Circuit decided that the asserted claims of the patents-in-suit were subject to an invalidating contract for sale prior to the critical date, and that the AIA did not change the statutory meaning of "on sale" in the circumstances involved.[8] The asserted claims were also ready for patenting prior to the critical date.[9] The district court's decision was reversed.[10]

The court first addressed the three pre-AIA patents and whether the inventions were subject to a sale or offer for sale prior to the critical date. The court explained that the question must be "analyzed under the law of contracts as generally understood" and "must focus on those activities that would be understood to be commercial sales and offers for sale 'in the commercial community.' "[11] A sale occurs when there is a "contract between parties to give and to pass rights of property for consideration which the buyer pays or promises to pay the seller for the thing bought or sold."[12]

The court noted that while certain details were redacted from the publicly disclosed copy of the Supply and Purchase Agreement, Helsinn commercially marketed its invention before the critical date.[13] It publicly sought "marketing partners for its patented [palonosetron] product," and ultimately contracted with MGI "to distribute, promote, market, and sell" the claimed invention.[14] The absence of FDA or other regulatory approval before the critical date does not prevent a sale or offer for sale from triggering the on-sale bar.[15] The court found that the Supply and Purchase Agreement constituted a commercial sale or offer for sale for purposes of § 102(b) as to the three pre-AIA patents.[16]

---

5. *Id.*
6. *Id.*
7. Helsinn Healthcare S.A. v. Teva Pharms. USA, Inc., 855 F.3d 1356, 1360 (Fed. Cir. 2017).
8. *Id.*
9. *Id.*
10. *Id.*
11. *Id.* at 1364.
12. *Id.* (citing Trading Techs. Int'l, Inc. v. eSpeed, Inc., 595 F.3d 1340, 1361 (Fed. Cir. 2010)) (internal quotation marks omitted).
13. Helsinn Healthcare S.A. v. Teva Pharms. USA, Inc., 855 F.3d 1356, 1364 (Fed. Cir. 2017).
14. *Id.*
15. *Id.* at 1365.
16. *Id.* at 1367.

Turning to the post-AIA patent. The AIA changed the on-sale bar provision by adding "the otherwise available to the public" phrase.[17] In congressional floor statements, it was mentioned that due to the change of language, the on-sale bar now does not encompass secret sales and requires that a sale make the invention available to the public in order to trigger application of the on-sale bar.[18] However, the Federal Circuit deemed congressional floor statements to be at most intent to overrule precedent involving a public use where the invention was not, as a result of the use, disclosed to the public.[19] According to the court, if Congress had intended to work such a sweeping change to on-sale jurisprudence, it would have done so by clear language.[20] Accordingly, after the AIA, "if the existence of the sale is public, the details of the invention need not be publicly disclosed in the terms of the sale."[21]

The court also noted that the invention would work for its intended purpose and was ready for patenting because it was reduced to practice before the critical date.[22] The district court had erred by applying a more rigorous standard that governs FDA approval of new drugs, including the various stages of clinical trials.[23]

Regarding the three pre-AIA patents in suit, the court concluded that the supply and purchase agreement, which obligated purchaser to buy owner's claimed invention once the solution was approved by FDA, constituted a "sale" of the claimed invention prior to critical date, as required for pre-AIA on-sale bar to patentability to apply.[24] Regarding the fourth post-AIA patent in suit, the court concluded that the supply and purchase agreement constituted a "sale" of the claimed invention prior to critical date, as required for AIA on-sale bar to patentability to apply.[25] The court also noted that the claimed invention was "reduced to practice" before the critical date, and thus was ready for patenting, as required for the on-sale bar to patentability to apply.[26]

Therefore, the court found the three pre-AIA patents and the post-AIA

17. *Id.* at 1368.
18. *Id.*
19. Helsinn Healthcare S.A. v. Teva Pharms. USA, Inc., 855 F.3d 1356, 1368–69 (Fed. Cir. 2017).
20. *Id.* at 1371.
21. *Id.*
22. *Id.* at 1373.
23. *Id.*
24. *Id.* at 1367.
25. Helsinn Healthcare S.A. v. Teva Pharms. USA, Inc., 855 F.3d 1356, 1371 (Fed. Cir. 2017).
26. *Id.* at 1375.

patent of Helsinn invalid.[27]

B. GOOGLE LLC V. NETWORK-1 TECHS. INC., 709 F. APP'X 705 (FED. CIR. 2018)

In a closely-watched case, the Federal Circuit affirmed the Patent Trial and Appeal Board's (PTAB) decision that Network-1 Technologies' patent for a method of identifying online media was valid.[28] The dispute attracted industry attention because it implicated a technology giant's profitable code.[29]

In 2013, Network-1 received Patent No. 8904464 for a "Method for Tagging an Electronic Media Work to Perform an Action."[30] The '464 Patent covers a method for identifying media linked over the Internet.[31] It is commercially valuable because it can support e-commerce or audience engagement without increasing hardware demands on computer systems, thus lowering the user's operating costs.[32]

Shortly thereafter, Network-1 sued Google and its subsidiary YouTube in the United States District Court for the Southern District of New York, claiming that YouTube's Content ID system infringed upon the '464 Patent.[33] YouTube's Content ID system compares uploaded videos in its media library in order to identify potential copyright infringement.[34] The Content ID system was allegedly generating significant revenue for YouTube.[35] Google responded to Network-1's infringement suit by attacking the validity of the '464 Patent as obvious and indefinite.[36] Google went on with the offensiveness and petitioned the PTAB for a covered business method (CBM) review of the contested patent, seeking to invalidate it.[37] In its petition, Google attacked the validity of all claims of the '464 Patent for violating 35 U.S.C. § 103 by being

27. *Id.*

28. Google LLC v. Network-1 Techs., 709 F. App'x 705, 705 (Fed. Cir. 2018).

29. Steve Brachmann, *Google Suffers IPR Defeat on Patent Asserted Against YouTube by Network-1*, IPWATCHDOG (Jan. 30, 2018), http://www.ipwatchdog.com/2018/01/30/google-ipr-defeat-youtube-network-1/id=92866/ [https://perma.cc/J4XH-XMJW].

30. U.S. Patent App. No. 8,904,464 (issued Dec. 2, 2014).

31. *Id.*

32. *Id.*

33. Brief for Appellant, Google LLC v. Network-1 Techs., No. 17-1379, 2017 WL 1520288, at *4 (Fed. Cir. Apr. 14, 2017) [hereinafter Brief for Appellant].

34. *How Content ID Works*, GOOGLE (Mar. 18, 2018), https://support.google.com/youtube/answer/2797370?hl=en [https://perma.cc/CDL8-98TF]

35. Complaint Against Google, at ¶ 23, Google LLC v. Network-1 Techs., No. 17-1379, 709 F. App'x 705 (Fed. Cir. 2018).

36. Answer by Google, at ¶ 37, Google LLC v. Network-1 Techs., No. 17-1379, 709 F. App'x 705 (Fed. Cir. 2018).

37. Google LLC v. Network-1 Techs., CBM2015-00113, 2016 Pat. App. LEXIS 13333 (P.T.A.B. October 18, 2016).

obvious.[38]

But Google's arguments proved unsuccessful.[39] The PTAB entered a final decision in the CBM review that the '464 Patent was nonobvious and that it was not anticipated by prior technology.[40] The PTAB found that Google failed to prove that any of the '464 Patent's claims were unpatentable for obviousness, specifically focusing on the meaning of "machine-readable instructions" in claims 1 and 18.[41] While Google argued for a broader understanding of the phrase as one referring to instructions that could be read by either a human or a computer, pointing to a Network-1 expert's testimony stating that changing computer code could change the message read by humans, the PTAB accepted Network-1's narrower construction to understand the phrase as referring to instructions that *must* be readable by machine.[42] By construing the pivotal term "machine-readable instructions" in a narrow fashion, the PTAB found that the '464 Patent was nonobvious and thus valid.

Having lost at the PTAB, Google appealed to the Federal Circuit on the grounds that the PTAB erred in its construction of the term "machine-readable instructions."[43] Google primarily argued that because subsequent dependent claims state that "machine-readable instructions comprise a hyperlink or URL," and there is no submitted evidence showing that hyperlinks or URLs are readable exclusively by machines, that the PTAB's construction was incorrect.[44] Network-1 defended the PTAB's construction by arguing that (1) these dependent claims are not contradictory to a narrow understanding of "machine-readable instructions" because this term of art is supported by expert testimony and objective sources; (2) Google was attempting to re-litigate facts; and (3) Google was asserting a baseless new theory.[45]

The Federal Circuit affirmed the PTAB's decision in a short, non-precedential opinion in January 2018.[46] Specifically, the court held that PTAB's narrow construction of "machine-readable instructions" was correct and that Google failed to produce sufficient evidence establishing obviousness.[47] The

38. *Id.*
39. *Id.*
40. *Id.*
41. *Id.*
42. *Id.*
43. Google LLC v. Network-1 Techs., 709 F. App'x 705, 705 (Fed. Cir. 2018).
44. Brief for Appellant, *supra* note 33.
45. Brief for Appellee, Google LLC v. Network-1 Techs., No. 17-1379, 2017 WL 2801084, at *13–18 (Fed. Cir. June 16, 2017).
46. *Network-1*, 709 F. App'x at 705.
47. *Id.*

court found "no error" in the PTAB's construction of "machine-readable instructions" because of the substantial supporting evidence in the record, including Google's own explicit assertions in its Petition.[48] Network-1's patent infringement suit against Google and YouTube can now proceed.[49]

C. LIFETIME INDUS., INC. V. TRIM-LOK, INC., 869 F.3D 1372 (FED. CIR. 2017)

The United States Court of Appeals for the Federal Circuit held that a patent infringement complaint meeting the pleading standard set in *Ashcroft v. Iqbal*, 129 S. Ct. 1937 (2009), and *Bell Atl. Corp. v. Twombly*, 127 S. Ct. 1955 (2007), was enough to survive a motion to dismiss within the meaning of Federal Rule of Civil Procedure 12(b)(6).[50] The Court found that the plaintiff adequately pleaded direct and indirect infringement by specifying where the alleged infringement occurred, when it occurred, who performed the allegedly infringing act, and why.[51]

On August 12, 2013, Lifetime Industries, Inc. ("Lifetime") brought an action against Trim-Lok, Inc. ("Trim-Lok"), alleging that Trim-Lok both directly and indirectly infringed U.S. Patent 6,966,590 ("the '590 patent") under 35 U.S.C. § 271 of the Patent Act.[52] The '590 patent describes a two-part seal for use in a mobile living quarter (a "recreational vehicle") with a slide-out room which is formed by extending a portion of the side wall of the RV outwards to create extra interior space.[53]

Lifetime argued that in the months before it filed the original complaint, two of its engineers, who participated in the design of Lifetime's seals and who had knowledge of the '590 patent, left Lifetime and began working at Trim-Lok.[54] Lifetime alleged that Trim-Lok was offering for sale a two-part seal for an RV with a slide-out room, soon after the two engineers began working.[55] Lifetime further alleged that they discovered a two-part Trim-Lok seal installed on an RV with a slide-out room at a plant run by Forest River, an RV manufacturer.[56]

Accordingly, Lifetime alleged that since Trim-Lok visited the Forest River plant while "acting on behalf of" Trim-Lok, and directly installed Trim-Lok's

48. *Id.*
49. Network-1 Techs., Inc. v. Google Inc., Case No. 1:14-cv-09558 (S.D.N.Y. Dec. 3, 2014).
50. Lifetime Indus., Inc. v. Trim-Lok, Inc., 869 F.3d 1372, 1376–77 (Fed. Cir. 2017).
51. *Id.* at 1379, 1381.
52. *Id.* at 1375, 1381.
53. *Id.* at 1373–74.
54. *Id.* at 1375.
55. *Id.*
56. Lifetime Indus., Inc. v. Trim-Lok, Inc., 869 F.3d 1372, 1375 (Fed. Cir. 2017).

two-part seal onto an RV having a slide-out room, there was direct infringement of the '590 patent.[57]

For induced infringement, Lifetime alleged that Forest River's "making . . . and selling of an RV having the two-part seal constitutes infringement," and that Trim-Lok "influenced Forest River" to include the seal in their RVs, "knowing that such combination would fulfill all elements of at least one claim of the '590 patent" and that "[Trim-Lok] assisted in the installation, [or] directed the installation" of the seals.[58] Thus, Lifetime alleged that Trim-Lok induced Forest River to infringe.[59]

For contributory infringement, Lifetime alleged that the seal sold by Trim-Lok had only one purpose (use on RVs with slide-out rooms), that Trim-Lok assisted in or directed the installation of the seal on an RV, and that the seals were not staple articles of commerce suitable for non-infringing use.[60]

Trim-Lok moved to dismiss the complaint, arguing that Lifetime had not adequately identified the accused product and had not adequately pleaded direct or indirect infringement.[61] Although the district court determined that Lifetime had adequately identified the accused product, it concluded that Lifetime had not adequately pleaded its case.[62]

The court determined that, Lifetime did not adequately plead direct infringement because Trim-Lok only manufactures the two-part seals without the RV.[63] The court determined that Lifetime's argument of Trim-Lok's assistance in installation of the seal was confusing liability for direct infringement with liability for contributory infringement, and dismissed Lifetime's direct infringement allegations.[64] Regarding indirect infringement, the court concluded that Lifetime had not alleged any facts from which intent to infringe could be inferred in this case, and accordingly dismissed Lifetime's indirect infringement allegations.[65]

In determining the standard to survive a motion to dismiss under Rule 12(b)(6), the Federal Circuit concluded that a complaint must "contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' "[66] A plaintiff meets this requirement if it "pleads factual

57. *Id.*
58. *Id.*
59. *Id.*
60. *Id.*
61. *Id.* at 1375–76.
62. Lifetime Indus., Inc. v. Trim-Lok, Inc., 869 F.3d 1372, 1376 (Fed. Cir. 2017).
63. *Id.*
64. *Id.*
65. *Id.*
66. *Id.* (citing Ashcroft v. Iqbal, 129 S. Ct. 1937 (2009); Bell Atl. Corp. v. Twombly, 127 S. Ct. 1955 (2007)).

content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged."[67]

Further, the court noted that direct infringement is a strict liability offense that does not require knowledge of the patent or intent to infringe.[68] The court also noted that "one who 'makes' a patented invention without authorization infringes the patent."[69] That is, limited internal manufacture and use can also infringe.[70]

Since Lifetime adequately alleged that Trim-Lok created an infringing combination by installing its seal onto an RV at the Forest River plant, these facts draw reasonable inferences in Lifetime's favor, making it plausible that a Trim-Lok agent installed the seal onto the Forest River RV.[71] The court concluded that Lifetime adequately alleged direct infringement.[72]

The court noted that for an allegation of induced infringement to survive a motion to dismiss, a complaint must plead facts plausibly showing that the accused infringer "specifically intended [another party] to infringe [the patent] and knew that the [other party]'s acts constituted infringement."[73] The court concluded that since Lifetime specifically alleged that two engineers had knowledge of the patent and its scope when they joined Trim-Lok, these facts make it plausible that Trim-Lok had knowledge of the '590 patent.[74] After Trim-Lok gained that knowledge, Lifetime alleged that it then assisted in or directed the installation of exactly the same type of seal as the one described in the patent onto an RV at the Forest River plant.[75] Thus, Lifetime plausibly pleaded that Trim-Lok had the intent to infringe.[76]

The Court then noted that contributory infringement occurs, *inter alia*, when a party sells in a manner set forth in 35 U.S.C. § 271(c).[77] Further, contributory infringement requires "only proof of a defendant's knowledge, not intent, that his activity cause infringement."[78] Because it is reasonable to

67. *Id.*

68. Lifetime Indus., Inc. v. Trim-Lok, Inc., 869 F.3d 1372, 1376 (Fed. Cir. 2017) (citing Commil USA, LLC v. Cisco Sys., Inc., 135 S. Ct. 1920, 1926 (2015)).

69. *Id.* at 1378 (citing Siemens Med. Sols. USA, Inc. v. Saint-Gobain Ceramics & Plastics, Inc., 637 F.3d 1269, 1290 (Fed. Cir. 2011)).

70. *Id.*

71. *Id.* at 1379.

72. *Id.*

73. *Id.* (citing R+L Carriers, Inc. v. DriverTech LLC (*In re* Bill of Lading Transmission & Processing Sys. Patent Litig.), 681 F.3d 1323, 1339 (Fed. Cir. 2012)).

74. Lifetime Indus., Inc. v. Trim-Lok, Inc., 869 F.3d 1372, 1380 (Fed. Cir. 2017).

75. *Id.*

76. *Id.*

77. *Id.* at 1381.

78. *Id.* (citing Hewlett-Packard Co. v. Bausch & Lomb Inc., 909 F.2d 1464, 1469 (Fed. Cir. 1990)).

infer that Lifetime plausibly pleaded that Trim-Lok knew of the patent and knew of infringement,[79] the Federal Circuit concluded that Lifetime has adequately pleaded both direct and indirect infringement.[80]

II. COPYRIGHT DEVELOPMENTS

A. BMG RIGHTS MGMT. V. COX COMMC'NS, INC., 881 F.3D 293 (4TH CIR. 2018)

The United States Court of Appeals for the Fourth Circuit held that an Internet Service Provider (ISP) cannot claim protection under the Digital Millennium Copyright Act (DMCA) safe harbors if it does not enforce its policies against repeat infringers in a meaningful way.[81] Such infringement need not be an adjudicated infringement and the ISP cannot willfully blind itself to the knowledge of infringement by its users.[82]

BMG Rights Management v. Cox Communications, Inc. is largely guided by the principle that in order to avail DMCA safe harbor protection, an ISP needs to implement its repeat infringer policy that provides for termination of services for subscribers who are repeat infringers in a "meaningful and consistent way."[83] The court rejected the argument that "infringer" under the DMCA refers to an "adjudicated infringer."[84] The court reasoned that the Copyright Act uses the term "infringer" to mean those who engage in infringing activity and is not limited to a narrow category of adjudicated infringers.[85] The court further referred to § 501(a) of the Copyright Act, which states that "anyone who violates any of the exclusive rights of the copyright owner" provided for in the statute "is an infringer of the copyright or right of the author," which implies that the term infringer is not restricted to adjudicated infringers.[86]

The plaintiff in the case, BMG Rights Management LLC (BMG) is a copyright holder in several musical compositions and the defendant, Cox Communications, is an ISP. Some of Cox's users shared and received copyrighted music files using a peer to peer file sharing mechanism called BitTorrent.[87] Cox's agreement with its subscribers stipulated a thirteen-strike policy for suspension and termination of user accounts as a deterrent to

79. *Id.*
80. Lifetime Indus., Inc. v. Trim-Lok, Inc., 869 F.3d 1372, 1381 (Fed. Cir. 2017).
81. BMG Rights Mgmt. v. Cox Commc'ns, Inc., 881 F.3d 293, 300 (4th Cir. 2018).
82. *Id.*
83. *Id.*
84. *Id.* at 303.
85. *Id.* at 301.
86. *Id.* at 301, 302 (citing 17 U.S.C. § 501(a) (2012)) (emphasis added).
87. BMG Rights Mgmt. v. Cox Commc'ns, Inc., 881 F.3d 293, 299 (4th Cir. 2018).

copyright infringement.[88] Cox had an automated system to process notifications from copyright owners alleging infringement.[89] The response to such activities was dependent on the number of acts of infringement alleged against a user and it ranged from sending warning e-mails to suspension of the account and consideration for termination.[90]

BMG, in order to address infringement of its rights, hired a third-party company, Rightscorp, Inc., to monitor BitTorrent activity and share infringement notices with Cox.[91] These notices, *inter alia*, contained information about the title of the copyrighted work, its owner, the infringer's IP address, and a settlement offer for the infringer.[92] Cox, upon receiving such notices notified Rightscorp that it would forward these notices to its users only if Rightscorp removed the settlement language from the notices.[93] Rightscorp refused to do so and Cox subsequently blacklisted Rightscorp and deleted all its notices without viewing or acting on them.[94] BMG subsequently brought an action alleging vicarious and contributory infringement against Cox.[95]

The United States District Court for the Eastern District of Virginia granted judgment against Cox after a jury found it liable for willful contributory infringement. The district court held that Cox was unable to produce evidence that its repeat infringer policy entitled it to a statutory safe harbor defense under the DMCA.[96] The court reasoned that BMG offered evidence that Cox knew that certain subscribers were using their accounts "repeatedly for infringing activity yet failed to terminate those accounts."[97] The district court instructed the jury that in order to prove contributory infringement, BMG had to show direct infringement by Cox's subscribers, that BMG "knew or should have known of such infringing activity" and that "Cox induced, caused, or materially contributed to such infringing activity."[98] It further instructed that such knowledge of the infringing activity could be proven by demonstrating willful blindness, that is, Cox "was aware of a high probability that [its] users were infringing BMG's copyrights but consciously avoided confirming that fact."[99]

88. *Id.*
89. *Id.*
90. *Id.*
91. *Id.*
92. *Id.* at 300.
93. BMG Rights Mgmt. v. Cox Commc'ns, Inc., 881 F.3d 293, 300 (4th Cir. 2018).
94. *Id.*
95. *Id.*
96. *Id.*
97. *Id.*
98. *Id.*
99. BMG Rights Mgmt. v. Cox Commc'ns, Inc., 881 F.3d 293, 300 (4th Cir. 2018).

In order to assess the district court's action, the court of appeals examined the meaning of the term "repeat infringer" under the DMCA, if Cox had actual knowledge of infringement activity by its users, and whether the district court erred in giving instructions to the jury. The court stated that the term infringer did not mean adjudicated infringer since Congress had referred to adjudicated infringers specifically in other parts of the Act.[100] It looked at legislative history, which indicated that Congress intended to punish those who abuse Internet access by disrespecting intellectual property of others with a "realistic threat of losing" their Internet access.[101] This wasn't restricted to deterring adjudicated infringers only.[102] The court also referred to *EMI Christian Music Grp., Inc. v. MP3tunes, LLC*, which defined repeat infringer to mean "someone who interferes with one of the exclusive rights of a copyright" "again or repeatedly."[103]

While assessing whether Cox had actual knowledge of infringement, it found that internal communications indicated that Cox did not terminate subscribers that its employees regarded as repeat infringers.[104] Cox always reactivated the accounts of its customers after termination regardless of its knowledge of actual infringement; its termination policy was merely a "symbolic gesture" to avail protection under the DMCA.[105] According to the court, their decision to disregard Rightscorp's notices indicated that it did not reasonably implement its policy.[106]

Cox argued that the instructions given to the jury were erroneous; according to Cox, the jury should have been instructed that it could not be liable for contributory infringement if its technology could be employed for substantial non-infringing use.[107] The court rejected this argument.[108] However, it agreed with Cox on the jury instructions related to the intent necessary to prove contributory infringement.[109] The district court had instructed the jury that it could impose liability if Cox "knew or should have known" of the infringing activity.[110] The court relied on *Metro-Goldwyn-Mayer*

100. *Id.* at 303.

101. *Id.* at 302 (citing H.R. REP. NO. 105-551, pt. 2, at 61 (1998); S. REP. NO. 105-190, at 52 (1998)).

102. *Id.*

103. *Id.* (citing EMI Christian Music Grp., Inc. v. MP3tunes, LLC, 844 F.3d 79, 89 (2d Cir. 2016)).

104. *Id.* at 303.

105. BMG Rights Mgmt. v. Cox Commc'ns, Inc., 881 F.3d 293, 303, 304 (4th Cir. 2018).

106. *Id.* at 304.

107. *Id.* at 305.

108. *Id.* at 305.

109. *Id.* at 307.

110. *Id.*

Studios, Inc. v. Grokster Ltd., which stated that "one infringes contributorily by *intentionally* inducing or encouraging direct infringement."[111] The formulation "should have known" reflected negligence.[112] Therefore, the court stated that Cox could be held liable for contributory infringement if there was willful blindness, not merely negligence.[113] The instruction given to the jury that Cox "should have known" was erroneous and too low a standard.[114] Cox also contended that the aforementioned jury instructions sought to make it liable for generalized knowledge of infringing activity, which according to Cox was not sufficient to establish liability.[115] The court agreed that an intent to cause infringement could only be established with specific knowledge of infringement or due to willful blindness to such instances of infringement.[116] Although, the court agreed with Cox that the district court erred in granting certain instructions, it rejected the argument that Cox was entitled to judgment as a matter of law.[117]

The court, therefore, affirmed the grant of summary judgment to BMG on the DMCA safe harbor defense.[118] It further reversed in part, vacated in part, and remanded for a new trial due to errors in jury instructions.[119]

Although many believe that this decision does not have any dramatic implications in terms of DMCA safe harbor provisions, Mitch Stoltz, a senior staff attorney with the Electronic Frontier Foundation, has expressed concerns that it will further encourage ISPs to act in an overly cautious manner and act on unverified complaints and accusations against their users.[120] He points out that Cox, in not forwarding Rightscorp's money demands to its customers, had reasonably stood by its customers.[121] Stoltz argues that the courts should treat secondary liability doctrines more thoughtfully considering the impact they have on the design of Internet services and ability of users to interact with

111. BMG Rights Mgmt. v. Cox Commc'ns, Inc., 881 F.3d 293, 307 (4th Cir. 2018) (citing Metro-Goldwyn-Mayer Studios, Inc. v. Grokster Ltd., 380 F.3d 1154, 1162 (9th Cir. 2004) (emphasis added)).

112. *Id.* at 308.

113. *Id.* at 309.

114. *Id.* at 310.

115. *Id.* at 311.

116. *Id.*

117. BMG Rights Mgmt. v. Cox Commc'ns, Inc., 881 F.3d 293, 312 (4th Cir. 2018)

118. *Id.* at 314.

119. *Id.*

120. Mitch Stoltz, BMG v. Cox: *ISPs Can Make Their Own Repeat-Infringer Policies, but the Fourth Circuit Wants A Higher "Body Count"*, ELECTRONIC FRONTIER FOUND. (Feb. 5, 2018), https://www.eff.org/deeplinks/2018/02/bmg-v-cox-isps-can-make-their-own-repeat-infringer-policies-fourth-circuit-wants [https://perma.cc/2WLU-DM74].

121. *Id.*

these services and use them.[122]

B. MALONEY V. T3 MEDIA, INC., 853 F.3D 1004 (9TH CIR. 2017)

The United States Court of Appeals for the Ninth Circuit held that college basketball players' right of publicity claim for a company's sale of their photos for personal use was preempted by the Copyright Act. Such claims are preempted because they seek "to hold a copyright holder liable for exercising his exclusive rights under the Copyright Act."[123]

This case is largely guided by the principle that a "publicity-right claim is not preempted when it targets non-consensual use of one's name or likeness on merchandise or in advertising."[124] However, if such likeness is captured in a copyrighted artistic visual work and the work itself is being distributed for personal use, a publicity-right claim is preempted for impinging on exclusive rights of the copyright holder.[125]

Plaintiffs here were former National Collegiate Athletic Association (NCAA) student athletes whose performance in a basketball game was placed in the NCAA's photo library. The NCAA owned and controlled the copyright in those photographs.[126] Subsequently, T3 Media Inc. (T3 Media) contracted with the NCAA to store, host, and license the images in the NCAA photo library.[127] T3 Media then sold non-exclusive licenses on its website, permitting consumers to download photographs from NCAA's photo library for non-commercial use.[128] Before downloading the photographs, users were required to agree to a license agreement that stipulated using a single copy of the image solely for non-commercial use.[129]

The district court held that the federal Copyright Act preempted Plaintiffs' claims, finding that the asserted rights fell under copyright and their names or likenesses could not be identified "independent of the display, reproduction, and distribution of the copyrighted material in which they are depicted."[130]

The Ninth Circuit applied a two-part test to determine when a right to publicity claim is preempted, considering first if the subject matter of State law falls within the scope of copyright, and then, if it does, whether the publicity rights under state law are equivalent to the rights granted by the Copyright

122. *Id.*
123. Maloney v. T3 Media, Inc., 853 F.3d 1004, 1020 (9th Cir. 2017).
124. *Id.* at 1013.
125. *Id.*
126. *Id.* at 1007.
127. *Id.*
128. *Id.*
129. Maloney v. T3 Media, Inc., 853 F.3d 1004, 1007 (9th Cir. 2017).
130. *Id.*

Act.[131] The court stated that the right of publicity seeks to prevent commercial exploitation of an individual's identity without that person's consent.[132] It looked to *Hilton v. Hallmark Cards*, 599 F.3d 894, 910 (9th Cir. 2009), where a central tenet of the right of publicity was preventing "merchandising [of] a celebrity's image without that person's consent."[133] The court also relied on *Toney v. L'Oreal USA, Inc.*, 406 F.3d 905, 910 (7th Cir. 2005), which held that the "basis of a right of publicity claim was whether the plaintiff endorses, or appears to endorse the product in question."[134] The Ninth Circuit found that Plaintiffs did not identify any use of their likenesses which did not relate to display, reproduction, and distribution of the copyrighted material.[135] Therefore, Plaintiffs' claims were not considered qualitatively different from claims under the Copyright Act[136] and it was held that the federal Copyright Act preempted their right to publicity claim.[137]

The decision has attracted criticism for vastly expanding the preemption defense in copyright law.[138] In particular, some have argued that establishing a "Merchandise vs. Personal Use dichotomy" can lead to confusion and uncertainty on what constitutes merchandise.[139] If Defendants delivered physical copies of photographs to its customers to be used as posters, would that be classified as merchandise? Would the distinction merely lie in physical or digital reproduction of the photograph?[140] Some further argue that the decision could potentially be read to mean that wholesalers and retailers are subject to different standards.[141] For instance, a wholesaler selling posters or photographs containing the likenesses of college athletes to retail outlets would be more vulnerable to right of publicity claims than the retailer selling it for personal use.[142] Thus, the *Maloney* court has raised more questions than it has answered regarding copyright preemption, creating uncertainty for future

131. *Id.* at 1011–18.
132. *Id.*
133. *Id.* at 1010.
134. *Id.*
135. Maloney v. T3 Media, Inc., 853 F.3d 1004, 1018 (9th Cir. 2017).
136. *Id.*
137. *Id.* at 1020.
138. Jennifer E. Rothman, *Copyright Law Blocks Student-Athlete Suit over Sale of Game Photos*, ROTHMAN'S RIGHT OF PUBLICITY ROADMAP (Apr. 5, 2017), http://www.rightofpublicityroadmap.com/news-commentary/copyright-law-blocks-student-athlete-suit-over-sale-game-photos [https://perma.cc/4SMH-K2LH].
139. Simon Frankel & Neema Sahni, *9th Circ. Ruling Generates Copyright Preemption Confusion*, LAW360 (Apr. 20, 2017), https://www.law360.com/articles/914891/9th-circ-ruling-generates-copyright-preemption-confusion [https://perma.cc/CU57-9ZQL].
140. *Id.*
141. *Id.*
142. *Id.*

decisions.

C. GOLDMAN V. BREITBART NEWS NETWORK, LLC., 2018 WL 911340 (S.D.N.Y. FEB. 15, 2018)

In *Goldman v. Breitbart News Network, LLC*, the Southern District Court of New York held that in-line linking violates a copyright holder's right of exclusive display.[143] In doing so, the court rejected the Ninth Circuit's server test, which freed websites from copyright infringement liability if the infringing content was not on their servers.[144]

On July 2, 2016, Justin Goldman, a photographer, took a well-timed photo of Tom Brady and other celebrities in the Hamptons.[145] Goldman posted the photo on his Snapchat Story, a service that publicly broadcasts the image to his followers for a limited time.[146] The photo was reproduced and distributed on several social media platforms, including Twitter, where it went viral as users posted the photo along with articles speculating that Brady was helping the Boston Celtics recruit.[147] Several news websites, including Breitbart and Vox, embedded tweets containing the photo on their websites via a process called in-line linking, whereby content is not directly copied but rather referenced via a link to the original content.[148] Goldman then brought this suit for use of his photograph without his permission.[149] Defendants filed for summary judgment.[150]

The right to exclusive display comes from § 106(5) of the Copyright Act, which specifically grants copyright holders the exclusive right to "display [their] copyrighted work publicly."[151] Defendants argued that they did not display the copyrighted photo. By embedding, they claimed that the computer code embedding Goldman's photo merely presents instructions to Twitter's server for public display, as the embedding code pulls the tweets from Twitter, never storing the photo at issue on the news site's servers.[152]

Defendant's arguments were based on the "server test," first outlined in *Perfect 10 v. Amazon.com*, an influential test regarding public display where third

143. Goldman v. Breitbart News Network, LLC., 2018 WL 911340, at *10 (S.D.N.Y. Feb. 15, 2018).
144. *Id.*
145. *Id.* at *1.
146. *Id.*
147. *Id.*
148. *Id.* at *2.
149. Goldman v. Breitbart News Network, LLC., 2018 WL 911340, at *2 (S.D.N.Y. Feb. 15, 2018).
150. *Id.* at *1.
151. 17 U.S.C. § 106(5) (2012).
152. *Goldman*, 2018 WL 911340, at *7.

party servers are present.[153] In *Perfect 10*, the Ninth Circuit explicitly rejected appellant's so-called "incorporation test," which would have held appellee liable for merely incorporating copyrighted content on its servers in favor of a server test, which held that the right of public display is only violated if the file is actually held on the alleged copyright violator's server.[154] While *Perfect 10* has never been accepted in its entirety anywhere else, the Seventh Circuit in *Flava Works, Inc. v. Gunter* explicitly accepted the server test for contributory infringement while rejecting it more generally.[155] Recent district court cases have split on whether to accept the server test.[156]

The key persuasive authority for the *Goldman* court is the Supreme Court case *American Broadcasting Cos. v. Aereo*.[157] Aereo was a then-promising startup with tens of thousands of subscribers and $97 million in funding, including from Diller IAC, that promised Internet streaming of live television.[158] Aereo assigned users an antenna in one of Aereo's warehouses which was tuned to the user's requested on-air programming, thus streaming it on the user's computer at around the same time as the live broadcast.[159] The *Aereo* Court held that, although Aereo only provided switching technology, it provided the technology that reacted to users' choices, thus enabling them to infringe.[160] In essence, the *Goldman* court noted that the *Aereo* decision implied that infringement should not hinge on the presence of a particularly clever technology undetected by end users.[161]

The *Goldman* court further noted that the Copyright Act was explicitly enacted to cover infringement by devices "now known or later developed," thus presumably including new, serverless display methods.[162] In fact, the

153. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146 (9th Cir. 2007).

154. *Id.* at 839, 844.

155. Flava Works, Inc. v. Gunter, 689 F.3d 754, 759, 761 (7th Cir. 2012).

156. *See, e.g.*, The Leader's Institute, LLC v. Jackson, 2017 WL 5629514, at *10 (N.D. Tex. Nov. 22, 2017) (rejecting the server test, stating that "framing" copyrighted content is infringement); Capitol Records, L.L.C. v. ReDigi Inc., 934 F. Supp. 2d 640, 652 (S.D.N.Y. 2013) (acknowledging the server test's existence); Live Face on Web, LLC v. Biblio Holdings LLC, 2016 WL 4766344, at *4 (S.D.N.Y. Sept. 12, 2016) (sidestepping the server test by noting that actual issue is distribution, not display right); Live Face on Web, LLC v. Smart Move Search, Inc., 2017 WL 1064664, at *4 (D.N.J. Mar. 21, 2017) (seemingly rejecting the server test on the basis that defendant's website caused copies of software to be distributed).

157. Am. Broad. Cos., Inc. v. Aereo, Inc., 134 S. Ct. 2498, 2508 (2014).

158. Emily Steel, *Aereo Concedes Defeat and Files for Bankruptcy*, N.Y. TIMES (Nov. 21, 2014), https://www.nytimes.com/2014/11/22/business/aereo-files-for-bankruptcy.html [https://perma.cc/L4AE-8GLS].

159. *Aereo*, 134 S. Ct. at 2503.

160. *Id.* at 2507.

161. Goldman v. Breitbart News Network, LLC., 2018 WL 911340, at *9 (S.D.N.Y. Feb. 15, 2018).

162. *Id.* at *3 (citation omitted).

Copyright Act "contemplates infringers who would not be in possession of copies" of copyrighted material, meaning that the server test doesn't even fit into the intellectual framework of the Copyright Act.[163]

The court found that the facts supported an infringement ruling once it rejected the server test.[164] Unlike in *Perfect 10*, Defendants were not passive search engines but destination websites intentionally embedding the tweets to attract traffic and displaying the tweets without any further user intervention.[165] Furthermore, Defendants made an explicit embedding choice, which even the dissent in *Aereo* admitted might lead to liability.[166]

If Defendants appeal, they may create a circuit split, thus inviting Supreme Court's guidance. The Second Circuit has issued decisions that cut in favor of online infringement defendants and in favor of looser standards for online copyright infringement.[167]

In-line linking is commonplace on the Internet. At issue in this case was a type of content that is common on the Internet: a picture of unknown providence with clear newsworthiness, which in today's 24-hour news cycle required a response from online news properties. Rejecting the server test opens up nearly every Internet user, from websites using links in place of footnotes to social media users retweeting a silly photo, potentially at risk of significant liability. Thus, Internet culture would be undermined for the sake of opportunism. On the other hand, affirming the server test on appeal could make it nearly impossible for copyright holders like Goldman to assert their rights against the parties that accelerate and profit most from appropriation of copyrighted material, as there is no feasible way for copyright holders to force Twitter to take down thousands of tweets using his work. Thus, a backdoor for infringement would be created.

D. COPYRIGHT OFFICE REPORT ON SOFTWARE-ENABLED CONSUMER PRODUCTS

On December 15, 2016, the Copyright Office published a report analyzing the impact of copyright law on software-enabled consumer products, as requested by Senate Judiciary Committee Chairman Chuck Grassley and Ranking Member Patrick Leahy.[168] The report focused on how copyrighted

163. *Id.* at *9.

164. *Id.* at *7.

165. *Id.*

166. Am. Broad. Cos., Inc. v. Aereo, Inc., 134 S. Ct. 2498, 2514 (2014) (Scalia, J., dissenting).

167. *See, e.g.*, Cartoon Network, L.P., LLLP v. CSC Holdings, Inc., 536 F.3d 121 (2d. Cir. 2008); Viacom Int'l., Inc. v. YouTube, Inc., 676 F.3d 19 (2d. Cir. 2012).

168. U.S. COPYRIGHT OFFICE, SOFTWARE-ENABLED CONSUMER PRODUCTS: A REPORT ON THE REGISTER OF COPYRIGHTS i (2016) [hereinafter SOFTWARE-ENABLED CONSUMER

software in consumer products has impacted privacy, cybersecurity, and intellectual property rights.[169] It concluded that existing law adequately protects consumer usage and encourages industry innovation and thus recommended no policy changes.[170]

First, the Office found that current law sufficiently addresses new implications posed by software in the inherent tension between incentivizing innovators to create new work and enabling consumers to fully utilize their property.[171] These new implications include user resale, research, and repair.[172] While the technology may be new, existing case law adequately addresses copyright issues in software-enabled products.[173]

Second, the Office lacked evidence that copyright holders were preventing consumers from reselling their devices and thus concluded that device resale was not impacted by current law.[174] However, the Office acknowledged that this was happening to commercial grade products.[175]

Similarly, the Office concluded that a consumer's "tinkering and repair" of a software-enabled device is likely fair use, although it may affect the copyright owner's exclusive rights regarding reproduction, derivative works, distribution, and public display.[176] The Office found it difficult to specifically define fair use in tinkering and repair because the technology is rapidly advancing.[177] It is clear, however, that tinkering is fair use because current law allows device owners to make functional changes to their devices—a "tinkerer" alters the device to change how the device functions without benefiting from the copyrightable, inherently creative elements of the code.[178] There are some limitations on the subsequent lease, sale, or transfer of lawfully altered devices,[179] but while consumer advocates may worry about aggressive enforcement, market forces may discourage manufacturers from preventing device repair.[180]

Additionally, the Office concluded that it is fair use for the public to conduct non-commercial cybersecurity research on software-enabled

---

PRODUCTS REPORT].

169. *Id.*

170. *Id.* at iii.

171. *See id.* at i–iii.

172. *Id.* at i.

173. *See id.*; *see also* H.R. 862, 114th Cong. (2015) (You Own Devices Act, aimed at curbing end-user license agreements and allowing consumers to reclaim ownership rights in purchased software-enabled devices).

174. SOFTWARE-ENABLED CONSUMER PRODUCTS REPORT, *supra* note 168, at 29–30.

175. *Id.*

176. *Id.* at 31–33.

177. *See id.* at 33.

178. *See id.* at 37 and 40.

179. *Id.* at 38.

180. SOFTWARE-ENABLED CONSUMER PRODUCTS REPORT, *supra* note 168, at 33.

consumer products.[181] This includes protecting public individuals who search for technical vulnerabilities in software and then notify the copyright owner of these weaknesses.[182] Notably, some copyright holders are effectively preventing cybersecurity research through aggressive DMCA takedown notices and license terms.

Next, the Office determined that current law enables interoperability between copyrighted devices and industry competition, even if emerging technologies create legal uncertainties.[183] Courts have repeatedly held that it is fair use to reverse-engineer a competitor's device to produce a new, compatible product.[184]

Finally, the Office addressed concerns that increasingly common software license agreements expressly narrow the permissible usage of consumer devices.[185] Under such end-user license agreements (EULAs), the owner of the device does not own the copy of the software, but is merely a licensee.[186] Some courts refuse to enforce EULAs on the grounds that they are unconscionably one-sided, or that state law requirements for contract formation are not met by "clickwrap" agreements.[187] However, when enforced, licensors have full control over the rights consumers can exercise over their devices.[188] While the Office acknowledges that consumers would benefit if EULAs were more clear, it found existing law adequate to protect consumer interests. The Office declined to comment on when the Copyright Act preempts software license agreements.[189]

Acknowledging that any policy recommendations would quickly become outdated due to the fast-paced nature of technology industry, the Office did not recommend any legislative changes.[190] While the ubiquity of software in consumer products does raise new questions, the Office concluded that the existing law is flexible enough to provide adequate protection to both

181. *Id.* at 49.
182. *Id.* at 45.
183. *Id.* at 52.
184. *See id.* at 54; *see also* Sega Enters. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992) (holding that it was fair use for a competitor to copy Sega's software to reverse-engineer the code and determine how to make game cartridges interoperable with Sega's console); Sony Computer Entm't, Inc. v. Connectix Corp., 203 F.3d 596 (9th Cir. 2000) (holding that the making of intermediate copies of video game console's operating system to create a console emulator that did not duplicate the copyrighted code in the new work, but allowed a PC to play console games, was a fair use).
185. SOFTWARE-ENABLED CONSUMER PRODUCTS REPORT, *supra* note 168, at 62–64.
186. *Id.* at 21.
187. *Id.* at 63.
188. *See id.* at 64.
189. *Id.* at 64–65.
190. *Id.* at 69.

copyright owners and consumers of software-embedded products.[191]

III. PRIVACY DEVELOPMENTS

A. *IN RE* SUPERVALU, INC., 870 F.3D 763 (8TH CIR. 2017)

The United States Court of Appeals for the Eighth Circuit held that customers whose financial information became compromised could not recover for possible future identity theft.[192]

Customers brought a putative class action against the owners and operators of the grocery stores SuperValu, AB Acquisition, and New Albertsons for their poor cybersecurity, which resulted in perpetrators stealing customers' financial information.[193] Perpetrators twice hacked into the store networks and installed malicious software to access credit card information in July 2014, compromising 1,045 stores.[194] The perpetrators accessed the names, account numbers, expiration dates, card verification value (CVV) codes, and personal identification numbers (PINs) of credit cards used in those stores.[195]

Operators issued a press release notifying customers of the first hack in August 2014.[196] The release acknowledged that the attack "may have resulted in the theft" of information, but could not definitively confirm stolen cardholder data or misuse of such data.[197] After the second data breach, operators issued another press release in September 2014 stating they could only confirm a breach but not whether the perpetrators actually stole the information and used it.[198]

Customers brought claims of negligence, breach of implied contract, negligence per se, and unjust enrichment, citing state consumer protection and data breach notification statutes.[199] Customers alleged that the two breaches stemmed from the same security failures.[200] According to them, operators failed to take adequate security measures by not installing firewalls, segregating their network, using more advanced passwords, and locking out users after unsuccessful login attempts.[201]

However, customers encountered legal issues when they could not

191. SOFTWARE-ENABLED CONSUMER PRODUCTS REPORT, *supra* note 168, at 69.
192. *In re* Supervalu, Inc., 870 F.3d 763, 773 (8th Cir. 2017).
193. *Id.* at 766.
194. *Id.*
195. *Id.*
196. *Id.*
197. *Id.*
198. *In re* Supervalu, Inc., 870 F.3d 763, 766 (8th Cir. 2017).
199. *Id.* at 767.
200. *Id.* at 766.
201. *Id.*

demonstrate actual harms.[202] Only one plaintiff, David Holmes, discovered a fraudulent charge on his credit card statement.[203] The district court held that, because the customers alleged only an "isolated single instance of an unauthorized charge," customers did not sufficiently show a general misuse of information for all customers.[204] Customers argued on appeal that they will likely suffer identity theft in the future, and that perpetrators can use their information to siphon money from accounts, make unauthorized card charges, open new accounts, or sell information on the black market.[205]

The Court of Appeals sided with the grocery stores. The court found that the customers must prove their threatened injuries to be: (1) certainly impending; and (2) of substantial risk.[206] Customers did not meet this standard since only one plaintiff experienced fraudulent charges.[207] The customers did not present any evidence of certainly impending threats of substantial risk, only speculations.[208] The court pointed out that most identity theft occurs with other personally identifiable and sensitive information such as Social Security numbers, dates of birth, or driver license numbers.[209] Not only that, but within the twenty-four largest data breaches reported between 2000–2005, only four resulted in identity theft.[210] All of these facts implied a low probability of future identity theft in the near-future.

The court subsequently affirmed the district court ruling that customers did not establish a substantial risk of identity theft.[211] These holdings reflect that the burden for plaintiffs may be high in similar cases unless plaintiffs experience actual harms. This has implications both for fairness to customers as well as the effectiveness of deterring poor cybersecurity within businesses.

B. STANDING AND CYBERSECURITY

Almost 2 billion files containing US citizens' personal data were reported leaked in 2017.[212] And yet, despite the frequency of data breaches, courts have struggled to reach consensus on whether their occurrence give victims

202. *Id.* at 773.
203. *Id.* at 767.
204. *In re* Supervalu, Inc., 870 F.3d 763, 773 (8th Cir. 2017).
205. *Id.* at 766–67.
206. Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2016).
207. *In re Supervalu*, 870 F.3d at 774.
208. *Id.* at 770.
209. *Id.*
210. *Id.*
211. *Id.* at 774.
212. Tara Seals, *Two Billion Files Leaked in US Data Breaches in 2017*, INFOSECURITY (Feb. 15, 2018), https://www.infosecurity-magazine.com/news/two-billion-files-leaked-in-us-data [https://perma.cc/6LJF-EU4S].

standing to sue.

Modern-day confusion traces back to Article III of the Constitution, delimiting federal judicial power to "cases" and "controversies." To have standing to sue, the Supreme Court set out three requirements: the plaintiff must have "(1) suffered an injury in fact (2) that is fairly traceable to the challenged conduct of the defendant (3) that is likely to be redressed by a favorable judicial decision."[213]

Data breach victims typically struggle to meet the first prong—an injury in fact. For an injury in fact, plaintiffs must show either an actual harm that the violation of the statute amounts to injury in itself or that there will be imminent future harm.[214] Of course, if plaintiffs can prove actual harm through showing real dollars lost, then standing is a slam dunk. However, data breach victims typically struggle to bring evidence of actual harm, since the consequences of stolen data do not necessarily equate to monetary damages. Moreover, harm via data theft is often temporally far-removed and difficult to trace. Thus, plaintiff attorneys are left with statutory claims or a showing of imminent future harm.

In *Spokeo, Inc. v. Robins*, the Supreme Court said "a bare procedural violation, divorced from any concrete harm" is not enough to establish standing.[215] But just what constitutes a concrete harm is still up for debate. Circuits have split over whether a statutory violation confers de facto standing, or if a more particularized showing of injury is necessary.[216] The Eleventh and Third Circuits have found that an allegation of a statutory violation sufficiently supports an inference of concrete injury.[217] The Eighth Circuit and District of Columbia, however, ground their analysis on how the violation allegedly affected the plaintiff.[218]

In lieu of a relevant statute, plaintiffs fall back on the theory of future harm. Circuits' receptivity to this argument turns on their estimate of whether a data

213. Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

214. Merritt Baer & Chinmayi Sharma, *Your Voter Records Are Compromised. Can You Sue? Theories of Harm in Data-Breach Litigation*, LAWFARE (Aug. 7, 2017), https://lawfareblog.com/your-voter-records-are-compromised-can-you-sue-theories-harm-data-breach-litigation [https://perma.cc/5AWJ-2HMV].

215. *Spokeo, Inc.*, 136 S. Ct. at 1549.

216. Andrew C. Glass, et al., *Federal Courts Follow Two Approaches Post-Spokeo When Analyzing Standing*, WASH. LEGAL FOUND. (Jan. 27, 2017), http://www.wlf.org/upload/legalstudies/legalbackgrounder/012717LB_Glass.pdf [https://perma.cc/Q4ST-VBUT].

217. Church v. Accretive Health, Inc., 654 F. App'x 990 (11th Cir. 2016) (per curiam); *In re* Horizon Healthcare Servs. Inc. Data Breach Litig., 846 F.3d 625, 639 (3d Cir. 2017) (holding any such data breach is an injury in fact, "whether or not the disclosure . . . increased the risk of . . . future harm.").

218. Braitberg v. Charter Communications, Inc., 836 F.3d 925 (8th Cir. 2016); Hancock v. Urban Outfitters, Inc., 836 F.3d 925 (8th Cir. 2016).

breach's risk of harm is considered sufficiently injurious to give plaintiffs standing. The Supreme Court has dismissed multiple cases involving potential future injury from data breach because there was insufficient showing of particularized harm.[219] The Third Circuit has rejected future harm as a justiciable theory for standing.[220] Most other circuits have operated in shades of gray, neither embracing nor rejecting the theory of future harm.[221] Within this spectrum, there is substantial variability: the Sixth, Seventh, and D.C. Circuits have found standing in data breach actions on the risk of future harm;[222] the Second, Fourth, and Eighth have denied standing on the same theory.[223]

With the Circuits in conflict and data breaches on the rise, judges and scholars must consider how to reconcile the competing approaches. On the one hand, awarding damages on the basis of per se statutory violation or a theory of future harm recognizes a need to deter sloppy cybersecurity and provide plaintiffs a legal remedy for lost data. On the other hand, society wants to ensure that defendants are punished, and plaintiffs compensated, only when harm is substantial. Indeed, it would seem unfair to "blame the victim" by sanctioning businesses for a data breach in all cases, especially when some data centers are under siege by sophisticated actors and even nation states.

In any event, time will tell how this plays out. The Supreme Court recently denied cert on the D.C. Circuit's *Attias v. CareFirst*.[224] The question was whether a plaintiff has Article III standing based on a substantial risk of harm that is not imminent and where the alleged future harm requires speculation about the choices of third-party actors not before the court. Undoubtedly, a similar issue will come to the Court again, the answer to which may well determine the future of cybersecurity litigation.

C. EUROPEAN DATA ENFORCEMENT AGAINST U.S. COMPANIES

United States technology companies doing business in the European Union (EU) render their services to roughly 500 million consumers, making

219. Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013); Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016).

220. Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011).

221. Catherine Padhi, *Standing in Data-Breach Actions: Injury in Fact?*, LAWFARE (Dec. 18, 2017), https://www.lawfareblog.com/standing-data-breach-actions-injury-fact [https://perma.cc/PTP7-G8F5].

222. Galaria v. Nationwide Mut. Ins. Co., 663 F. App'x 384 (6th Cir. 2016); Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688 (7th Cir. 2015); Attias v. Carefirst, Inc., 865 F.3d 620 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 981 (2018).

223. Beck v. McDonald, 848 F.3d 262 (4th Cir.), *cert. denied sub nom.* Beck v. Shulkin, 137 S. Ct. 2307 (2017); *In re* Supervalu, Inc., 870 F.3d 763, 773 (8th Cir. 2017).

224. Attias v. Carefirst, Inc., 138 S. Ct. 981 (2018).

this region one of the most important overseas markets for such companies.[225] Yet policy makers in the 28-member European Union stringently scrutinize the data collection, transfer, and processing mechanisms of these corporations. Each member state of the EU operates under the 1995 Data Protection Directive (Directive) and has its own national laws.[226] National Data Protection Authorities (DPAs) established under the Directive are appointed to implement and enforce data protection laws in the EU.[227]

In 2016, the French data protection authority, CNIL, fined Google $115,000 for failing to extend beyond the borders of EU the "right to be forgotten" mandate which removes inadequate or irrelevant information from web results under searches for people's names.[228] While the French DPA argued that the removal must be global to uphold Europeans' rights to privacy because experienced users could circumvent the domestic domain of Google, Google defended itself by saying that such removal should not go beyond Europe and into countries with different laws on the subject.[229] To prevent a dangerous precedent on the territorial reach of national, Google argued that each country should be able to balance freedom of expression and privacy in the way that it chooses, not in the way that another country chooses.[230] Google filed an appeal against CNIL's decision before France's Conseil d'État, the country's highest administrative court, which further referred the matter to the Court of Justice of the European Union (ECJ) to determine whether search engines must apply the "right to be forgotten" decision to their search domains outside of the European Union. As of publication, the matter is currently pending before the ECJ.[231]

Similarly, the data protection commissioner of Hamburg, Germany

225. Mark Scott, *What US Tech Giant Face in Europe in 2017*, N.Y. TIMES (Jan. 1, 2017), https://www.nytimes.com/2017/01/01/technology/tech-giants-europe-2017.html [https://perma.cc/B6ZK-ZYR5].

226. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data, 1995 OJ (L 281) 31, 45–46.

227. *Id.*

228. Commission Nationale de L'informatique et des Libertés [French National Commission of Computing and Freedoms], decision no. 2016-054SANCTION, Mar. 10, 2016, LEGIFRANCE, https://www.legifrance.gouv.fr/affichCnil.do?oldAction=rechExpCnil&id=CNILTEXT000032291946&fastReqId=273825503&fastPos=1 [https://perma.cc/48XQ-45B4].

229. *France's Fight Over Google Search Results Was Kicked to Europe's Top Court*, FORTUNE (July 19, 2017), http://fortune.com/2017/07/19/france-google-right-forgotten-eu-court [https://perma.cc/P39Q-U3UH].

230. *Id.*

231. *See* CE, July 19, 2017, CONSEIL D'ÉTAT, http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC [https://perma.cc/B7VB-WGEJ] (Fr.).

ordered Facebook to stop collecting and storing data on WhatsApp users when the latter announced that it will start to share some of its users' online information with Facebook. The regulator made user consent compulsory before such data could be shared between the two companies. It also called on the social network to delete all information already forwarded from WhatsApp on roughly 35 million German users.[232] In September 2017, the Spanish data protection regulator (AEPD) issued a $1.4 million fine against Facebook for violations regarding its data harvesting activities.[233] The AEPD claimed that when Facebook collects, stores, and uses data for advertising purposes, it does so without obtaining adequate user consent.[234]

In a similar situation, the Hague Administrative Court in the Netherlands upheld a decision by the Dutch Data Protection Authority that WhatsApp was in breach of the Dutch Data Protection Act on account of its alleged failure to identify a representative within the country responsible for compliance with the Act, despite the processing of personal data of Dutch WhatsApp users on Dutch smartphones.[235] The DPA concluded that WhatsApp must appoint a representative in the Netherlands within three months, subject to a penalty of €10,000 per day with a maximum of €1,000,000.[236]

In light of these events and to bring about an effective regulation, the U.S. Department of Commerce and the EU recently signed a trans-Atlantic data transfer agreement, the EU-US Privacy Shield Framework, which imposes strong obligations on U.S. technology companies handling data.[237] The EU-US Privacy Shield Framework enforces clear safeguards and transparency obligations on U.S. government access, effective protection of individual rights, and an annual joint review mechanism. Earlier, many U.S. companies engaging in cross-border transfers of personal data between Europe and the

232. Mark Scott, *Facebook Ordered to Stop Collecting Data on WhatsApp Users in Germany*, N.Y. TIMES (Sept. 27, 2016), https://www.nytimes.com/2016/09/28/technology/whatsapp-facebook-germany.html [https://perma.cc/SDM8-DQT7].

233. *Resolution R/01870/2017*, Spanish Data Protection Agency (Mar. 8, 2016), http://www.agpd.es/portalwebAGPD/resoluciones/procedimientos_sancionadores/ps_2017/common/pdfs/PS-00082-2017_Resolucion-de-fecha-21-08-2017_Art-ii-culo-4-5-6-7-LOPD.pdf.

234. *Id.*

235. *Court Decides WhatsApp Data Protection Case*, LEXOLOGY (Nov. 28, 2016), https://www.lexology.com/library/detail.aspx?g=0c58295a-0d8f-4252-aa7f-35c5a8ad3fd6 [https://perma.cc/A6CM-A22X].

236. WhatsApp Inc. v. Authority Personal Data, No. SGR 15/9125, Court of the Hague (Nov. 22, 2016), https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2016:14088 [https://perma.cc/3X6K-8K8D].

237. Dep't of Commerce, *EU-U.S. Privacy Shield Framework Principles*, https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg [https://perma.cc/6ZQ2-NM5Y].

U.S. relied on the EU-US Safe Harbor program, as well as on the validity of other mechanisms for transfers to the U.S. such as standard contractual clauses (SCCs) and binding corporate rules (BCRs).[238] However, in 2015, the ECJ struck down the Safe Harbor framework in the *Schrems v. Facebook* ruling.[239] The "safe harbor" arrangement enabled Facebook, for example, to store the profiles of its Spanish and Italian users on the same facilities it uses for customers in New York.[240] In *Schrems*, the plaintiff complained that Facebook Ireland was transferring his data via SCCs to servers located in the US, where it was being processed, without ensuring sufficient protection for it as required under the Charter of Fundamental Rights of the EU.[241] In light of the ruling, companies could no longer rely on self-certification to establish compliance with EU privacy laws.[242]

To tighten the noose around data processing, data storage and protection practices of companies which offers goods and services to EU individuals, the European Parliament adopted the General Data Protection Regulation (GDPR) in April 2016, replacing the outdated data protection Directive. As a unified data protection law, the GDPR will do away with the current fragmentation and costly administrative burdens of companies doing business in EU. The Regulation will be enforced not only against companies that are located within the EU, but upon all organizations regardless of their physical location. To ensure strict compliance, the GDPR allows for steep penalties of up to €20 million or 4 percent of global annual turnover.[243]

Organizations and companies that are currently subject to the EU DPAs and that are either 'controllers' or 'processors' of personal data and sensitive personal data will be covered by the GDPR. Personal data will include any

238. Mark Young et al., *EU DPA Enforcement Guidance Post-Schrems*, INSIDE PRIVACY (Feb. 18, 2016), https://www.insideprivacy.com/international/european-union/eu-dpa-enforcement-guidance-post-schrems [https://perma.cc/3HEQ-2DM2].

239. Data Protection Commissioner v. Facebook Ireland Ltd. & Maximilian Schrems, [2016] IEHC 414 (Ir.).

240. *How European Privacy Concerns Could Hurt U.S. Tech Firms*, L.A. TIMES (Oct. 8, 2015), http://www.latimes.com/opinion/editorials/la-ed-europe-data-privacy-20151007-story.html [https://perma.cc/XRA9-8KCZ].

241. Mary Carolan, *Irish Data Protection Case 'of The Utmost Importance' to US*, IRISH TIMES (June 27, 2016), https://www.irishtimes.com/business/technology/irish-data-protection-case-of-the-utmost-importance-to-us-1.2701891 [https://perma.cc/G2JM-6DPA].

242. Leun Jolly, *Data protection in the United States: Overview*, WESTLAW (July 1, 2017), https://content.next.westlaw.com/Document/I02064fbd1cb611e38578f7ccc38dcbee/View/FullText.html?contextData=(sc.Default)&transitionType=Default&firstPage=true&bhcp=1.

243. *See* Regulation (EU), of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 206 OJ (L 119) 1, 1–88.

information that can be used to identify a person, e.g., name, address, IP address, etc.[244] Sensitive personal data encompasses genetic data, information about religious and political views, sexual orientation, and more. Where the GDPR differentiates from current data protection laws is that pseudonymized personal data can fall under the law if it is possible that a person could be identified by a pseudonym.[245]

Privacy advocates have welcomed the GDPR because it will not only improve transparency and certainty, but it will also empower individuals to understand the privacy implications of the data they share with companies. However, there are a few fundamental loopholes in the regulation that might dampen its effectiveness. The rules allow private companies to collect personal data for "legitimate interests," the definition of which has not been provided in the text. The regulations also allow governments and law enforcement agencies to retain great leeway in collecting data through provisions that allow data collection for national security purposes. For some of these reasons, there is quite a bit of uncertainty in how the regulations will be enforced. Moreover, U.S. technology companies doing business in Europe have very little time to finalize their implementation mechanisms to ensure full compliance with the rules.

D. CHINA'S NEW CYBERSECURITY LAW

China's new Cybersecurity Law, which went into effect on June 1, 2017,[246] imposes regulations on both network operators and Critical Information Infrastructure (CII) sectors to protect their networks.[247] CII includes telecommunications, information services, and governmental agencies.[248] The law requires CIIs to conduct security inspections, appoint cybersecurity management, and complete "disaster recovery backups."[249]

One of the law's greatest impacts is on cross-border data transfers. The law mandates a new data localization policy, which requires CIIs to store all

244. Matt Burgess, *GDPR Will Change Data Protection—Here's What You Need to Know*, WIRED (Nov. 7, 2017), http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 [https://perma.cc/3MKG-449B].

245. *Id.*

246. Jack Wagner, *China's Cybersecurity Law: What You Need to Know*, DIPLOMAT (June 1, 2017), https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/ [https://perma.cc/D94X-5X9N].

247. *Id.*

248. *Id.*

249. Jeff C. Dodd, Jerry Jie Li, Dora Luo & Ross Campbell, *People's Republic of China Cybersecurity Law: A Preliminary Overview of Western Companies*, NAT'L L. REV. (July. 17, 2017), https://www.natlawreview.com/article/people-s-republic-china-cybersecurity-law-preliminary-overview-western-companies [https://perma.cc/6TUE-ZBBX].

"personal data" and "important data" within Chinese borders.[250] Therefore, if network operators or CIIs want to transfer personal data or information outside of China, Chinese national authorities must first conduct a security assessment according to its national security, economic, and social welfare concerns.[251] Network operators who want to transfer more than one terabyte of data or collect data on more than 500,000 subjects need to both obtain permission of subjects and pass the security assessment.[252]

The law grants enforcement agencies considerable discretion in blocking any transfer they believe will endanger China's political, economic, or security systems.[253] Consequently, data localization policies can create market uncertainty and increase costs for U.S. and multi-national corporations operating in China by: (1) unpredictability due to ambiguous definitions and China's decentralized data protection systems; and (2) the importance of data analytics and cloud computing.[254]

With regards to (1), the law regulates "personal data" or "important data" without explicitly defining what those terms mean.[255] In addition, different data regulators work in different industries.[256] Each industry will conduct security assessments separately, resulting in inconsistent and "patchy" results.[257] For instance, regulators in the banking industry will conduct assessments differently compared to the health care industry, sending mixed signals and fostering uncertainty for U.S. firms. Corporations may be fined or forced to suspend operations if they violate the law.[258] Therefore, corporations that necessitate data storage and collection may find it too risky to operate in China.

With respect to (2), corporations rely on data for numerous functions: from monitoring supply chains and production systems to managing global

250. Rong Cheng, *China's Cyberspace Body Issues Draft on Cross-Border Data Flow Controls*, FORBES (Apr. 26, 2017), https://www.forbes.com/sites/roncheng/2017/04/26/chinas-cyberspace-body-issues-draft-on-cross-border-data-flow-controls/#4929da6e5880 [https://perma.cc/N8RA-NCDF].

251. *Id.*

252. *Id.*

253. *See* Dodd et al., *supra* note 249.

254. Nigel Cory, *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost*, INFO. TECH. & INNOVATION FOUND. (May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost [https://perma.cc/SP2F-N2AZ].

255. Carly Ramsey & Ben Wootliff, *China's Cyber Security Law: The Impossibility Of Compliance?*, FORBES (May 29, 2017), https://www.forbes.com/sites/riskmap/2017/05/29/chinas-cyber-security-law-the-impossibility-of-compliance/#74a8e085471c [https://perma.cc/2CWV-WPUJ].

256. Cheng, *supra* note 250.

257. Ramsey & Wootliff, *supra* note 255

258. *See* Cheng, *supra* note 250.

workforces.[259] Furthermore, corporations use personal data to understand consumer preferences and willingness to pay in order to modify advertising strategies. Companies will need to complete mandatory assessments any time they want to transfer data from China back to the U.S. or to third parties such as data processing contractors. However, due to the tremendous discretion Chinese law enforcement possesses in denying transfer requests, U.S. corporations may give up on these data transfers altogether.

In order to hedge against these concerns, the U.S. can try striking a bilateral trade agreement or "data-services agreement" to work around the localization policies.[260] For example, in February 2016, the European Commission and the U.S. negotiated the "EU-US Privacy Shield," a framework to permit transatlantic transfers of personal data in which the U.S. agreed to limited access to data for law enforcement and national security purposes.[261] A similar agreement could be reached with China should the Cybersecurity Law bring significant harm to U.S. firms.

IV. OTHER DEVELOPMENTS

A. FTC CRACKDOWN ON SOCIAL MEDIA INFLUENCERS

Brands are increasingly relying on social media for advertising and marketing their goods and services.[262] As a result, companies are turning to social media influencers (with built-in audiences) to get their products and messages out to consumers. Aside from their large following, influencers themselves are considered a brand such that followers consider influencers' opinions and endorsements to be credible.

The Federal Trade Commission (FTC) requires social media influencers to clearly disclose any blog or social media post sponsored by a company.[263] In fact, in spring of 2017 the FTC sent out more than ninety letters addressed to influencers and marketers reminding them that, when promoting or endorsing a brand, the relationship with the brand must be clearly disclosed to the audience.[264] The FTC Endorsement Guides state that a "material connection"

259. Cory, *supra* note 254.

260. *See id.*

261. Markus Evans, Adam Smith & Christoph Zieger, *EU and US Reach Agreement on Cross-Border Data Transfer Framework, But Uncertainty Remains*, DATA PROT. REPORT (Feb. 2, 2016), http://www.dataprotectionreport.com/2016/02/2809 [https://perma.cc/WS5A-TEG5].

262. *A Brand New Game*, ECONOMIST (Aug. 27, 2015), https://www.economist.com/news/business/21662543-people-spend-more-time-social-media-advertisers-are-following-them-brand-new-game [https://perma.cc/JY79-H6GK].

263. FTC, THE FTC'S ENDORSEMENT GUIDE: WHAT PEOPLE ARE ASKING (2017), [hereinafter FTC ENDORSEMENT GUIDE].

264. Press Release, Fed. Trade Comm'n, FTC Staff Reminds Influencers and Brands to

needs to be clearly communicated.[265] Material connections are defined as a business or family relationship, gift or free product, or monetary payment.

The FTC's intent is to warn social media influencers and marketers that it is monitoring their activities, and that proper disclosures are required. The FTC also provided guidelines for proper disclosure formats.[266] As it pertains to Instagram posts, users are only able to view the first three lines of the post unless they click "more." The FTC has concluded that most consumers do not click the "more" button and rather only look at the first three lines.[267] Thus, any disclosure as to an endorsement needs to be made above the "more" button.[268]

The FTC's efforts to regulate social media posts is not a new phenomenon: in 2015, the FTC warned Kim Kardashian about an Instagram post for a morning sickness drug wherein she failed to disclose that it was a paid advertisement.[269] In fact, in September of 2017, one of the first FTC cases against social media influencers was settled. In *In re CSGOLOTTO, Inc*, the FTC filed a complaint against two YouTubers for failing to disclose their connection with the brand being promoted.[270] The YouTubers in question, Trevor "TmarTn" Martin and Thomas "Syndicate" Cassell, are social media influencers widely followed in the online gambling community.[271] The two regularly made videos and published tweets promoting a gambling website, Counter-Strike: Global Offensive. The YouTubers would post videos of themselves winning large amounts of money while gambling on the Counter Strike site.[272] However, the YouTubers failed to disclose that they were also owners of the website Counter Strike.[273] Ultimately, the FTC settled the charges by requiring Martin and Cassell to clearly and conspicuously disclose any material connection with an endorser and any promoted product.[274]

The FTC works to promote competition as well as to protect and educate consumers. To this end, consumers should be informed and be able

Clearly Disclose Relationship (Apr. 19, 2017) [hereinafter FTC Press Release on Disclose Relationship].

265. FTC ENDORSEMENT GUIDE, *supra* note 263.

266. *Id.*

267. FTC Press Release on Disclose Relationship, *supra* note 264.

268. *Id.*

269. Jeff John Roberts, *The FTC Says Celebrity Social Media Ads Are Still Too Sneaky*, FORTUNE (Apr. 20, 2017), http://fortune.com/2017/04/20/ftc-instagram [https://perma.cc/MXK5-BVDB].

270. Press Release, Fed. Trade Comm'n, CSGO Lotto Owners Settle FTC's First Ever Complaint Against Individual Social Media Influencers (Sept. 7, 2017).

271. *Id.*

272. *Id.*

273. *Id.*

274. *Id.*

differentiate when they are being presented with a paid advertisement as opposed to an unsolicited opinion on a product or a service.

B. OCCUPATIONAL LICENSING AND THE "SHARING ECONOMY"

The Supreme Court's 1889 decision in *Dent v. West Virginia*, concluding a state may adopt a physician licensing scheme to protect public health and safety, introduced government gatekeeping to a narrow set of occupations via licensing requirements.[275] This power was exercised only moderately in the past, as less than five percent of American jobs demanded a license in the 1950s.[276] However, the floodgates have since opened: recent labor market analysis estimates 25 to 29 percent of American occupations require licenses, making it one of the fastest growing institutions in the US labor market.[277]

Today, technological innovation—particularly the "sharing economy"[278]—has come into conflict with extant occupational licensing law.[279] While proponents of licensing requirements advocate their ability to assure quality services for consumers,[280] detractors contend these barriers create artificial supply-side scarcity that raises the cost of services and stifles competition from emerging service platforms. This impacts the development not only of tech giants like Uber and Airbnb, but also lesser-known startups in sectors ranging from food-sharing[281] to cosmetology.[282]

---

275. Dent v. West Virginia, 129 U.S. 114 (1889); *see* Morris M. Kleiner, *A License for Protection*, 29 REG. 17, 17 (2006).

276. M. Kleiner & Alan B. Krueger, *The Prevalence and Effects of Occupational Licensing*, 48 BRIT. J. INDUS. REL. 676, 678 (2010).

277. *Id.*

278. Though there is no consensus definition, the "sharing economy" can be defined generally as an economic system in which assets or services are shared between private individuals, either free or for a fee, typically by means of the Internet. *See generally* Vanessa Katz, *Regulating the Sharing Economy*, 30 BERKELEY TECH. L.J. 1067 (2015).

279. *See, e.g.*, Wallen v. St. Louis Metro. Taxicab Comm'n, No. 4:15CV1432 HEA, 2016 WL 5846825 (E.D. Mo. Oct. 6, 2016) (Uber's suit against the St Louis Taxi Commission); Teledoc, Inc. v. Texas Med. Bd., 112 F. Supp. 3d 529 (W.D. Tex. 2015) (telemedicine provider Teledoc's suit against the Texas Medical Board).

280. *See* Austin Raynor, Note, *Economic Liberty and the Second-Order Rational Basis Test*, 99 VA. L. REV. 1065, 1085 (2013) ("The most common public justification for imposing licensing requirements on a profession is to provide protection to consumers against 'unethical or incompetent practitioners.") (quoting Michael J. Phillips, *Entry Restrictions in the* Lochner *Court,* 4 GEO. MASON L. REV. 405, 411 (1996).

281. Sarah Kessler, *The Foot-Sharing Economy is Delicious and Illegal—Will It Survive?*, FAST COMPANY (July 7, 2016), https://www.fastcompany.com/3061498/the-food-sharing-economy-is-delicious-and-illegal-will-it-survive [https://perma.cc/BFU2-NHW5].

282. Brittany Hunter, *"Sharing Economy" Reveals that Licensing Laws Are Really About Shutting Down the Competition*, MISES INST. (Oct. 7, 2016), https://mises.org/blog/sharing-economy-reveals-licensing-laws-are-really-about-shutting-down-competition [https://perma.cc/87DN-Q5AR].

The mechanism of occupational licensing regulation is well established. States are generally empowered to tailor their economies as they see fit, with power to impose occupational requirements, regulate market entry, or otherwise limit competition as deemed appropriate in pursuit of public policy goals.[283] Thus, in most situations, "federal antitrust laws are subject to supersession by state regulatory programs."[284]

Specifically, State regulation is granted "*Parker* immunity" (establishing federal antitrust oversight is inappropriate because state agencies are politically accountable to elected officials and voters) where the challenged restraint is "clearly articulated and affirmatively expressed as state policy" and is "actively supervised by the State itself."[285]

Practically, this means licensing requirements can vary by state and even by municipality, often drafted by a board of professionals.[286] This dynamic makes regulatory or legislative reform difficult, as public choice theory predicts laws with concentrated benefits (for the occupation), diffused costs (for consumers), and cohesive professional organizations incentivized to defend the status quo are unlikely candidates for reform.[287]

Nonetheless, some of the larger companies in the space have successfully lobbied the government against enforcing licensing restrictions for their particular service. For example, Uber was forced to launch a campaign in 2015 after New York Mayor Bill de Blasio threatened to curb the company's expansion.[288] Similarly, Airbnb defeated a San Francisco ballot measure restricting short-term rentals after spending $8 million lobbying against it.[289] However, for smaller companies with limited resources, lobbying can be an

283. N.C. State Bd. of Dental Exam'rs v. F.T.C., 135 S. Ct. 1101 (2015).

284. F.T.C. v. Ticor Title Ins. Co., 504 U.S. 621, 632 (1992).

285. Parker v. Brown, 217 U.S. 341 (1943); California Retail Liquor Dealers Ass'n v. Midcal Alum., Inc., 445 U.S. 97, 105 (1980).

286. Austin Raynor, Note, *Economic Liberty and the Second-Order Rational Basis Test*, 99 VA. L. REV. 1065, 1086 ("[O]ccupational licensing boards are frequently composed of members of the regulated occupation, thereby endowing established producers with the discretion to exclude their own potential competitors.").

287. *See* Milton Friedman, *Occupational Licensure*, *in* CAPITALISM AND FREEDOM 137, 142 (1962); *see also* John Blevins, *License to Uber: Using Administrative Law to Fix Occupational Licensing*, 64 UCLA L. REV. 844 at 868–69 (2017); Robert J. Thornton & Edward J. Timmons, *The De-Licensing of Occupations in the United States*, MAY MONTHLY LAB. REV. 1, 13 (2015)

288. Josh Dawsey, *Uber Targets Mayor Bill de Blasio on Proposed Curbs on Growth*, WALL ST. J. (July 16, 2015), http://www.wsj.com/articles/uber-targets-mayo-bill-de-blasio-on-proposed-curbs-on-growth-1437096154 [https://perma.cc/QL9L-DPX2].

289. Heather Somerville, *Airbnb Wages $ 8 Million Campaign to Defeat San Francisco Measure*, REUTERS (Nov. 1, 2015), http://www.reuters.com/article/us-airbnb-election-sanfrancisco/airbnb-wages-8-million-campaign-to-defeat-san-francisco-measure-idUSKCN0SQ2CJ20151101 [https://perma.cc/7ULF-SWGS].

expensive route, making litigation the only practical means by which to challenge and reform occupational licensing schemes.[290] Indeed, the friction between upstart startups and established occupational license regimes has increasingly sparked litigation that typically takes two forms: antitrust and constitutional challenges.[291]

The constitutional case against occupational licensing relies on the violation of rights to economic liberty under due process and equal protection clauses of federal and/or state constitutions;[292] antitrust cases generally swing on whether occupational licensing amounts to anticompetitive regulatory capture.[293] But startup services differ in kind, so the outcome and implication of any single lawsuit may well vary. For example, startup Teladoc is currently being sued by Texas' medical board for connecting physicians with patients without in-person consultations.[294] But it is unclear how this suit relates to companies like Your.MD, who use chatbots to answer healthcare issues.

At a time when people can be seamlessly connected by the Web and ratings systems can sometimes substitute for occupational licenses in controlling for service quality, which professional fields remain appropriate for state-sponsored occupational protection? What sorts of legal arguments are available for startups affected by licensing regimes? Is the current "ask for forgiveness, not permission" approach (and the binary, litigate-or-leave-it choice this presents to professionals and regulators) pursued by many startups the best way to address these challenges, or is a more cohesive approach tenable? The jury is still out.

290. Blevins, *supra* note 287, at 870.

291. *Id.* at 870–84. Note that Blevins suggests a novel approach—using administrative law as a means to challenge extant licensing regulations.

292. *Id.* at 870; *see, e.g.*, Complaint for Declaratory and Injunctive Relief, at 15–18, Eck v. Battle, No. 1:14-CV-00962-MHS (N.D. Ga. Apr. 1, 2014).

293. Ilya Shapiro, *Protecting Economic Liberty by Other Means*, 10 N.Y.U. J.L. & LIBERTY 118, 118 (2016).

294. Teladoc Inc. v. Tex. Med. Bd., 112 F. Supp. 3d 529 (W.D. Tex. 2015).