

## Federal Circuit v. Ninth Circuit: A Split Over the Conflicting Approaches to DMCA Section 1201

Robert Arthur

Follow this and additional works at: <http://scholarship.law.marquette.edu/iplr>



Part of the [Intellectual Property Commons](#)

---

### Repository Citation

Robert Arthur, *Federal Circuit v. Ninth Circuit: A Split Over the Conflicting Approaches to DMCA Section 1201*, 17 *Intellectual Property L. Rev.* 265 (2013).

Available at: <http://scholarship.law.marquette.edu/iplr/vol17/iss2/4>

This Comment is brought to you for free and open access by the Journals at Marquette Law Scholarly Commons. It has been accepted for inclusion in Marquette Intellectual Property Law Review by an authorized administrator of Marquette Law Scholarly Commons. For more information, please contact [megan.obrien@marquette.edu](mailto:megan.obrien@marquette.edu).

# COMMENTS

## **Federal Circuit v. Ninth Circuit: A Split Over the Conflicting Approaches to DMCA Section 1201**

INTRODUCTION .....	265
I. ORIGINAL POLICY GOALS OF THE DMCA .....	267
II. CHAMBERLAIN I & II .....	269
III. THE RIGHT OF ACCESS .....	272
IV. CHAMBERLAIN III: REASONABLE RELATION .....	275
V. REASONABLE RELATIONSHIP TESTS .....	277
A. But-for causality .....	278
B. Reasonable foreseeability .....	278
C. Substantial non-infringing use .....	279
D. Defendant's intent .....	279
E. Vicarious liability .....	280
F. Aimster balancing test .....	280
VI. THE NINTH CIRCUIT TAKES THE OPPOSITE VIEW: MDY INDUSTRIES ...	281
CONCLUSION .....	284

### INTRODUCTION

Prior to opening statements in *U.S.A. v. Crippen*,<sup>1</sup> a federal criminal DMCA case, U.S. District Judge Phillip Gutierrez vented his frustration during a 30-minute tirade to prosecutors. “I really don’t understand what we’re doing here,” he began.<sup>2</sup> The defendant, Matthew Crippen, was charged with two counts of violating the anti-circumvention provisions of the DMCA, facing a maximum of five years in prison for each count. The government alleged that Crippen ran a business modifying the firmware on Xbox systems to make them capable of running pirated copies of games. Crippen asserted

---

1. *U.S.A. v. Crippen*, 2010 U.S. Dist. LEXIS 143583 (C.D. Cal. 2010).

2. David Kravets, *Xbox-Modding Judge Berates Prosecution, Puts Trial on Hold*, WIREDCOMMUNICATIONS THREAT LEVEL, (Dec. 1, 2010), <http://www.wired.com/threatlevel/2010/12/xbox-judge-riled>.

the *Betamax* defense,<sup>3</sup> arguing that his firmware modifications were legal because they had significant non-infringing uses, such as allowing the user to run alternative software or to make backup copies of their own games. Prosecutors responded that the DMCA did not allow a defendant in a § 1201 action to use the defenses of traditional copyright law, such as the *Betamax* defense. Judge Gutierrez seemed to think (and this author agrees) that the anti-circumvention and anti-trafficking provisions in § 1201 are oddly disconnected from familiar copyright law and policy.

The root of Judge Gutierrez's frustration is that the DMCA's anti-circumvention provisions are in direct conflict with traditional intellectual property doctrine and public policy. Thanks to the misinterpretation of the statute, the lack of any relationship between these provisions and traditional copyright protection has allowed for absurd conclusions, bizarre limitations of fair use, and obtuse applications of the law that threaten long-standing policy goals of intellectual property law and antitrust law.

The *Chamberlain* line of cases provided an opportunity for the Federal Circuit to examine the balance between the DMCA's prohibition of unauthorized access and traditional copyright protection, in light of consumers' expectations regarding the products they own. Misinterpretation of the DMCA was threatening to create a dangerous new property right, the right of access, completely detached from the traditional bundle of rights in § 106 of the Copyright Act, resulting in two distinct copyright regimes. In *Chamberlain III*, the Federal Circuit countered the threat of access right theory, adding a new limitation to the scope of § 1201: a reasonable relation between access and the traditional protections of copyright. The Federal Circuit's reasonable relation test brought § 1201 of the DMCA back in harmony with the rest of the Copyright Act and its legislative intent, restoring the balance between the interests of content owners in countering the digital threat and consumers' expectations regarding the products they own.

Unfortunately, the Ninth Circuit recently rejected the Federal Circuit's reasonable relation test in *MDY Industries*, breathing new life into the notion that § 1201 creates a new right of access, distinct from the rights of traditional copyright law. Because the two holdings are completely incompatible, with the Ninth Circuit expressly rejecting the Federal Circuit's interpretation of § 1201, the result is a circuit split. The time is ripe for either a Supreme Court review or Congressional action to determine which court got it right.

The first part of this paper discusses the original policy goals of the DMCA. In the second part, I examine the issues in *Chamberlain I & II*. In the third part, I discuss the dangers of creating a new property right in the

---

3. Sony Corp. of Am, v. Universal City Studios, Inc., 464 U.S. 417 (1984).

DMCA, the right of access. In the fourth part, I consider how the Federal Circuit corrected this misinterpretation in *Chamberlain III*, adding a new limitation to § 1201: a reasonable relation between access and the traditional rights of copyright. In the fifth part, I propose several reasonable relationship tests. In the sixth part, I examine the Ninth Circuit's contrasting treatment of § 1201 in *MDY Industries*. Finally, I give my conclusions.

### I. ORIGINAL POLICY GOALS OF THE DMCA

To protect copyright owners from the “digital threat,” Congress enacted the DMCA, which created a new cause of action that prohibits unauthorized access to a copyrighted work that is protected by a technological measure. Congress wrote the DMCA in 1998 to implement two treaties adopted by the World Intellectual Property Organization (WIPO): the WIPO Copyright Treaty and the WIPO Phonograms Treaty.<sup>4</sup> These treaties required signing nations to enact laws providing “adequate legal protection and effective legal remedies against the circumvention of effective technological measures in connection with the exercise of their rights.”<sup>5</sup> Existing U.S. copyright laws had already addressed most of the obligations of the WIPO treaty. However, new statutes were needed to implement the protection of the “technological measures” referred to in the treaty language that, in turn, protected copyrighted works. At about the same time, content owners were lobbying Congress for greater protection for their works to counter the “digital threat.”

The content industry's concern over the copying of digital media and the threat it posed to copyright was well-founded, at least in theory. Due to the unique nature of digital content, it can be copied as many times as desired without any loss of quality. The simultaneous rise of the Internet made the transmission of those digital copies cheap, easy, and virtually instantaneous. To the content industry, the combination of the two was frightening. In the past, copyright owners would shut down printing presses to stop illegal copying, countering the infringement one source at a time.

However, this new digital threat was something completely different, more like an infectious disease. One pristine digital copy could be transmitted to another person, that person could copy and transmit, and so on. Very quickly, one infringing copy of a work could become thousands, even millions of infringing copies. Moreover, the strategy of attacking the source was useless against this new digital threat because the sources were distributed throughout the population. A single illegal printing press is

---

4. Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 315–16 (S.D.N.Y. 2000).

5. World Intellectual Property Organization Copyright Treaty, art. 11, Dec. 20, 1996; World Intellectual Property Organization Performances and Phonograms Treaty, art. 18, Dec. 20, 1996.

relatively easy to find, but when the source becomes thousands of personal computers in individual living rooms, the problem becomes too large to attack in the old way.

To rights owners, the only solution was to prevent all unauthorized digital copying completely, locking down digital content using encryption and other technological measures. However, they realized that this protection was highly vulnerable for the same reasons their content was threatened. In a digital future, only one person needs to discover a way to defeat the protection, and then this method can be transmitted rapidly through the Internet. To protect the protection, rights owners convinced Congress that new laws were needed.

To that end, the DMCA added chapter twelve, “Copyright Protection and Management Systems,” to the Copyright Act. Among the provisions is § 1201,<sup>6</sup> which made it illegal to circumvent the technological measures that protect digital content (the anti-circumvention provisions). This section also made it illegal to traffic in devices that accomplish such circumvention (the anti-trafficking provisions). At issue in this paper are the provisions in § 1201(a), which specifically protect “access control” measures, prohibiting both the circumvention of and the trafficking in devices used to circumvent such measures.

The anti-circumvention provision, § 1201(a)(1)(A), provides that no person may “circumvent a technological protection measure” used by the copyright owner which “effectively controls access” to a copyrighted work.<sup>7</sup> As defined in the DMCA, a technological measure effectively controls access to a work “if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.”<sup>8</sup> To circumvent such a technological measure is “to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner.”<sup>9</sup>

The anti-trafficking provision, § 1201(a)(2), prohibits manufacturing, importing, or otherwise trafficking in any means that “is primarily designed . . . for the purpose of circumventing a technological measure that effectively controls access to a work . . . [,] has only limited commercially significant purpose or use other than to circumvent . . . [, or] is marketed . . .

---

6. 17 U.S.C. § 1201 (1998).

7. *Id.* § 1201(a)(1)(A).

8. *Id.* § 1201(a)(3)(B).

9. *Id.* § 1201(a)(3)(A).

for use in circumventing a technological measure.”<sup>10</sup> Violation of this anti-trafficking provision led to the main cause of action in *Chamberlain*. Since its enactment, most DMCA cases dealing with circumvention have been anti-trafficking cases because it is much easier for plaintiffs to target a single device manufacturer or software developer rather than pursue many individual anti-circumvention actions.

Three features of chapter twelve are noteworthy. First, § 1203 created a new civil cause of action—completely separate from actions for infringement elsewhere in the Copyright Act—for “any persons injured by a violation” of §§ 1201 or 1202.<sup>11</sup> Damages can include injunctive relief, impoundment of equipment, actual and statutory damages, costs, and attorney’s fees.<sup>12</sup> Second, § 1204 created a new criminal offense—also separate from criminal offenses for copyright infringement—for willful violations of §§ 1201 or 1202 for the purpose of commercial advantage or private financial gain.<sup>13</sup>

Third, and most importantly, § 1201 only prohibits *unauthorized* access to a work. This is a dispositive issue in *Chamberlain*, and the principle is firmly rooted in DMCA legislative history. As the House Judiciary Committee Report noted, this important distinction prohibits an individual from being able to “circumvent in order to gain unauthorized access to a work, but [an individual] would be able to [circumvent] in order to make fair use of a work which he or she has acquired lawfully.”<sup>14</sup>

By enacting the DMCA § 1201 provisions, Congress intended to be responsive to content owner’s concerns toward the digital threat and protect the walls of encryption protecting their content from unauthorized access. However, they set in motion a divergence between DMCA access protection, traditional copyright protection, and the expectations of consumers. This divergence would be examined in *Chamberlain v. Skylink*.

## II. CHAMBERLAIN I & II

*Chamberlain I* and *II* provided an opportunity for courts to examine the balance between the DMCA’s prohibition of unauthorized access and traditional copyright protection, in light of consumers’ expectations regarding the products they own. Plaintiff Chamberlain manufactured and sold garage doors together with hand-held remote transmitters, or remote controls. In this

---

10. *Id.* § 1201(a)(2)(A)–(C).

11. *Id.* § 1203(a).

12. *Id.* § 1203(b)–(c).

13. *Id.* § 1204(a).

14. H.R. REP. NO. 105-551, pt. 1, at 18 (1998).

case, the technology at issue was the garage door opener (GDO) system.<sup>15</sup> A GDO facilitates the opening of the garage door through an opening device when a user activates the remote transmitter. The opening device is mounted on the door and consists of both a receiver with associated signal processing software and a motor to open and close the door. A homeowner wishing to open or close the garage door activates the remote transmitter, which sends a radio frequency signal to the receiver located on the opening device. Upon receiving a recognized signal from the transmitter, the signal processing software activates the opening device and commands the motor to open or close the door.

In Chamberlain's Security+ line of GDOs, the system uses a copyrighted "rolling code" computer program that, for enhanced security purposes, constantly changes the transmitter signal required to open the door.<sup>16</sup> The remote transmitter is only able to generate a limited number of codes, and Chamberlain was concerned that homeowners with multiple residences may exhaust all the possible codes while out of range of one of the openers and not be able to activate that opener when they return.<sup>17</sup> To prevent this, Chamberlain developed a "resynchronization" sequence, which would activate the door after comparing and calculating two signals sent one after the other in rapid succession.

Competing with Chamberlain, Defendant Skylink manufactured and sold a universal GDO transmitter that could operate Chamberlain's GDO systems.<sup>18</sup> Skylink's Model 39 was designed to interoperate with common GDOs, whether they used a "rolling code" computer program or not.<sup>19</sup> Although Model 39 does not use "rolling code" technology, it is able to simulate the effect of the rolling code. By sending three codes in rapid succession, Skylink's transmitter triggers the resynchronization sequence in Chamberlain's GDO. As a result, one press of the button on a Skylink universal remote transmitter will activate the opening device mounted on Chamberlain's doors.<sup>20</sup>

Chamberlain never explicitly restricted its customers from using other types of remote transmitters with its GDOs.<sup>21</sup> Skylink marketed its Model 39 universal transmitter to consumers either as a replacement for a lost remote

---

15. Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1183 (Fed. Cir. 2004).

16. *Id.*

17. *Id.* at 1184.

18. *Id.*

19. *Id.* at n.3.

20. *Id.* at 1184–85.

21. *Id.* at 1183.

transmitter or as a spare.<sup>22</sup> The Federal Circuit found that Chamberlain and Skylink were the only significant distributors of universal GDO remote transmitters.<sup>23</sup> Further, the court found that “[a]ftermarket consumers have long been able to purchase ‘universal transmitters’ that they can program to interoperate with their GDO system regardless of make or model.”<sup>24</sup>

Chamberlain sued Skylink under the civil cause of action created in § 1203, alleging a violation of the anti-trafficking provision in § 1201(a)(2). Chamberlain argued (1) that its GDO software was a copyrighted work protected by a technological measure and (2) that Skylink’s universal remote transmitter was primarily designed for the purpose of circumventing that technological measure, which effectively controls access to its software.

Chamberlain had registered both the software that controls the opening device and the software that controls its remote transmitter with the Copyright Office.<sup>25</sup> There was some dispute between the parties as to whether the registered software code was exactly the same as used in Chamberlain’s products. However, the court assumed as a matter of law that all the software code in question was protected by copyright, either directly or as a derivative work.<sup>26</sup>

The District Court for the Northern District of Illinois tried the case and issued two separate decisions. In the first decision (*Chamberlain I*), the court denied Chamberlain’s motion for summary judgment on its § 1201(a)(2) claim.<sup>27</sup> The court found a triable dispute of material fact “concerning whether the computer program in Chamberlain’s rolling code is a work protected by copyright and whether the owner of a Chamberlain rolling code GDO is *authorized* to use the Model 39 universal transmitter” (emphasis added).<sup>28</sup>

In the second decision (*Chamberlain II*), which followed shortly thereafter, the court granted Skylink’s motion for summary judgment.<sup>29</sup> The district court rejected Chamberlain’s § 1201(a)(2) claim, holding (1) that Chamberlain had not met the burden of proof for showing that Skylink’s Model 39 transmitter was an “unauthorized” access to Chamberlain’s software and (2) that Chamberlain neither explicitly restricted the ability of

---

22. Chamberlain Grp., Inc. v. Skylink Techs., Inc., 292 F. Supp. 2d 1023, 1030–32 (N.D. Ill. 2003).

23. *Chamberlain*, 381 F.3d at 1183.

24. *Id.*

25. *Id.* at 1185.

26. *Id.*

27. *Chamberlain*, 292 F. Supp. 2d. at 1024–25.

28. *Id.* at 1040.

29. *Id.*

purchasers of its GDOs to buy an “unauthorized” (replacement or spare) transmitter from third parties, nor were purchasers implicitly bound to use only “authorized” devices.<sup>30</sup> The court further maintained that consumers had a reasonable expectation of having the ability to “replace the original product with a competing, universal product without violating federal law.”<sup>31</sup> Chamberlain appealed this second decision before the Federal Circuit in *Chamberlain III*.<sup>32</sup>

In arguments for appeal before the Federal Circuit, Chamberlain argued that the only way for Skylink’s universal remote transmitter to operate Chamberlain’s GDO is by “accessing” copyrighted software through circumvention of its rolling code protection, thereby committing a *per se* violation of § 1201(a)(2).<sup>33</sup> Effectively, Chamberlain was rebutting the holding in *Chamberlain II* by asserting that *all access to a protected work was per se unauthorized by statute*—beyond access by the rights owners’ own system, presumably—and that the issue of implicit or explicit authorization in *Chamberlain I & II* was irrelevant to a § 1201(a) violation. Chamberlain did not allege that Skylink infringed any of its § 106 rights under traditional copyright law, nor did it allege that Skylink contributed to third-party infringement of those rights. Rather, Chamberlain asserted a dangerous new property right, completely detached from the traditional “bundle of rights” in § 106: the right of access.<sup>34</sup>

### III. THE RIGHT OF ACCESS

Misinterpretation of the DMCA threatened to create a dangerous new property right, the right of access, completely detached from the traditional bundle of rights in § 106 of the Copyright Act, resulting in two distinct copyright regimes. To the Federal Circuit, Skylink’s asserted separation—between the traditional protections of copyright and the protection of access in § 1201(a)—would create two distinct copyright regimes.<sup>35</sup> The first, a traditional “protection” regime, would extend only the traditional bundle of rights in § 106 to owners of a copyrighted work protected by a technological measure. These rights would be subject to all the additions, exceptions, and limitations in the rest of the Copyright Act, including the fair use exceptions in § 107. Owners can seek relief through the traditional infringement actions

---

30. *Id.* at 1044–45.

31. *Id.* at 1046.

32. *Chamberlain*, 381 F.3d 1178.

33. *Id.* at 1197.

34. *Id.* at 1199.

35. *Id.*

in Chapter 5 of the Copyright Act, with additional ability to hold traffickers in circumvention devices liable under § 1201(b). These § 1201(b) violations, however, are linked to § 106 rights.<sup>36</sup>

The second, an “access” regime, would extend a new right of access to owners of a copyrighted work protected by a technological measure.<sup>37</sup> This right amounts to a new property right in copyright law and seems to be without limitation. Owners can seek relief through the separate cause of action for § 1201(a) violations. This cause of action is not dependent on any infringement of § 106 rights, as Chamberlain argued before the Federal Circuit.

**Table 1:** Two distinct copyright regimes created by DMCA misinterpretation.

	Protection Regime	Access Regime
<b>Eligible works</b>	Copyrighted works protected by a technological measure	Copyrighted works protected by a technological measure
<b>Rights</b>	Bundle of rights enumerated in § 106, subject to all the additions, exceptions, and limitations in the rest of the Copyright Act	Access right in § 1201(a), a new property right without limitation
<b>Causes of action</b>	Chapter 5 protections against infringement, plus separate cause of action for violation of § 1201(b) linked to infringement of § 106 rights	Separate cause of action for violation of § 1201(a), detached from infringement of § 106 rights

Up to this point, this paper has concentrated on § 1201(a), which prohibits unauthorized access to a copyrighted work protected by a technological measure. There is a companion sub-section, § 1201(b), which prohibits trafficking in devices that circumvent rights, or “copy-control,” technological measures. This provision is only applicable, however, when a technological measure effectively “protects the right of a copyright owner under this title in a work or portion thereof.”<sup>38</sup> Therefore, the protections in § 1201(b) are linked to § 106 rights, and presumably apply after initial lawful access is obtained.<sup>39</sup>

36. *Id.* at 1199–1200.

37. *Id.* at 1200.

38. 17 U.S.C. 1201(b)(1)(A–C).

39. Zohar Efroni, *A Momentary Lapse of Reason: Digital Copyright, the DMCA and a Dose*

One theory of § 1201 interpretation sheds light on this regime split. As described by Zohar Efroni, “access right theory” presumes that Congress intentionally created a new exclusive right to control access to copyrighted works in § 1201(a), while § 1201(b) is intended to protect traditional rights.<sup>40</sup> Liability for violating the right of access is unrelated to, and independent of, copyright infringement liability. As a result, all traditional limitations on copyright infringement liability are not applicable to an access right violation. This is the theory that Skylink used as the basis for its argument in *Chamberlain III*.

This new property right, the right of access, has the following characteristics:<sup>41</sup> (1) the right of access is not codified in § 106 of the Copyright Act, but resides separately in the new Chapter 12; (2) authors must employ technological protection measures within the meaning of the DMCA in order to receive legal protection; (3) the standard for violating the access right is not copyright infringement, but rather circumvention or trafficking in circumvention devices; (4) violation of the access right is a completely independent cause of action; and (5) defendants accused of violating the access right may only assert the special defenses afforded by § 1201.

However, an interpretation of § 1201 by “access right theory” resulting in this new right of access creates a number of serious problems, some of them very dangerous to public policy goals. A key statutory problem is that the access right is inconsistent with a key limitation within the same section, in § 1201(c)(1). That section provides that “nothing . . . shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.”<sup>42</sup> As the Federal Circuit noted, creation of a completely new property right of access would clearly affect rights, limitations, remedies, and defenses in the Copyright Act.<sup>43</sup> The interpretation of a right of access in § 1201(a) flatly contradicts a plain reading of § 1201(c)(1). More importantly, the lack of any relationship between the right of access and traditional copyright allows for distorted applications of § 1201(a) that reach absurd conclusions, which threaten long-standing policy goals of intellectual property and antitrust.

First, access right theory renders § 1201(a) completely blind to the defendant’s intent. An individual could circumvent a technological protection measure that happens to be protecting a copyrighted work, and be liable for

---

of *Common Sense*, 28 COLUM. J.L. & ARTS 249, 285 (2005).

40. *Id.*

41. *Id.* at 294–95.

42. 17 U.S.C. § 1201(c)(1).

43. *Chamberlain*, 381 F.3d at 1200.

violating an access right *regardless of whether the defendant intended to infringe*. The Federal Circuit noted that disabling a burglar alarm in a house with copyrighted books inside would be a per se violation of § 1201(a) under this interpretation.<sup>44</sup> Tort and criminal laws are the proper deterrents for this sort of behavior, not the DMCA. Besides, the law should not be so blind as to permit ridiculous conclusions such as this; silly applications of statutes undermine the social legitimacy that undergirds all laws.

Second, access right theory allows an individual or company to insert a single copyrighted element to its product, protect it with a nominal technological measure, and commit an array of mischief with antitrust and intellectual property policies.<sup>45</sup> From an antitrust standpoint, any company could use the threat of per se § 1201(a) violations to restrict competition by creating aftermarket monopolies in opposition to both antitrust and copyright misuse doctrines. From an intellectual property standpoint, any company could use the right of access to impart patent-like protection to a device, but with a potentially unlimited duration. If the device contains even a single copyrighted element, a “protected” device will have the weight of § 1201(a) protection for a copyright duration. Moreover, there is nothing to prevent the device manufacturer from “refreshing” the copyrighted element periodically, thus potentially extending the duration of protection infinitely. Such device protection is an absurd distortion of copyright doctrine.

This divergence in copyright regimes desperately needed to be addressed by the federal courts, in order to place § 1201 back into harmony with traditional copyright law. In *Chamberlain III*, the Federal Circuit took the challenge.

#### IV. CHAMBERLAIN III: REASONABLE RELATION

In *Chamberlain III*, the Federal Circuit countered the threat of access right theory, adding a new limitation to the scope of § 1201: a reasonable relation between access and the traditional protections of copyright. In deciding *Chamberlain III*, the Federal Circuit could have ignored *Chamberlain*’s right of access argument and simply affirmed *Chamberlain II*, restricting itself to the unauthorized access issue, and it would have reached the same result. Thankfully, the court chose to confront *Chamberlain*’s argument head on. In doing so, the Federal Circuit adopted a theory of § 1201 interpretation that is more internally consistent and is in complete harmony with traditional

---

44. *Id.* at 1201.

45. Heather A. Sapp, Note, *Garage Doors and Toner Cartridges: Why Congress Should Revisit the Anti-Circumvention Provisions of the DMCA*, 3 BUFF. INTELL. PROP. L.J. 135, 146–47 (2006).

copyright law, along with antitrust and intellectual property policy.

An alternative to access rights theory, “ancillary action theory” presumes that Congress merely intended to create an ancillary cause of action to traditional copyright infringement in § 1201(a).<sup>46</sup> Liability under this cause of action is related to traditional copyright infringement because the legislative intent was merely to add statutory protection for the new technological measures that protect copyrighted works against the new “digital threat.” Since no separate right of access is created in § 1201, then liability must be linked to traditional copyright infringement, with all of its traditional exceptions and limitations. This is the theory that the Federal Circuit applied in *Chamberlain III*.

Under this theory, the Federal Circuit held that § 1201 does not create a new property right; rather, it simply provides property owners with new ways to secure their property.<sup>47</sup> While acknowledging that the severance of access from protection is plausible when viewed out of context,<sup>48</sup> such a division would lead to results “so bizarre that Congress could not have intended it.”<sup>49</sup> When viewed in context with the total statutory structure of the Copyright Act, other provisions of the DMCA, and Congressional intent, it becomes clear that the DMCA granted additional legal protections to copyright owners, but did not rescind “the basic bargain granting the public noninfringing and fair uses of copyrighted materials, § 1201(c) . . . .”<sup>50</sup>

In order to correct the misinterpretation of § 1201(a), the Federal Circuit formed a new rule for § 1201(a)(2) violations:

A plaintiff alleging a violation of § 1201(a)(2) must prove: (1) ownership of a valid copyright on a work, (2) effectively controlled by a technological measure, which has been circumvented, (3) that third parties can now access (4) without authorization, in a manner that (5) infringes or facilitates infringing a right protected by the Copyright Act, because of a product that (6) the defendant either (i) designed or produced primarily for circumvention; (ii) made available despite only limited commercial significance other than circumvention; or (iii) marketed for use in circumvention of the controlling technological

---

46. Efroni, *supra* note 39, at 286.

47. *Chamberlain*, 381 F.3d at 1193-94.

48. *Id.* at 1199.

49. *Id.* at 1202 (quoting *Central Bank of Denver, N.A. v. First Interstate Bank of Denver, N.A.*, 511 US 164, 188).

50. *Id.* at 1202.

measure.<sup>51</sup>

A plaintiff must establish the first five elements to prove a prima facie case. A plaintiff need only establish one of the sub-elements in (6) to shift the burden to the defendant. Most importantly, the Federal Circuit elaborated on element (5), holding that a plaintiff must prove a “reasonable relationship” or “nexus” between the alleged access and the traditional copyright owner’s rights.<sup>52</sup>

Using this rule, the Federal Circuit affirmed summary judgment in favor of Skylink. The court held that (1) Chamberlain failed to show a reasonable relationship between Skylink’s access and an infringement of Chamberlain’s copyright, and (2) Chamberlain failed to show that Skylink’s access was not authorized.<sup>53</sup>

The Federal Circuit’s decision changed the application of § 1201 for the better, bringing it into harmony with the rest of copyright law by using the ancillary action theory of interpretation. However, the decision left much ground to cover. For example, how would a plaintiff in future anti-trafficking cases show a reasonable relationship?

#### V. REASONABLE RELATIONSHIP TESTS

Six possible “reasonable relationship” tests give courts a wide range of methods to implement *Chamberlain III*’s new limitation on § 1201(a)(2) violations. To show a prima facie § 1201(a)(2) violation, a plaintiff must show a reasonable relationship between a defendant’s access of the plaintiff’s copyrighted work and the protections that the Copyright Act grants to the plaintiff. Without defining a specific test to apply, however, *Chamberlain III* makes it difficult for others to apply this holding. Zoe Argento proposes six possible “reasonable relationship” tests: (1) but-for causality, (2) reasonable foreseeability, (3) substantial non-infringing use, (4) defendant’s intent, (5) vicarious liability, and (6) the Aimster balancing test.<sup>54</sup>

To help understand the approaches, I will apply each test to the facts in *RealNetworks v. Streambox*.<sup>55</sup> Plaintiff RealNetworks is a software developer that markets a method for content providers to deliver streaming audio and

---

51. *Id.* at 1203.

52. *Chamberlain*, 381 F.3d at 1204.

53. *Id.*

54. Zoe Argento, *Interpreting Chamberlain’s “Reasonable Relation” Between Access and Infringement in the Digital Millenium Copyright Act*, 2008 B.C. INTELL. PROP. & TECH. F. 102902, 15 (November 2008).

55. *RealNetworks, Inc., v. Streambox, Inc.*, No. C9-2070 P, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000).

video to website visitors. Its software only allows customers to stream the content on demand, not download it for later viewing. To protect the content, RealNetworks software utilizes a secret “handshake” between its player (which resides on the user’s computer) and its server (which is operated by the content provider). This secret handshaking protocol ensures that only RealNetworks players can view RealNetworks protected content. Defendant Streambox makes a series of software products that allows users to download RealNetworks content by circumventing the handshaking protocol. RealNetworks sued Streambox, claiming a § 1201(a)(2) anti-trafficking violation. RealNetworks argued that Streambox’s software is primarily designed to circumvent a technological measure (the handshaking protocol) that protects access to a copyrighted work (the copyrighted audio and video). After users of Streambox’s software have downloaded the RealNetworks-protected copyrighted content, it has no further protection against a user’s subsequent infringement by copying, distribution, or preparation of derivative work. For the purposes of this illustration, I will assume that there is evidence that at least some of the Streambox users have illegally copied downloaded content.

#### A. *But-for causality*

The classic but-for test is very simple: but for the action, the result would not have happened. In the case of a § 1201(a)(2) violation, a plaintiff would have to demonstrate that but for the defendant’s circumvention of access, the violation of the copyright owner’s § 106 rights would not have happened. This is an extremely low bar for the plaintiff, and it would be rare to find a case where this test would not be satisfied.

In the *RealNetworks* case, the test would be satisfied. But for the circumvention of the handshake protocol by Streambox’s software, subsequent infringement of the downloaded audio and video would not have happened.

#### B. *Reasonable foreseeability*

This next test introduces a reasonable person element to the analysis: would a reasonable person in a similar situation reasonably foresee the outcome? In the case of a § 1201(a)(2) violation, a plaintiff would have to demonstrate that a reasonable person in similar circumstances as the defendant should have foreseen a violation of the copyright owner’s § 106 rights through use of the circumvention device. This is a higher bar for the plaintiff and involves the very familiar reasonable person element. It has the significant advantage of giving a court the latitude to make an equitable judgment on the facts. However, it also creates a burden on potential

defendants to manage their risk of § 1201 liability by being conscious of the foreseeable infringement potential of their devices.

In the *RealNetworks* case, the test would likely be satisfied. Streambox was a sophisticated software developer, very familiar with RealNetworks' protocols and the reasons for protecting content from download. Moreover, their software also disabled a "copy switch" in the content, allowing the content to be copied. Streambox should have foreseen that users of its software may violate the content provider's § 106 rights. However, if the software developer was much less sophisticated, or if Streambox's software did not disable the "copy switch," then this test might not be satisfied.

### *C. Substantial non-infringing use*

This third test revives and modifies the rule in *Sony v. Universal* (The Betamax case): that a circumvention device is legal if it has a substantial non-infringing use. Previously, the use of this rule for DMCA cases would have been barred because, under the access right theory, legality of the access is tested separately from the infringement. The *Sony* test would have been barred. By bringing the two back together with the ancillary action theory, *Chamberlain III* has potentially revived *Sony's* relevance in DMCA cases. This would be a welcome addition to DMCA law, because the *Sony* court formed the test to balance the rights of copyright owners with the reasonable expectations of consumers, which is exactly what the *Chamberlain* courts were struggling with. The inclusion of this test would give courts a well-understood test to apply in DMCA cases. In the case of a § 1201(a)(2) violation, a plaintiff would have to demonstrate that a circumvention device that could result in infringement of a copyright owner's § 106 rights does not have a substantial non-infringing use.

In the *RealNetworks* case, the test may be satisfied, but would depend heavily on the facts. In *Sony*, VCR users were overwhelmingly using their devices to time-shift, not copy, copyrighted works. In *RealNetworks*, this is not as clear. If RealNetworks could show that a substantial number of Streambox's customers were using its software to illegally copy downloaded content instead of simply time-shifting, the test would likely be satisfied.

### *D. Defendant's intent*

This fourth test is a highly subjective analysis into the defendant's intent in creating the circumvention device: did the defendant create the device with the intention of infringing or facilitating infringement of copyrighted works? This analysis would likely assess the defendant's commercial motive and degree of sophistication. In the case of a § 1201(a)(2) violation, a plaintiff would have to demonstrate that the defendant intentionally created a

circumvention device for the purpose of facilitating a violation of the copyright owner's § 106 rights. Depending on the facts, this could be a difficult bar to meet.

In the *RealNetworks* case, this test is difficult to evaluate because the facts do not address the subjective intent of the Streambox developers. This test could be difficult to meet simply because of evidentiary requirements. To show a prima facie case, plaintiff RealNetworks would have to obtain Streambox internal documents and emails, which would involve extensive discovery. For that reason alone, widespread use of this test would probably cause most § 1201 cases to settle.

#### *E. Vicarious liability*

This fifth test is a bit different from the others, in that it applies to parties other than the creator of the circumvention device. To establish a reasonable relationship to third parties, a plaintiff would have to show that the party was vicariously liable. In the case of a § 1201(a)(2) violation, a plaintiff would have to demonstrate that the defendant either (1) received financial benefit from the creator of the circumvention device or (2) had the right and ability to control the creator's actions. This test would mirror vicarious infringement liability in traditional copyright law, extending the access liability along the same lines of culpability.

In the *RealNetworks* case, this test could apply if the Streambox software was initially created by an employee on his own time and RealNetworks sued the employee. RealNetworks could then sue Streambox under the vicarious liability test. Then RealNetworks would have to show that Streambox either benefited from the employee's circumvention device or had the right and ability to control the employee's actions. This would be another fact-based inquiry involving internal documents.

#### *F. Aimster balancing test*

This final test is based on Judge Posner's proposed balancing test in *In re Aimster*: "If the infringing uses are substantial then to avoid liability as a contributory infringer the provider of the service must show that it would have been disproportionately costly for him to eliminate or at least reduce substantially the infringing uses."<sup>56</sup> Posner's test balances the cost of preventing infringing uses with the amount of damage the infringing uses would cause to copyright owners. In the case of a § 1201(a)(2) violation, a plaintiff would have to demonstrate that the amount of damage sustained by

---

56. *In re: Aimster*, 334 F.3d 643, 653 (7th Cir. 2003).

violation of the copyright owner's § 106 rights is greater than the cost the defendant would have incurred if he would have eliminated all infringing uses of his circumvention device. This test also has roots in the Hand Formula in tort law, which also determines liability by balancing burden of prevention with cost of injury. This would also be a fact-based inquiry, but a more focused one than the test of intent. The inquiry would concentrate economic analysis, which has the possibility of being more objective while still taking the circumstances of the case into account. Like the Hand Formula in tort law, this test causes the court to consider the larger economic issues in DMCA cases.

In the *RealNetworks* case, this test would probably be satisfied. Streambox could have eliminated the substantial infringing uses of its software by keeping the "copy switch" intact. This would have required no cost at all, except that it may have made its products slightly less popular because it would have only enabled time-shifting of content. The substantial costs of the subsequent infringement to the content owners would definitely be greater than the minimal costs for Streambox to keep the "copy switch" intact.

Of the six proposed reasonable relationship tests, the most promising are reasonable foreseeability, substantial non-infringing use, and the *Aimster* balancing test. All three of these tests inject more procedural fairness into § 1201 actions by introducing a sense of reasonableness to the process. In early 2011, however, the Ninth Circuit muddied the appellate waters when it resuscitated access right theory in *MDY Industries*.

#### VI. THE NINTH CIRCUIT TAKES THE OPPOSITE VIEW: MDY INDUSTRIES

In *MDY Indus., LLC v. Blizzard Entm't, Inc.*, the Ninth Circuit declined to follow the Federal Circuit's approach in *Chamberlain III*, holding that the Federal Circuit's decision was (1) contrary to the plain language of § 1201 and (2) overly dependent on policy considerations that are best left to Congress, not the courts.<sup>57</sup> In direct opposition to the Federal Circuit's ancillary action theory, the Ninth Circuit expressly endorsed access rights theory, holding that "§ 1201(a) creates a new anti-circumvention right distinct from the traditional exclusive rights of a copyright owner."<sup>58</sup>

*MDY Industries* involved the Internet-based, massively multiplayer online role-playing game, World of Warcraft (WoW), which is produced by Blizzard Entertainment. In WoW, the players interact in a virtual world, role-playing

---

57. *MDY Indus., LLC v. Blizzard Entm't, Inc.*, No. 09-15932, No. 09-16044, 2011 U.S. App. LEXIS 3428, 46 (9th Cir. Feb. 17, 2011).

58. *MDY Industries*, 2011 U.S. App. LEXIS 3428 at 47.

different characters, such as humans, elves, and dwarves.<sup>59</sup> A player's objective is to advance the character through the game, participating in quests and battling monsters. WoW has over ten million subscribers worldwide, with approximately two and half million in North America.<sup>60</sup> The software for WoW has two components: (1) the game client software that a player installs on the player's computer and (2) the game server software, which the player accesses on a subscription basis by connecting to Blizzard's online servers.<sup>61</sup>

In 2005, a WoW player and software programmer, Michael Donnelly, developed Glider, a software "bot" (short for robot) that automated play of WoW's early levels, for his personal use. Through the use of Glider, Donnelly did not need to actually play the game in order to advance his character through the early stages of the game. Instead, the Glider "bot" would automatically play WoW according to pre-determined parameters while Donnelly was eating dinner or going to a movie, for example.<sup>62</sup> When Donnelly returned, Glider would have amassed experience and treasure for his WoW character, allowing Donnelly to advance to higher levels with little effort. In the summer of 2005, Donnelly began selling Glider to other WoW subscribers through his company, MDY Industries, for fifteen to twenty-five dollars per license.<sup>63</sup>

As a response to WoW players complaining about competing against robots instead of real people, Blizzard banned the use of bots in an updated license agreement.<sup>64</sup> Then, in late 2005, Blizzard created the Warden software, which inspects WoW player actions to detect and banish those using bots to automate WoW characters.<sup>65</sup> Warden was initially very effective at detecting most Glider users and banning them from the game.<sup>66</sup> MDY Industries responded by modifying Glider to avoid detection by Warden, offering it as a premium version on a subscription basis. By late 2008, MDY Industries had gross revenues of \$3.5 million based on 120,000 Glider subscriptions.<sup>67</sup>

In late 2006, Blizzard threatened to sue MDY for copyright infringement; MDY then filed for declaratory judgment, contending that Glider did not

---

59. *Id.* at 3.

60. *Id.*

61. *Id.*

62. *Id.* at 4-5.

63. *Id.* at 5.

64. *Id.* at 5-6.

65. *Id.* at 5.

66. *Id.* at 5-6.

67. *Id.* at 6.

violate any of Blizzard's rights.<sup>68</sup> A series of actions in Arizona District Court followed, culminating in a bench trial in January 2009, in which the court held MDY Industries liable under §§ 1201(a)(2) and (b)(1).<sup>69</sup> MDY Industries appealed to the Ninth Circuit.

In early 2011, the Ninth Circuit found that Warden was a technological measure designed to control access to the WoW game experience. Because Glider was specifically designed to circumvent Warden, MDY Industries was found to be trafficking in a circumvention device prohibited by § 1201. However, the court also held that Glider neither created nor facilitated copyright infringement. While Glider users violated the terms of the Blizzard license, those terms were not related to the protection of Blizzard's copyright.

In assessing Blizzard's § 1201(a)(2) claims, the Ninth Circuit faced a stark choice: it could follow the Federal Circuit's new reasonable relation test from *Chamberlain III*, or it could revert to access rights theory. If the court applied the reasonable relation test, then Blizzard's claim would fail, as the court found that the use of Glider had no relationship at all to copyright infringement.<sup>70</sup> Under all six of the reasonable relation tests proposed *supra*, Blizzard would fail to show a reasonable relation between the use of Glider and traditional copyright infringement because Glider neither created nor facilitated copyright infringement.

Instead, the Ninth Circuit chose to reject the Federal Circuit's reasonable relation test, holding that it is "contrary to the plain language of the statute."<sup>71</sup> The Ninth Circuit was unpersuaded by the Federal Circuit's broad reading of § 1201 in context with traditional copyright law and policy.<sup>72</sup> Rather, the court focused narrowly on the text of the statute and the legislative record to find that Congress intended to create a new "anti-circumvention right," or right of access, distinct from the traditional rights of copyright owners.<sup>73</sup> In contrast with the Federal Circuit's approach, the Ninth Circuit was unwilling to go beyond the bare text of § 1201. In the court's view, adopting a reasonable relation test would override congressional intent and add a "non-textual element" to § 1201.<sup>74</sup>

Therefore, the Ninth Circuit's approach in *MDY Industries* creates a circuit split, as the two appellate court's holdings are completely incompatible with each other. There is no middle ground to be found between the two

---

68. *Id.* at 7-8.

69. *Id.* 8-9.

70. *Id.* at 20.

71. *Id.* at 46.

72. *Id.* at 48.

73. *Id.* at 50.

74. *Id.* at 51-52.

approaches, because *MDY Industries* expressly rejects all of the relevant reasoning in *Chamberlain III*.

#### CONCLUSION

In light of the stark contrast between *MDY Industries* and *Chamberlain III*, the time is now ripe for the Supreme Court to review the competing interpretations of § 1201 and decide which court got it right. In the alternative, Congress could amend § 1201 to clarify if they actually intended to create a distinct right of access, disconnected from traditional copyright law. Just as this article goes to press, Rep. Joe Lofgren has introduced H.R. 1892, the Unlocking Technology Act of 2013, which would effectively resolve this circuit split in favor of the Federal Circuit's interpretation. The bill amends § 1201 to make clear that it is not a violation to circumvent a technological measure if the purpose of the circumvention is to use a work in a manner that is not an infringement of copyright.<sup>75</sup>

In this author's opinion, the Federal Circuit's reasonable relation test in *Chamberlain III* brings § 1201 of the DMCA back in harmony with the rest of the Copyright Act, creates a better balance of interests between copyright owners and the reasonable expectations of consumers, prevents content owners from misusing their limited monopoly under the Copyright Act, and restricts the misuse of copyright for functional applications traditionally protected by patent, such as replacement part markets. For the sake of public policy and common sense, I hope the Supreme Court agrees.

ROBERT ARTHUR\*

---

75. Unlocking Technology Act of 2013, H.R. 1892, 113th Cong. (2013).

\* Juris Doctor, Marquette University Law School, August 2012. Thanks to all of my family, friends, and professors who made law school enjoyable and aided me in the writing of this comment.