



School of Law  
UNIVERSITY OF GEORGIA

Prepare.  
Connect.  
Lead.

Journal of Intellectual Property  
Law

---

Volume 8 | Issue 2

Article 5

---

March 2001

## The Digital Millennium Copyright Act and the First Amendment: Can They Co-exist?

Rachel Simpson Shockley

Follow this and additional works at: <https://digitalcommons.law.uga.edu/jipl>



Part of the [First Amendment Commons](#), and the [Intellectual Property Law Commons](#)

---

### Recommended Citation

Rachel S. Shockley, *The Digital Millennium Copyright Act and the First Amendment: Can They Co-exist?*, 8 J. INTELL. PROP. L. 275 (2001).

Available at: <https://digitalcommons.law.uga.edu/jipl/vol8/iss2/5>

This Notes is brought to you for free and open access by Digital Commons @ University of Georgia School of Law. It has been accepted for inclusion in Journal of Intellectual Property Law by an authorized editor of Digital Commons @ University of Georgia School of Law. [Please share how you have benefited from this access](#) For more information, please contact [tstriepe@uga.edu](mailto:tstriepe@uga.edu).

## THE DIGITAL MILLENNIUM COPYRIGHT ACT AND THE FIRST AMENDMENT: CAN THEY CO-EXIST?

On October 28, 1998, President Clinton signed a piece of legislation into law entitled the "Digital Millennium Copyright Act" ("DMCA" or "Act").<sup>1</sup> The legislation was enacted, among other reasons, to address intellectual property concerns in the digital age. The DMCA addresses the fear of copyright holders that "their works, now available on the Internet in digital form, will be misappropriated."<sup>2</sup> The Act accomplishes this first by making it illegal to "circumvent a technological measure that effectively controls access to a work protected"<sup>3</sup> under the Act. However, it does not stop there. Not only is it illegal to actually "hack around" a protective security measure for the purposes of copying protected works, but it is also illegal to "manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof that . . . is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to" a protected work.<sup>4</sup>

Think about that for a minute. It may sound reasonable at first blush, but when one gets beyond all the technical language, the provision is essentially preventing anyone from telling someone else how to make a copy of a protected work. Essentially, it is illegal for me to tell you how to deactivate a protective measure installed on a copyrighted work. Admittedly, once the information has been passed along, you are armed with knowledge of how to "circumvent" a "technological measure," but so what? Where is the harm? Knowing how to copy and actually copying are two entirely different things. More importantly, doesn't preventing us from telling one another how to make copies present a problem in the face of the First Amendment freedom of speech?

This Note will discuss some of the history and goals of the Digital Millennium Copyright Act, as well as the policy in support of its broad reach. It will then follow the application of the DMCA in the August 2000

---

<sup>1</sup> Carolyn Andrepont, *Digital Millennium Copyright Act: Copyright Protection for the Digital Age*, 9 DEPAUL-LCA J. ART & ENT. L. & POL'Y 397, 398 (1999).

<sup>2</sup> *Id.* at 399.

<sup>3</sup> Copyright Protection and Management Systems, 17 U.S.C. § 1201(a)(1)(A) (Supp. V 1999).

<sup>4</sup> 17 U.S.C. § 1201(a)(2)-(a)(2)(A) (Supp. V 1999).

case *Universal City Studios, Inc. v. Reimerdes*.<sup>5</sup> First, in its discussion of *Reimerdes*, this Note will recount the events giving rise to plaintiff's suit. Then the Note will analyze the court's application of the DMCA to plaintiff's claim. Following that, an effort will be made to determine the constitutional validity of the provision prohibiting the dissemination of information as to how to circumvent technological measures that prevent protected works in light of the First Amendment guarantee of freedom of speech.

It has been clearly recognized by the Supreme Court of the United States that essential economic incentives for creative processes are provided by copyright protection.<sup>6</sup> The Court has stated, "encouragement of individual effort by personal gain is the best way to advance public welfare through the talents of authors and inventors in 'Science and useful Arts.'"<sup>7</sup> It would be difficult for anyone to disagree with the overwhelming importance of copyright protection in achieving an environment which fosters creativity and thereby promotes social and technological advancement in pursuit of a greater good. We are now in the twenty-first century, and the Internet and other technological advances have created a global marketplace for the exchange of ideas and creative works.<sup>8</sup> These advances have created new opportunities "for copyright owners to exploit and benefit from their work."<sup>9</sup> However, along with the benefits that these advancements have bestowed upon copyright holders, there is a tremendous increase in the ease with which protected works can be pirated.<sup>10</sup> This by-product of the Internet and the "information age" resulted in the need to revisit copyright law and update it in an effort to combat these new problems.<sup>11</sup> This update came in the form of the Digital Millennium Copyright Act, which is intended to extend copyright law to provide the necessary tools to protect copyrighted materials in the technologically enhanced marketplace.<sup>12</sup> The question is: has it been expanded too far?

---

<sup>5</sup> *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 55 U.S.P.Q.2d (BNA) 1873 (S.D.N.Y. 2000).

<sup>6</sup> Jo Dale Carothers, Note, *Protection of Intellectual Property on the World Wide Web: Is the Digital Millennium Copyright Act Sufficient?*, 41 ARIZ. L. REV. 937, 946 (1999).

<sup>7</sup> *Id.* at 947.

<sup>8</sup> Andrepont, *supra* note 1, at 397.

<sup>9</sup> *Id.* at 398.

<sup>10</sup> *Id.*

<sup>11</sup> *Id.*

<sup>12</sup> *Id.* at 399.

In the context of this paper, the question of expansion will be limited to an examination of 17 U.S.C. § 1201(a)(2), the provision which makes it illegal to “manufacture, import, offer to the public, provide or otherwise traffic in any technology, product, service, device, component, or part thereof, that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to” a protected work.<sup>13</sup> The broad reach of this provision will become more clear when we turn to its practical application in *Universal City Studios, Inc. v. Reimerdes*.

Before going directly to the case, the policy reasons asserted in support of the broad reach of the Act within the context of the movie industry should be briefly enumerated. Copyright industries are the United States’ most important generator of exports.<sup>14</sup> “The international sale and export of films and videos, literature, music and software, exceeds the export of both automobiles and agricultural products.”<sup>15</sup> Unfortunately, these are the industries most vulnerable to advancing technology. The movie industry is undoubtedly one of the most affected industries.<sup>16</sup> According to the Vice-President of Trade and Federal Affairs for the Motion Picture Association of America (MPAA), the American film industry loses almost \$2.5 billion a year because of inadequate protection available to intellectual property in the face of current technology.<sup>17</sup> Obviously, the concern is that without adequate protection from piracy, the movie industry will experience a severe devaluation, and because the industry is so important to the national economy, the effects would be far reaching.<sup>18</sup>

For years now, the MPAA has made their films available for rental on video cassette. As you are aware, when you make a trip to the movie rental store, more and more films are available both in the old video format as well as on what is called a digital versatile disc, or “DVD.” DVDs were first introduced in the United States in 1996, and currently more than 4,000 films have been released in DVD format, and more are being issued at the rate of

---

<sup>13</sup> 17 U.S.C. § 1201(a)(2)-(a)(2)(A) (Supp. V 1999).

<sup>14</sup> Andrepont, *supra* note 1, at 405.

<sup>15</sup> *Id.*

<sup>16</sup> *Id.*

<sup>17</sup> *Id.*

<sup>18</sup> *Id.* at 407.

over 40 new titles each month.<sup>19</sup> Movies in DVD format are of higher visual and audio quality than videotapes due to their digital encoding.<sup>20</sup>

Digital technology involves the use of computers to encode visual and auditory information so it can be “stored, displayed, transmitted and manipulated.”<sup>21</sup> In addition to providing a higher viewing quality, the digital format allows works to be copied for distribution with greater ease and speed than was possible with video technology.<sup>22</sup> The other key difference between video tapes and DVDs is that the digital format ensures that the first copy is of the exact same quality as the fiftieth copy.<sup>23</sup> This is not the case with video tapes. If you copy a video, the quality diminishes to a great extent with each copy that is made. Since successive copies of DVDs do not experience a reduction in quality, current “electronic information systems make it possible for individuals to deliver perfect copies of digitized works to an infinite number of recipients throughout the world.”<sup>24</sup> This is the crux of the movie industry’s worries.

To aid in the protection of their copyrighted works, motion picture companies, like the plaintiffs in the *Reimerdes* case, “insisted upon the development of an access control and copy prevention system to inhibit the unauthorized reproduction and distribution of motion pictures” before they would release films in the digital format.<sup>25</sup> The “technological measure” that was developed and put into place is called the Content Scramble System, or CSS,<sup>26</sup> which is “an encryption-based security . . . system that requires the use of appropriately configured hardware such as a DVD player or a computer DVD drive to decrypt, unscramble and play back, *but not copy*, motion pictures on DVDs.”<sup>27</sup> In other words, the makers of DVD players buy a license to install a decryption program in the DVD player itself, and that decryption program unscrambles the CSS encryption program so that

---

<sup>19</sup> *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 2d 211, 214, 53 U.S.P.Q.2d (BNA) 1780 (S.D.N.Y. 2000) (citing to the preliminary injunction, not the final adjudication on the merits found at 111 F. Supp. 294. Both the preliminary injunction and the final adjudication will be discussed later in the Note).

<sup>20</sup> *Id.*

<sup>21</sup> *Andrepoint*, *supra* note 1, at 400.

<sup>22</sup> *Id.*

<sup>23</sup> *Id.*

<sup>24</sup> *Id.*

<sup>25</sup> *Reimerdes*, 82 F. Supp. 2d at 214.

<sup>26</sup> *Id.*

<sup>27</sup> *Id.* (emphasis added).

only licensed machines can play back the movies published on DVD. Additionally, the CSS program prohibits copying the material on the DVDs without the aid of a decryption device. The creation of the encryption system was successful in mitigating the movie industry's fears, as "CSS has been licensed to hundreds of DVD player manufacturers and DVD content distributors in the United States and around the world,"<sup>28</sup> and, as mentioned above, films are being marketed at a very fast rate in the digital format.<sup>29</sup>

Unfortunately for those relying on the protection of the Content Scramble System, in late September of 1999, Jon Johansen, a Norwegian teenager who was fifteen years old at the time, and two individuals with whom he had made contact over the Internet, "reverse engineered a licensed DVD player and discovered the CSS encryption algorithm . . ."<sup>30</sup> The three then used this information to create what they cleverly called "DeCSS."<sup>31</sup> DeCSS is a computer program "capable of decrypting or 'ripping' encrypted DVDs, thereby allowing playback on non-compliant computers as well as the copying of decrypted files to computer hard drives."<sup>32</sup> In other words, they had hacked the CSS device. More specifically, to quote the statutory language, they had "circumvent[ed] a technological measure that effectively controls access to a work protected under" the DMCA.<sup>33</sup>

Unfortunately, the three young men didn't stop there. Jon Johansen posted the code to DeCSS on his personal Internet web site and sent out a message to members of an Internet mailing list, informing them that he had done so.<sup>34</sup> Since this initial spreading of the word, "DeCSS has become widely available on the Internet."<sup>35</sup> In fact, "hundreds of sites now purport to offer the software for download."<sup>36</sup> In addition, a few other programs which promise to decrypt CSS-protected DVDs have also appeared on the Internet.<sup>37</sup> In January of 1999, Jon Johansen was prosecuted in Norway for the development of DeCSS.<sup>38</sup> At the time of this writing, the disposition of

---

<sup>28</sup> *Id.*

<sup>29</sup> *Id.*

<sup>30</sup> *Reimerdes*, 111 F. Supp. 2d at 311.

<sup>31</sup> *Id.*

<sup>32</sup> *Id.*

<sup>33</sup> 17 U.S.C. § 1201(a)(1)(A) (Supp. V 1999).

<sup>34</sup> *Reimerdes*, 111 F. Supp. 2d at 311.

<sup>35</sup> *Id.*

<sup>36</sup> *Id.*

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

Johansen's case did not appear on record.<sup>39</sup> It is at this point that we turn to the substance of the *Reimerdes* case, which demonstrates the broad reach of 17 U.S.C. § 1201(a)(2).

Almost immediately following the development and distribution of DeCSS, the Motion Picture Association of America acted under the DMCA and "demand[ed] that Internet service providers remove DeCSS from their servers and, where the identities of the individuals responsible were known, that those individuals stop posting DeCSS."<sup>40</sup> While this action did succeed in removing many of the known DeCSS postings, it did not stop everyone.<sup>41</sup>

The original defendants in *Reimerdes*, Shawn Reimerdes, Roman Kazan, and Eric Coley, a.k.a "Emmanuel Goldstein" (after the leader of the underground in George Orwell's *1984*<sup>42</sup>), are each associated with web sites that began distributing DeCSS, and each one was personally involved in that distribution.<sup>43</sup> Needless to say, Reimerdes, Kazan and Corley did not respond to the Motion Picture Association's demand that they remove DeCSS from their web sites, and the MPAA took legal action under the DMCA alleging violation of the provision prohibiting trafficking in technology which circumvents a technological measure that controls access to copyrighted material, 17 U.S.C. § 1201(a)(2)(A).<sup>44</sup> The Association moved for a preliminary injunction which would stop further dissemination of DeCSS pending resolution of the suit.<sup>45</sup>

### THE PRELIMINARY INJUNCTION

On February 2, 2000, the memorandum opinion granting the preliminary injunction was delivered by Judge Lewis Kaplan of the Southern District of New York.<sup>46</sup> To obtain a preliminary injunction, the moving party must show "(a) irreparable harm, and (b) either (1) a likelihood of success on the merits, or (2) sufficiently serious questions going to the merits to make them fair grounds for litigation and a balance of hardships tipping decidedly in its

---

<sup>39</sup> *Id.*

<sup>40</sup> *Reimerdes*, 82 F. Supp. 2d at 214.

<sup>41</sup> *Id.*

<sup>42</sup> *Id.* at 308.

<sup>43</sup> *Id.* at 214-15.

<sup>44</sup> *Id.* at 215.

<sup>45</sup> *Id.* at 211.

<sup>46</sup> *Reimerdes*, 82 F. Supp. 2d at 211.

favor.”<sup>47</sup> The court, on examining the MPAA’s motion, decided that they met the requirement of irreparable injury.<sup>48</sup> In arriving at this conclusion, the court determined that the fact that the plaintiffs did not allege that defendants had infringed their copyrights, but instead alleged that defendants had facilitated that infringement by offering technology that circumvents plaintiffs’ copyright protection system, was a “distinction without a difference” with respect to the irreparable injury inquiry.<sup>49</sup> The court based this finding on the assertion that “[I]f plaintiffs are correct on the merits, they face substantially the same immediate and irreparable injury from defendants’ posting of DeCSS as they would if defendants were infringing directly.”<sup>50</sup>

With respect to the likelihood of the movant’s success on the merits, the court’s analysis was more detailed. Judge Kaplan found that the “plaintiffs ha[d] an extremely high likelihood of prevailing on the merits”<sup>51</sup> because it is “clear that CSS is a technological measure that effectively controls access to plaintiffs’ copyrighted movies”<sup>52</sup> and “there is no evidence of any commercially significant purpose of DeCSS other than circumvention of CSS . . . .”<sup>53</sup> Having made those findings, the court concluded that the defendants had “likely” violated not only § 1201(a)(2)(A), which prohibits any person from “manufactur[ing], import[ing], offer[ing] to the public, provid[ing] or otherwise traffic[king] in any technology . . . that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access”<sup>54</sup> to a protected work, but § 1201(a)(2)(B) as well. Section 1201(a)(2)(B) prohibits all of the above mentioned activities if the technology “has only limited commercially significant purpose or use other than to circumvent a technological measure” that protects a copyrighted work.<sup>55</sup>

At that point, the defendants’ only hope was to show that their activities fell within one of the exceptions to the DMCA, to show that the DMCA

---

<sup>47</sup> *Id.* at 215.

<sup>48</sup> *Id.*

<sup>49</sup> *Id.*

<sup>50</sup> *Id.* It is necessary for the court to extinguish this distinction because they did not want to address contributory infringement as Congress did not include contributory infringement in the Act.

<sup>51</sup> *Id.* at 217.

<sup>52</sup> *Reimerdes*, 82 F. Supp. 2d at 216.

<sup>53</sup> *Id.* at 217.

<sup>54</sup> 17 U.S.C. § 1201(a)(2)(A) (Supp. V 1999).

<sup>55</sup> § 1201(a)(2)(B).



restricted “fair use” of the copyrighted material, or to show that there was a constitutional impediment to the provisions that they had allegedly violated.<sup>56</sup> The court found that upon this initial review, the defendants’ activities in no way fell within the DMCA exceptions.<sup>57</sup> Additionally, despite the court’s earlier assertion that for the purposes of an immediate and irreparable injury it was a “distinction without a difference”<sup>58</sup> that the defendants were not themselves infringing on the copyright, the court abandoned this reasoning with respect to the fair use argument. Instead, the court stated that defendants were not entitled to a fair use defense as they themselves were not actually infringing on the copyright, only assisting infringement by posting the DeCSS code!<sup>59</sup>

The question of the constitutionality of the Act itself still remained. The “[d]efendants contend[ed] that the DeCSS computer program is protected speech and that the DMCA, at least insofar as it purports to prohibit the dissemination of DeCSS to the public, violates the First Amendment.”<sup>60</sup> As this issue is the crux of this paper, at this time we will simply acknowledge that the Southern District of New York determined for the purposes of the preliminary injunction that it was unlikely that the DMCA was unconstitutional since 1) the broad power given Congress by the Necessary and Proper Clause could be seen to justify the DMCA as an instrument in carrying out the objective of the Copyright Clause<sup>61</sup> and 2) in applying a traditional balancing test between the public interest in the restriction and the public interest in the type of speech at issue, the restrictions provided by the DMCA exist to “‘encourage individual effort by personal gain’ and thereby ‘advance public welfare’ through the ‘promot[ion of] the Progress of Science and useful Arts,’”<sup>62</sup> while the computer code of the type at issue “does little to further traditional First Amendment interests.”<sup>63</sup> Hence, the preliminary injunction was granted.

---

<sup>56</sup> *Reimerdes*, 82 F. Supp. 2d at 217.

<sup>57</sup> *Id.* at 217-19.

<sup>58</sup> *Id.* at 215.

<sup>59</sup> *Id.* at 219.

<sup>60</sup> *Reimerdes*, 82 F. Supp. 2d at 219.

<sup>61</sup> *Id.* at 221.

<sup>62</sup> *Id.* at 222 (quoting *Mazer v. Stein*, 347 U.S. 201, 219 (1954)); U.S. CONST. art. I, § 8, cl. 8.

<sup>63</sup> *Reimerdes*, 82 F. Supp. 2d at 222; Judge Kaplan also found that the defendants’ other attacks on the DMCA, “vagueness” and “overbreadth,” and their attack on the injunction itself, “prior restraint,” would also fail, *see id.* at 223-26.

Following the grant of the preliminary injunction, both Shawn Reimerdes and Roman Kazan settled with the motion picture association, leaving only Eric Corley and his company, 2600 Enterprises, Inc., in the suit.<sup>64</sup> At the conclusion of the preliminary injunction hearing, the plaintiffs attempted to enjoin the defendants from “linking” to other sites that posted DeCSS.<sup>65</sup> “Linking” refers to the ability to jump from one web page or web site to another on the Internet by moving the cursor over the “link” text and pressing the mouse button.<sup>66</sup> It allows for very quick navigation from one web page or site to another. In this case, the plaintiffs had been granted a preliminary injunction which prohibited the defendants from posting the code on their own web sites, but the plaintiffs neglected until the end of the hearing to ask that the defendants be enjoined from providing these easy-access links to other web sites where the code was still available.

Unfortunately for the MPAA, the court did not enjoin the defendants from linking to sites still offering copies of the DeCSS code.<sup>67</sup> Because of this, in an act which Eric Corley termed one of “electronic civil disobedience,” his web site continued to support links to web sites that still offered DeCSS.<sup>68</sup> His web site proclaimed: “ ‘We have to face the possibility that we could be forced into submission. For that reason it’s especially important that as many of you as possible, all throughout the world, take a stand and mirror [copy] these files.’ ”<sup>69</sup> Bad attitude? Probably. Within his rights? I think so. At this point, we will turn to the main opinion in the case.

AUGUST 17, 2000 DECISION OF THE SOUTHERN DISTRICT OF  
NEW YORK IN *UNIVERSAL CITY STUDIOS, INC. V. REIMERDES*

Before moving to the arguments presented and the decisions made in the case, it will be helpful and important for our understanding to review the provisions of the DMCA which will be relevant to this discussion. As mentioned above, the provision which this case centers upon is 17 U.S.C. § 1201(a)(2). For the purposes of this paper, the arguments and defenses surrounding § 1201(a)(2)(A) will constitute the majority of the discussion,

---

<sup>64</sup> *Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 312 n.91.

<sup>65</sup> *Id.* at 312.

<sup>66</sup> *Id.* at 324.

<sup>67</sup> *Id.* at 312.

<sup>68</sup> *Id.*

<sup>69</sup> *Reimerdes*, 111 F. Supp. 2d at 313.

but it is helpful to be familiar with § 1201(a)(2)(B) and § 1201(a)(2)(C) as well, as there were arguments we will touch on briefly that were asserted based on these provisions.

To review: Section 1201(a)(2) of the Digital Millennium Copyright Act provides for the following:

No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology . . . that—(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title; (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title [17 U.S.C.A. § 1 et seq.]; or (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.<sup>70</sup>

The first obvious question is, does DeCSS qualify as “technology” which “circumvent[s] a technological measure that effectively controls access”<sup>71</sup> to a protected set? The court tells us that computer code is “unquestionably . . . ‘technology’ within the meaning of the statute.”<sup>72</sup> Since the statutory definition of “circumvent a technological measure” includes “descrambl[ing] a scrambled work, [or] . . . decrypt[ing] an encrypted work,”<sup>73</sup> it is clear that DeCSS, which decrypts, or “rips” DVDs encrypted with the Content Scramble System thereby allowing the DVDs to be copied,<sup>74</sup> is exactly what the statute is designed to prevent. Therefore, as long as the Content Scramble System (CSS) itself is a “technological measure [designed to] ‘effectively control access to a [protected] work,’” the defendants will have violated the DMCA.<sup>75</sup> To answer this question, the court looks not only to

---

<sup>70</sup> 17 U.S.C. § 1201(a)(2) (Supp. V 1999).

<sup>71</sup> 17 U.S.C. § 1201(a)(2)(A) (Supp. V 1999).

<sup>72</sup> *Reimerdes*, 111 F. Supp. 2d at 317.

<sup>73</sup> 17 U.S.C. § 1201(a)(3)(A) (Supp. V 1999).

<sup>74</sup> *Reimerdes*, 111 F. Supp. 2d at 317.

<sup>75</sup> *Id.*

the statutory language defining “effectively controls access to a work,” but also to the legislative history of the DMCA.<sup>76</sup>

The statute itself tells us that “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>77</sup> The court goes through the technical application of CSS and determines that since one cannot gain access to a CSS-protected work without three keys that are required by the software, and those keys can only be lawfully acquired by entering into a license agreement under authority of the copyright holder or by purchasing a licensed DVD player, “under the express terms of the statute, CSS ‘effectively controls access’ to copyrighted DVD movies.”<sup>78</sup>

In response to the defendants’ argument that CSS obviously did not “effectively” control access to copyrighted works since a method to circumvent it had been created, the court pointed to the legislative history of the statute where the House Commerce Committee made it clear that “measures based on encryption or scrambling ‘effectively control’ access to copyrighted works, although it is well known that what may be encrypted or scrambled often may be decrypted or unscrambled.”<sup>79</sup> Additionally, the defendants’ interpretation of the statute would inexplicably limit the statute’s protection to those works which were completely protected and give no protection to those measures which were vulnerable to being circumvented.<sup>80</sup> Clearly, this is nonsensical. It is pretty clear at this point that, as written, the DMCA without question renders the defendants’ conduct unlawful. There can be no doubt that the posting of the DeCSS code on Eric Corley’s website is “offer[ing] to the public, provid[ing], or otherwise traffic[king] in . . . technology . . . that—(A) is primarily designed or produced for the purpose of circumventing a technological measure [CSS] that effectively controls access to” a protected work.<sup>81</sup> So, since the court seems to have this correct, unless the defendants can convince the court that their actions fall within the statute’s stated and implied exceptions or a traditional fair use exception, or

---

<sup>76</sup> *Id.* at 318.

<sup>77</sup> 17 U.S.C. § 1201(a)(3)(B) (Supp. V 1999).

<sup>78</sup> *Reimerdes*, 111 F. Supp. 2d at 317-18.

<sup>79</sup> *Id.*

<sup>80</sup> *Id.* at 318.

<sup>81</sup> 17 U.S.C. § 1201(a)(2)(A) (Supp. V 1999).

unless they can show that the statute itself is constitutionally unsound, they will be, and should be under this law as written, enjoined. First, we will examine the defendants' attempts to squeeze themselves into available exceptions, and then we will turn to the constitutional defenses and issues presented by this case.

First, the defendants insisted that DeCSS was not created for the purpose of pirating copyrighted motion pictures from DVDs.<sup>82</sup> In other words, it is not technology "primarily designed or produced for the purpose" of circumventing a copyright protection measure. They support this argument with the testimony of the developer, Jon Johansen, who testified that he created DeCSS in order to make a DVD player that would operate on a computer running an operating system called "Linux."<sup>83</sup> An "operating system is a software program that . . . supports the functions of software programs called 'applications' that perform specific user-oriented tasks."<sup>84</sup> CSS, among other things, prohibits CSS-encrypted DVDs from being played back on non-compliant computers, computers that do not have a certain operating system.<sup>85</sup> Windows, by Microsoft, is the most commonly used operating system in the United States<sup>86</sup> and is a compliant operating system, while Linux, at the time DeCSS was created, was not.<sup>87</sup> So, Johansen insisted that he was just trying to develop a way to play DVDs on a different operating system.

First of all, the court did not credit Johansen's testimony,<sup>88</sup> and second, it defeated the argument by pointing out that the reason why DeCSS was developed is unrelated and immaterial to whether or not the defendants before this court violated the anti-trafficking provision of the DMCA.<sup>89</sup> Since Jon Johansen was not a defendant in this case, his motivations for developing DeCSS were irrelevant.

The defendants then tried to fit themselves inside the explicit statutory exceptions for "reverse engineering,"<sup>90</sup> "encryption research,"<sup>91</sup> and "security

---

<sup>82</sup> *Reimerdes*, 111 F. Supp. 2d at 316.

<sup>83</sup> *Id.* at 305.

<sup>84</sup> *Id.*

<sup>85</sup> *Id.* at 303.

<sup>86</sup> *Id.* at 305.

<sup>87</sup> *Id.*

<sup>88</sup> *Reimerdes*, 111 F. Supp. 2d at 320.

<sup>89</sup> *Id.* at 338.

<sup>90</sup> 17 U.S.C. § 1201(f) (Supp. V 1999).

<sup>91</sup> 17 U.S.C. § 1201(g) (Supp. V 1999).

testing.<sup>92</sup> With respect to the reverse engineering exception, the statute provides that a person who has

lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability<sup>93</sup> of an independently created computer program with other programs . . . to the extent any such acts of identification and analysis do not constitute infringement under this title.<sup>94</sup>

Additionally, the dissemination of the technology used to circumvent a measure such as CSS would be permitted if it was “solely for the purpose” of achieving interoperability with an independently created computer program.<sup>95</sup> In this case, the defendants argued that they were just disseminating the DeCSS information so that DVDs could be interoperable with Linux systems.

The court first points out that the defendants were not the authors of DeCSS; they had not done any reverse engineering.<sup>96</sup> Instead, they simply copied the DeCSS code and posted it on their website for public access.<sup>97</sup> Additionally, as mentioned above, the court did not believe the author Johansen’s testimony that he had created the program for the “sole purpose” of creating a Linux DVD player.<sup>98</sup> (This would be an example of interoperability). Instead, the court found that both the defendants and the developer knew that the DeCSS program was developed on and runs on a Windows operating system, and therefore could be used to decrypt and copy CSS-protected DVDs on both Windows and Linux machines. It seems that

---

<sup>92</sup> 17 U.S.C. § 1201(j) (Supp. V 1999).

<sup>93</sup> “[T]he term ‘interoperability’ means the ability of computer programs to exchange information, and . . . mutually . . . use the information which has been exchanged.” 17 U.S.C. § 1201(f)(4) (Supp. V 1999).

<sup>94</sup> 17 U.S.C. § 1201(f)(1) (Supp. V 1999).

<sup>95</sup> 17 U.S.C. § 1201(f)(3) (Supp. V 1999).

<sup>96</sup> *Reimerdes*, 111 F. Supp. 2d at 320.

<sup>97</sup> *Id.*

<sup>98</sup> *Id.* at 311.

the court is correct in dismissing this defense as well, especially when we remember the proclamation made by the defendants on their website with regard to copying DeCSS: “[It is] especially important that as many of you as possible, all throughout the world, take a stand and mirror [copy] these files.”<sup>99</sup> This statement hardly seems the statement of someone who just wants to let those few individuals who happen to have Linux operating systems to be able to playback rented DVDs!

With respect to the “encryption research” exception, it is not a violation of the DMCA for an individual who is involved in “good faith encryption research” to develop means to circumvent protective technology, if 1) the person has lawfully obtained the encrypted copy of the work, 2) the act is necessary to conduct the encryption research, and 3) a good faith effort has been made to obtain authorization from the copyright owner before developing and executing the circumvention.<sup>100</sup> To determine if an individual is engaged in good faith encryption research,

the Court is instructed to consider factors including whether the results of the putative encryption research are disseminated in a manner designed to advance the state of knowledge of encryption technology versus facilitation of copyright infringement, whether the person in question is engaged in legitimate study of or work in encryption, and whether the results of the research are communicated in a timely fashion to the copyright owner.<sup>101</sup>

It would be difficult to disagree with the court’s finding that the defendants were not in any way involved in “good faith” encryption research as defined by the statute. They posted the DeCSS code for all the world to use; they did not make any effort to inform the copyright owners of the results of DeCSS development, and they made no effort to gain authorization from the copyright owners to do the research in the first place.<sup>102</sup> Additionally, though not specifically mentioned by the court in this instance, the

---

<sup>99</sup> *Id.* at 313.

<sup>100</sup> 17 U.S.C. § 1201(g) (Supp. V 1999).

<sup>101</sup> *Reimerdes*, 111 F. Supp. 2d at 321.

<sup>102</sup> *Id.*

defendants were not involved in encryption research at all, good faith or otherwise; they simply disseminated the information.

The third explicit exception the defendants attempted to fall within was that of “security testing,” which allows an individual to assess a computer, computer system, or computer network, solely for the purpose of a good faith investigation or to correct a security flaw or vulnerability, all done with the authorization of the owner of the computer system or network.<sup>103</sup> The court in this instance also arrives at the only possible correct conclusion. There is no evidence whatsoever that DeCSS has anything to do with testing computers, computer systems, or networks, let alone the absence of any sort of authorization for such testing.<sup>104</sup>

Finally, the court addresses the defendants’ argument that their activities were permitted under the fair use doctrine. This doctrine, “limits the exclusive rights of a copyright holder by permitting others to make limited use of portions of the copyrighted work, for appropriate purposes, free of liability for copyright infringement.”<sup>105</sup> The traditional value of the doctrine has been that it facilitates literary and artistic criticism, teaching and scholarship, or other socially useful forms of expression, by allowing one other than the person who holds the copyright to reprint or quote the copyrighted work in certain circumstances.<sup>106</sup> It has been viewed as the “safety valve that accommodates the exclusive rights conferred by copyright with the freedom of expression guaranteed by the First Amendment.”<sup>107</sup> The defendants argue that “the DMCA cannot properly be construed to make it difficult or impossible to make any fair use of plaintiffs’ copyrighted works and that the statute therefore does not reach their activities, which are simply a means to enable users of DeCSS to make such fair uses.”<sup>108</sup>

Once again, as in the preliminary injunction, the court makes the distinction that the defendants here are not accused of infringement; they are accused of trafficking in the technology that allows circumvention of copyright protection measures.<sup>109</sup> Additionally, the court points to legislative history, which demonstrates that the decision not to have fair use

---

<sup>103</sup> 17 U.S.C. § 1201(j) (Supp. V 1999).

<sup>104</sup> *Reimerdes*, 111 F. Supp. 2d at 321.

<sup>105</sup> *Id.*

<sup>106</sup> *Id.*

<sup>107</sup> *Id.* at 322.

<sup>108</sup> *Id.*

<sup>109</sup> *Id.* at 322.



as a defense to a claim under § 1201(a) was intentional.<sup>110</sup> Those two findings legitimize the court's conclusion to disregard the fair use defense. Additionally, the court later points out the fact that not being able to copy a DVD does not put a very meaningful restriction on fair use of the copyrighted material.<sup>111</sup> All types of fair use would necessarily involve one or more of the following: "1) quotation of the words of the script, 2) listening to the recorded sound track, including both verbal and non-verbal elements, and 3) viewing of the graphic images."<sup>112</sup> All of these types of use can be accomplished without copying a DVD. For example, most movies available on DVD are also available on videocassette, which can be rented and, with permission, can be easily copied if copying from a DVD is impossible without a decryption code.<sup>113</sup> Additionally, anyone needing to quote language from a DVD could simply rent or purchase the DVD and write the language down, giving credit to the authors.<sup>114</sup> Accordingly, up to this point, it does not seem that an error was made by the Southern District of New York in its interpretation of the DMCA and its application to this case. As the DMCA is written, it seems very clear that the defendants are in violation of the Act. But is the Act written correctly? Is it constitutional? As we turn to the constitutional defense presented by the defendants, it is less certain that the court has reached the correct conclusion.

In what appears to be their most viable defense, the defendants assert that the DMCA, at least as it applies to the public dissemination of the DeCSS computer code, violates the First Amendment to the Constitution.<sup>115</sup> They claim that the violation occurs in two ways. First, defendants argue that computer code is protected speech. Therefore, the DMCA's prohibition of dissemination of the DeCSS computer code violates their First Amendment rights.<sup>116</sup> Secondly, they argue that the DMCA is unconstitutionally overbroad because of the prevention of fair use of the encrypted works, and because it is vague.<sup>117</sup> This Note will focus on the defendants' contentions regarding the First Amendment, and will touch on the fair use issue.

---

<sup>110</sup> *Reimerdes*, 111 F. Supp. 2d at 324.

<sup>111</sup> *Id.* at 337-38.

<sup>112</sup> *Id.* at 337.

<sup>113</sup> *Id.*

<sup>114</sup> *Id.* at 338.

<sup>115</sup> *Id.* at 325.

<sup>116</sup> *Reimerdes*, 111 F. Supp. 2d at 325.

<sup>117</sup> *Id.* at 325-26.

The court begins its analysis by examining the defendants' claim that computer code is speech and therefore protected by the First Amendment. The court is willing to accept that computer code is speech in the sense that it is "expressive," stating, "All modes by which ideas may be expressed or, perhaps, emotions evoked—including speech, books, movies, art, and music—are within the area of First Amendment concern. As computer code . . . is a means of expressing ideas, the First Amendment must be considered before its dissemination may be prohibited or regulated."<sup>118</sup> However, the court goes on to point out that the "long history of First Amendment jurisprudence makes equally clear that the fact that words, symbols and even actions convey ideas and evoke emotions does not inevitably place them beyond the power of government."<sup>119</sup> Then the court states that the regulation of different types or categories of expression is subject to varying levels of judicial scrutiny.<sup>120</sup>

In broad terms, the restrictions on expression fall into two main categories: content-based restrictions and content-neutral restrictions.<sup>121</sup> Content-based restrictions are "restrictions on the voicing of particular ideas," while content-neutral restrictions have "nothing to do with the content of the expression," but instead have an "incidental effect of limiting expression."<sup>122</sup> Generally, the "government has no power to restrict expression because of its message, its ideas, its subject matter, or its content."<sup>123</sup> Consequently, content-based restrictions are subject to strict scrutiny and "permissible only if they serve compelling state interests by the least restrictive means available."<sup>124</sup> The court then suggests that content-neutral restrictions are examined with a less exacting standard.<sup>125</sup> This is the rule according to case law cited by the court because "restrictions of this type are not motivated by a desire to limit the message, [and therefore] they will be upheld if they serve a substantial governmental interest and restrict First Amendment freedoms no more than necessary."<sup>126</sup>

---

<sup>118</sup> *Id.* at 327.

<sup>119</sup> *Id.*

<sup>120</sup> *Id.*

<sup>121</sup> *Id.* at 327.

<sup>122</sup> *Reimerdes*, 111 F. Supp. 2d at 327.

<sup>123</sup> *Id.* at 327 (quoting *Police Dept. of City of Chicago v. Mosley*, 408 U.S. 92, 95-96 (1972)).

<sup>124</sup> *Id.*

<sup>125</sup> *Id.*

<sup>126</sup> *Id.* at 327-28 (citing *Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 662 (1994) and *United States v. O'Brien*, 391 U.S. 367, 377 (1968)).

Clearly, to make its job easier, the court wishes to find that the DMCA, as it restricts the dissemination of the computer code DeCSS, is a content-neutral restriction and therefore subject to a less strict standard of scrutiny with respect to the First Amendment. To have the DMCA labeled “content-neutral,” the court must show, according to its own definition, that the restriction has “nothing to do with the content of the expression” and that any limitation on expression is incidental.<sup>127</sup> If the court decides that the restriction is content-neutral, the standard to be applied with respect to the First Amendment, as reiterated above, is that a substantial governmental interest is served by the restriction and it “restrict[s] First Amendment freedoms *no more than necessary*.”<sup>128</sup>

Obviously, the court determines that the DMCA is a content-neutral restriction. It does so by quoting *Ward v. Rock Against Racism*, stating, “the principal inquiry in determining content neutrality . . . is whether the government has adopted a regulation of speech because of [agreement or] disagreement with the message it conveys,”<sup>129</sup> and then concluding that it is not the “message” that is harmful here, but the “distinctly functional” aspect of the code, which as a “series of instructions,” causes the computer to perform a particular task.<sup>130</sup> The court continues to attempt to separate out expression and functionality, stating, “[t]he reason that Congress enacted the anti-trafficking provision of the DMCA had *nothing to do* with suppressing particular ideas of computer programmers and everything to do with functionality.”<sup>131</sup> With this language (“nothing to do with suppressing . . . ideas”), the court attempts to trick us into thinking they have met the definition of content neutral, but the argument is empty, and it fails.

Why does the court’s argument fail? The court accepts that computer code is speech.<sup>132</sup> How can expression and functionality be separated? Speech is expressive and functional all at once. Why would anyone speak if not to achieve some function? The function of fictional literature is to explore human crisis and make the reader feel things and understand things that may not be readily available to her in her small part of the world. The function of non-fiction is to teach, to explain our origins, to understand our

---

<sup>127</sup> *Reimerdes*, 111 F. Supp. 2d at 327.

<sup>128</sup> *Id.* at 328 (emphasis added).

<sup>129</sup> *Id.* (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989)).

<sup>130</sup> *Reimerdes*, 111 F. Supp. 2d at 328-29.

<sup>131</sup> *Id.* at 329 (emphasis added).

<sup>132</sup> *Id.* at 326.

biology, to relive our history, to figure out what motivates us. The function of persuasive speech is to persuade, whether it be who to vote for, what product to buy, or what god in which to believe. If we accept that computer code is speech, it is both expressive and functional. It expresses instructions to a computer. Function cannot be separated from expression.

It is easy to see the absurdity of the court's suggestion that some speech is "functional" while other speech is "expressive" when we ask ourselves why anyone would ever write a book, give a speech, or even talk to their neighbor if there was no purpose, or function? Even mindless banter with an acquaintance over lunch serves the function of building community and friendship. Functionality is inherent in any expression; it simply cannot be separated out. If you remove function, you have evaporated expression. We can't buy the court's empty language here. It doesn't give us any reason to understand function as separable from expression other than just telling us that is the case. What does the court think it is disagreeing with if not the ideas and expressions of the programmers? It disagrees with the message conveyed. It disagrees with the *function* of the message conveyed. The two are one and the same.

The court acknowledges the argument of Lee Tien, a commentator who suggests that "functionality" is a "proxy for effects or harm."<sup>133</sup> The court agrees that this may be true, but states that it is incorrect to assume that "the chain of causation is too attenuated to justify the use of functionality to determine the level of scrutiny."<sup>134</sup> Both assumptions are wrong as they are based upon the faulty premise that functionality can be separated from speech and expression. Because the two are inseparable, it is clear that this is a content-based restriction, and therefore should be subject to strict scrutiny under First Amendment doctrine, rendering the restriction permissible by the court's own terms *only* if compelling state interests are being served by the *least restrictive means available*.<sup>135</sup>

It is clear that the anti-trafficking provision of the Act infringes on the First Amendment rights of the defendants by prohibiting them from posting the DeCSS computer code on their Web sites. Clearly, the Act is prohibiting the defendants from sharing the ideas and expressions of the computer

---

<sup>133</sup> *Id.* at 331 (quoting Lee Tien, *Publishing Software as a Speech Act*, 15 BERKELEY TECH. L.J. 629, 695 (2000)).

<sup>134</sup> *Reimerdes*, 111 F. Supp. 2d at 331.

<sup>135</sup> *Id.* at 327.

programmers, *i.e.* the DeCSS code. The Act is restricting their freedom of speech. The court, having determined that the provision is “content neutral” rather than “content based,” now launches into an extended discussion of the harmful “function” of the code, assuming incorrectly that it is capable of limiting its attack to “function” at the exclusion of “expression.”<sup>136</sup> As it has been shown that this is not a viable argument, we will set that aspect of the court’s discussion aside and focus on the court’s attempt to establish a state interest in retaining the protection provided by the anti-trafficking provision.

The discussion begins with the court suggesting that while there was a time when copyright infringement could be adequately dealt with by locating and prosecuting the infringer himself or herself, that is no longer the case.<sup>137</sup> The example is given of making and selling unauthorized copies of a copyrighted book. The copyright holder, once made aware of the unauthorized copies, could trace the copies to the owner of the printing press responsible and cut off the infringement at the source.<sup>138</sup> The court then asserts, and no doubt correctly so, that the digital world presents some different problems for the copyright holders of digitized works since the copies made of the works can be sent almost instantly all over the world, and each recipient can then send the works out again, resulting in an exponential rather than linear explosion of the unauthorized copies of the works.<sup>139</sup> Because of this phenomenon, the old solution of locating the original source of the infringement and cutting it off is no longer an effective remedy to the situation, according to the court.<sup>140</sup>

To help explain this situation, the court uses an elaborate metaphor likening the infringement of copyright to a disease. In a common-source epidemic, where members of the population contract a non-contagious disease from a source such as a contaminated well, the disease stops spreading once the well is closed off.<sup>141</sup> This is, of course, the printing press example of yesteryear; once we stop the printing press owner from copying the books, we have eliminated the source of the disease.<sup>142</sup> On the other hand, if there is a contagious disease, the disease will spread from person to person,

---

<sup>136</sup> *Id.* at 330.

<sup>137</sup> *Id.* at 331.

<sup>138</sup> *Id.*

<sup>139</sup> *Id.* at 331.

<sup>140</sup> *Reimerdes*, 111 F. Supp. 2d at 331-32.

<sup>141</sup> *Id.* at 332.

<sup>142</sup> *Id.*

and eliminating the initial source of the infection does not end the spreading of the disease, or in our case, the infringement of the copyright.<sup>143</sup>

The court suggests that the metaphor breaks down principally at what it refers to as the “final point.”<sup>144</sup> This “break down” refers to the fact that

“[i]ndividuals infected with a real disease become sick, usually are driven by obvious self-interest to seek medical attention, and are cured of the disease if medical science is capable of doing so.”<sup>145</sup> The difference with this situation, according to the court, is that [i]ndividuals infected with the ‘disease’ of capability of circumventing measures controlling access to copyrighted works in digital form, however, do not suffer from having that ability. They cannot be relied upon to identify themselves to those seeking to control the “disease.” And their self-interest will motivate some to misuse the capability, a misuse that; [sic] in practical terms, often will be untraceable.<sup>146</sup>

While this metaphor and its “break down” may appear accurate at first blush, when examined closely, there are several problems with the court’s analysis. First, the court begins by equating the actual infringement of a copyright with the contagious disease, then quickly changes to speaking of the “capability of circumventing measures controlling access to copyrighted works in digital form” as the “disease.”<sup>147</sup> This is obviously a problem when we remember that while it is wrong to *actually infringe* on a copyright, there is absolutely nothing wrong with *knowing how to infringe* on a copyright. I know how to buy a copy machine and some paper and copy John Grisham’s latest novel a thousand times and turn around and sell it at half of what the bookstores are offering. I know how to take the copyrighted pictures that the professional photographer took at my wedding and copy them all day long on a Kodak laser printer for much cheaper than it would be to order them all from him. Indeed, after writing this Note, I know how

---

<sup>143</sup> *Id.*

<sup>144</sup> *Id.*

<sup>145</sup> *Reimerdes*, 111 F. Supp. at 332.

<sup>146</sup> *Id.*

<sup>147</sup> *Id.*

to download DeCSS and copy DVDs to my heart's content. The point is, I don't do any of these things, and the fact that I know how to do them is irrelevant to any discussion of actual infringement; it is not a harm to the holder of a copyright or a wrong with respect to copyright law to carry around that knowledge. We cannot punish people for knowing how to infringe on a copyright, and we should not be able to punish people for telling others how to infringe on a copyright; no wrong has been committed at that point. We need to focus on the infringers themselves. The individuals who have actually *used* the knowledge of how to infringe on copyrighted material should be punished.

The court would no doubt respond to that argument by suggesting that, with the book copying or laser copying of the photographs, it would be easy to locate who was actually doing the infringing, and once the original infringer was located and stopped, the infringement would end.<sup>148</sup> I do not know if that is actually true, considering that, as soon as one person bought a Xeroxed copy of the John Grisham novel, they could themselves copy it a thousand times, as could any of the other purchasers. Xerox machines are just not that hard to come by. I will admit that it would be more difficult for the infringers themselves, as it is a more cumbersome undertaking to make Xerox copies than copies of a digital file.

So, for the sake of the discussion, we will examine the court's argument that it would be easy to stop these other types of infringement and impossible to stop the copying of digital copyrighted works. As we mentioned above, the court believes that those individuals who have the ability to circumvent technological copyright protection measures are not going to identify themselves because it is not in their self-interest to do so.<sup>149</sup> My response is, why should they reveal themselves? Have my confessions above that I *know how* to infringe on various copyrights done anyone any good in the quest to stop copyright infringement? For argument's sake, let's assume that not everyone who has the knowledge of how to copy DVDs is as honest as I am; is that enough for us to throw the First Amendment out the window? I do not think so. The anti-trafficking provision simply does not meet the strict requirement of being the least restrictive means available<sup>150</sup> to serve the state interest in copyright protections. The court seems to just

---

<sup>148</sup> *Id.* at 332.

<sup>149</sup> *Id.*

<sup>150</sup> *Id.* at 327.

throw up its hands and toss out the First Amendment in the face of the “untraceable” nature of digital copyright infringement. I think they were a little too hasty. It seems that there are other options which would not infringe so greatly on First Amendment freedoms and yet still further and protect state interests.

One of the court’s main concerns is that there is no way to stop the infringement at the source, so their answer is to suppress the communication of the method of infringement. My suggestion to answer that concern is to at least explore the option of stopping it at its source.

I am not a computer programmer. The extent of my knowledge with respect to DVDs and DeCSS has been revealed in this Note. However, there are plenty of people, as is evidenced by the terror the court feels at the prospect of allowing communication between them, who are very well-versed in all the ins and outs of computer programming and digital code. These are the same people that came to the aid of the movie industry in the early 1990s when the movie companies feared placing DVDs on the market for home viewing because of the potential for copying them.<sup>151</sup> In the early 1990s, these computer programmers came up with the Content Scramble System to help allay the movie industry’s fears.<sup>152</sup> As I said, I am not a computer programmer, but just off the top of my head I can think of several things the movie industry could try before we disregard the First Amendment.

First, why not install something on DVDs that destroys the original when anyone attempts to copy it? That way, if I rent a DVD from the movie store and attempt to copy it, as soon as I begin the process, the original DVD is wiped out. Then when I get back to the store and attempt to turn the DVD in, store personnel could check the DVD for damage. If the DVD is destroyed, you just located the elusive “original source,” and action can be taken against a person who actually attempted to infringe on a copyright, not just someone who possessed the knowledge of how to infringe on a copyright and shared that information with someone else. Additionally, any “exponential” increase in the spreading of the ability to copy the movie would be eliminated as the movie would have been destroyed and unavailable for copying and/or posting on the Internet.

---

<sup>151</sup> *Reimerdes*, 82 F. Supp. 2d at 314.

<sup>152</sup> *Id.*



Another suggestion would be to make it more difficult for infringers by creating several different content scrambler systems that could be installed at random on DVDs so that the individual attempting to copy the digital file would have to search for and try many different decryption devices in an effort to copy any protected material. With this suggestion, the copying could still be accomplished, but the court emphasizes the ease and quickness with which DVDs can be copied in comparison to books (this is debatable with respect to the time factor, as a courtroom demonstration indicated that it would take approximately six hours to exchange decrypted movies with another individual over the Internet<sup>153</sup>). Perhaps if it were more of an ordeal, if it took more time and effort to copy the works, we could eliminate much of the infringement.

The court does acknowledge the possibility of developing new technology to protect against piracy, but dismisses it saying, "development and implementation of a new DVD copy protection system is . . . difficult and costly . . . and may carry with it the added problem of rendering the existing installed base of compliant DVD players obsolete."<sup>154</sup> It is clear that cost would be involved in any attempt to avoid DVD piracy; research and implementation of new protective methods will be expensive, but if they are effective, we will save the outrageous cost inherent in an unnecessary restriction of freedom of speech and expression. Additionally, the court does not offer any evidence that the monetary cost involved in developing new protection technology would be debilitating to the motion picture industry. It seems that, at the very least, we should not abandon First Amendment freedoms before even exploring the costs of alternative solutions.

Another very viable and much less restrictive means to protecting the state's interest is the doctrine of contributory infringement. Contributory infringement is a concept which derives its origins from tort law.<sup>155</sup> It stems from the idea that "one who directly contributes to another's infringement should be held accountable."<sup>156</sup> The often-cited statement of the doctrine is in *Gershwin Publishing Corp. v. Columbia Artists Management, Inc.*: "One who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another, may be held liable as a

---

<sup>153</sup> *Reimerdes*, 111 F. Supp. 2d at 314.

<sup>154</sup> *Id.* at 315.

<sup>155</sup> CRAIG JOYCE ET AL., COPYRIGHT LAW 781 (5th ed. 2000).

<sup>156</sup> *Id.* at 781-82.

'contributory' infringer."<sup>157</sup> In an amicus brief to the court, Associate Professor of Law, Julie E. Cohen of Georgetown University Law Center, asserts that the doctrine of contributory infringement may well be exactly what the DMCA should have included rather than the overly restrictive anti-trafficking provision.<sup>158</sup> Cohen points out that the doctrine affords strong protection for copyright owners despite the holding in *Sony Corp. of America v. Universal City Studios, Inc.* in which the Supreme Court ruled that contributory infringement liability would not rest with the VCR manufacturer, despite the fact that the VCR enabled ("contributed to") copying of copyrighted works.<sup>159</sup> Despite that particular holding, as Cohen points out, "[c]ourts have uniformly extended contributory infringement liability to those who use dual-purpose devices actively to participate in acts of infringement, as well as to those who knowingly provide facilities to infringers."<sup>160</sup> Indeed, contributory infringement, in addition to being a much less restrictive alternative with respect to infringing on First Amendment freedoms, also promotes the government's interest in promoting progress through copyright law.<sup>161</sup> This doctrine would accomplish what was suggested above—punishing those who actually *intend to do harm* by helping or encouraging others to infringe on copyrights. At the same time however, it would not make it illegal to disseminate information regarding the means to access copyrighted material for fair use purposes. In other words, the freedom to share information would not be so violently restricted as it is currently under the DMCA, but copyright owners would still have a remedy against those individuals who were infringing or assisting in infringement.

When we realize the less restrictive alternatives which are available to us, it seems that the court has executed a knee-jerk reaction to what is, without argument, a potentially dangerous situation. Unfortunately, it is not always

---

<sup>157</sup> *Gershwin Publ'g Corp. v. Columbia Artists Mgmt., Inc.*, 443 F.2d 1159, 1162, 170 U.S.P.Q. (BNA) 182, 184-85 (2d Cir. 1971).

<sup>158</sup> Brief of Amici Curiae Julie E. Cohen at 20, *Reimerdes* (No. 00 Civ. 0277 (LAK)).

<sup>159</sup> *Id.* (discussing *Sony Corp. of America v. Univ. City Studios, Inc.*, 464 U.S. 417, 440-42, 220 U.S.P.Q. (BNA) 665, 699 (1984)) (where the court decided that the VCR had too many substantial non-infringing uses to be subjected to contributory liability).

<sup>160</sup> Brief of Amici Curiae Julie E. Cohen at 21; *see, e.g., Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 37 U.S.P.Q.2d (BNA) 1590 (9th Cir. 1996); *Sega Enters. v. MAPHIA*, 948 F. Supp. 923, 41 U.S.P.Q.2d (BNA) 1705 (N.D. Cal. 1996); *A&M Records, Inc. v. Gen. Audio Video Cassettes, Inc.*, 948 F. Supp. 1449, 39 U.S.P.Q.2d (BNA) 1818 (C.D. Cal. 1996).

<sup>161</sup> Brief of Amici Curiae Julie E. Cohen at 21.

the knee-jerk reaction that is the best. This decision has been made too abruptly and without exploration into alternative solutions.

### CONCLUSION

No one is denying that the digital age is presenting, and will continue to present, new and numerous challenges for copyright law, but we cannot let fear rule the day. The ultimate problem with this case is that the anti-trafficking provision is unconstitutional in the face of the First Amendment. The court acknowledges computer code as speech and that computer code is expressive. The court then tells us that the restriction on this expressive speech provided by the DMCA is not out of line with the First Amendment because the problem with the code is its *function*, not its *message*.<sup>162</sup> As discovered above, the two concepts, function and message, are inextricably bound to one another. If speech had no function, it would have no message, and it would cease to be speech. The court fails from the beginning to understand what the implications of this restriction really are.

The court then likens the ability to circumvent a technological measure which protects a copyrighted work to having a disease which one does not wish to cure in himself because he is not harmed by it. Therefore, there is no method to stop the spread of the disease in this case, and people all over the world may become infected with the knowledge of how to copy movies from DVDs. Throughout the entire disease metaphor, the court has forgotten one important fact—there is no harm in knowing how to copy a DVD, or any other type of copyrighted material. There is only a problem if one utilizes that knowledge to actually infringe on the intellectual property rights of another or encourages others to infringe copyrighted works.

Of course the court believes, and no doubt rightfully so, that there are people who will, once they have this knowledge, use it to pirate copies of movies. Unfortunately, based on that fear alone, the court jumps to the conclusion that this *possibility* is so horrific that it warrants throwing out First Amendment freedoms to avoid it. Meanwhile, no other alternatives are explored. In fact, we do not even really know what the degree of injury to the movie industry would be in this case. No projections are made in that regard; it is seemingly just assumed that the injury would be catastrophic.

---

<sup>162</sup> *Reimerdes*, 111 F. Supp. 2d at 329.

It hardly seems just to abandon an elemental freedom without more of an indication as to what the result of the exercise of that freedom would be. Additionally, it seems extremely unreasonable when there are several alternatives which would be enormously less restrictive and still further the objectives of copyright law, which are progress and protection.

The Digital Millennium Copyright Act is the product of a new age. It is the product of a time when the owners of copyrighted works can benefit from the new venues for their work, but also a time when they must be careful of new dangers presented by these venues. There is no question that as the Act is currently written, the defendants in this case violated the law. But is the law written correctly? This author does not believe that it is.

The defendants in this case told others how to decrypt a computer code which protects copyrighted material. Was there any copyright infringement by these defendants? No. Was there the possibility that someone they told would infringe on a copyright? Yes, there is that possibility. Should not our goal be to write our laws to punish or restrict people who do harm to others or who intend to aid other individuals in causing harm? The Digital Millennium Copyright Act as it is written today goes beyond that goal; it restricts people who are not committing any harm at the expense of an elemental freedom.

RACHEL SIMPSON SHOCKLEY

