Copy Right and Copy Wrong: DVD Jon and 321 Studios Take on the Movie Industry

STEPHEN LIU*

I. Introduction

In 1999, the Motion Picture Association of American (MPAA) and the DVD Copyright Control Association (DVD CCA) flexed their collective Hollywood muscle and encouraged Norwegian authorities to prosecute Jon Johansen, a fifteen-year-old computer whiz.[1] The teen, with the help of two acquaintances, developed a code to hack a DVD encryption and authentication system designed to limit access to the contents of a DVD.[2] Consequently, Johansen was indicted, tried, and recently acquitted on appeal for charges predicated upon a violation of Norwegian Penal Code section 145, which makes it a crime to access data by circumventing security measures.[3] However, similar cases tried in U.S. courts under the Digital Millennium Copyright Act (DMCA), the comparable anti-circumvention statute, yielded different results.[4]

This note begins with a discussion of the technology relevant to the understanding of circumvention issues now before the courts. It follows with a presentation of the principal Norwegian and U. S. statutes covering this area and concludes with a discussion of the Johansen case and a comparable U.S. case brought by 321 Studios.

II. Anti-Circumvention Technology

A digital versatile disc, universally known as a "DVD," is an optical storage medium designed to hold enormous amounts of information.[5] This massive storage capacity makes

*Stephen Liu's BIOSMU, JD 2005. Univ. of Texas at Austin B.S. in Chemical Engineering. Dec. 2001.

1. Public Prosecutor v. Johansen, [2003] E.C.D.R. 28, *311.

2. *Id.* at 314.

3. *See id.*

4. *See, e.g.*, Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294 (S.D.N.Y. 2000), (judgment entered by 111 F. Supp. 2d 346, *affirmed by* Universal City Studios, Inc. v. Corley, 273 F.3d 429, 436 (2d Cir. 2001) (holding that Plaintiff's program was properly restricted despite First Amendment protection and that "fair use" was not unconstitutionally limited by a court ordered injunction).

5. For reference, consider one estimate stating that a single CD can store the same amount of textual data as a one-hundred-yard-long bookshelf completely filled with books. Wikipedia, *CD-ROM*, *at* http://en.wikipedia.org/wiki/CD-ROM (last modified Oct. 1, 2004). A DVD, on the other hand, can store more than sixteen times that information.

a DVD ideal for encoding movies, which are essentially very large data files. In its unadulterated and unencrypted form, the information stored within a DVD could be perfectly copied and disseminated over the Internet to a vast army of modern-day pirates. Consequently, movie studios endorsed an authentication and encryption system called the Content Scrambling System (CSS) in order to protect their intellectual property rights.[6] The DVD CCA is tasked with administering this system.[7]

Authentication, the first layer of CSS protection, ensures that a DVD and the DVD player are compatible. This is done through special CSS circuitry that can only be incorporated into players manufactured by licensees of the DVD CCA.[8] Incompatibility, which precludes decryption and subsequent viewing, generally occurs when DVDs encoded for one of the seven different zones of the world, are inserted into a foreign DVD player.[9] The purpose of zone control is to permit production studios to control the global release of movies at different times in order to maximize profit and/or deal with other distribution-related issues.[10] Circumvention of authentication occurs by manually inserting an after-market chip into the player or by implementing specially coded software such as DeCSS.[11]

Encryption, the second layer of CSS protection, is comprised of a cascading security scheme centered on "keys."[12] A title key encrypts an entire movie.[13] This key is encrypted by a disc key, which in turn is encrypted by one of approximately 400 play keys.[14] Play keys are licensed out to manufacturers of DVD players.[15] To view a DVD, a DVD player must be equipped with the aforementioned CSS circuitry, which, in conjunction with a functioning play key, decrypts the disc key, which then decrypts the title key, which finally decrypts the movie for viewing.[16] This key scheme was thought to be an effective way to give the DVD CCA teeth to regulate this system by allowing the deactivation of play keys licensed to DVD manufacturers that run afoul of DVD CCA rules and regulations.[17]

As its name implies, the program DeCSS defeats a DVD's CSS authentication-encryption security system. The two functional parts of DeCSS, the anti-authentication algorithm and the anti-encryption algorithm, were created through what the movie industry calls "hacking," but what the law considers "reverse engineering."[18] Johansen was responsible for creating a simple user interface that enables the average, technologically unsophisticated layperson to implement both algorithms and crack the CSS for viewing and/or copying of DVDs.[19]

6. *Corley*, 273 F.3d at 436.

7. Jim Taylor, *DVD Frequently Asked Questions (and Answers)*, *at* http://www.dvddemystified.com/dvdfaq.html (last visited Oct. 9, 2004) [hereinafter Taylor].

8. *Id.*

9. *Id.*

10. *Id.*

11. Sean Byrne, *Sony Wins Case: Playstation 2 Mods Ruled Illegal in the UK*, *at* http://www.cdfreaks.com/news2.php?ID=10181 (last modified July 24, 2004).

12. Public Prosecutor v. Johansen, [2003] E.C.D.R. 28, *313.

13. *Id.* at *313.

14. *Id.*

15. Taylor, *supra* note 7.

16. *Id.*

17. *Id.*

18. *Id.*; Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 319-20 (S.D.N.Y., 2000).

19. Public Prosecutor v. Johansen, [2003] E.C.D.R. 28, *315.

III. Anti-Circumvention Legislation

As a result of the obvious inadequacies of global copyright protection, the international community came together and drafted the World Intellectual Property Organization (WIPO) Copyright Treaty in 1996.[20] WIPO signatories agreed to enact legislation to protect against *circumvention* of technological measures—as distinguished from protection against the actual *copying* of copyrighted works.[21] As one of the signatories to the treaty, the United States enacted the DMCA in 1998.[22] Norway, however, did not sign the WIPO Treaty,[23] and it is not a member of the European Union, which did sign the treaty.[24] However, Norway enacted Penal Code section 145 to essentially serve the same purpose.

A. Norwegian Penal Code section 145

In comparison to its U.S. counterpart, the applicable Norwegian anti-circumvention statute is noticeably underdeveloped. Norwegian Penal Code section 145, paragraph 2 specifies a cause of action against anyone who, "by breaking the protection or in a similar way without authorisation [sic], accesses data or programs stored or communicated by electronic or other technical means."[25]

B. The Digital Millennium Copyright Act

The DMCA, although codified within the same title of the U.S. Code containing the Copyright Act, does not affect any of the substantive rights or remedies of copyright holders.[26] Rather, it is a strictly anti-circumvention statute that attaches liability regardless of whether or not one would be permitted to use the copyrighted work. The DMCA specifically provides liability for three types of acts: (1) circumvention of access control devices,[27] (2) trafficking in technology for circumventing access control devices,[28] and (3) trafficking in technology for circumventing copy control devices.[29] To illustrate the difference, the use of DeCSS to decrypt a DVD would be unauthorized *circumvention* of an access control device whereas posting DeCSS on the internet for sale would be an unauthorized *trafficking in technology for circumventing* access control devices. Since DVDs lack any protective mea-

20. Terese Foged, *U.S. v. E.U. Anti-Circumvention Legislation: Preserving the Public's Privileges in the Digital Age*, E.I.P.R. 2002, 24(11), 525-542, 526 (2002).

21. *Id.* at 526.

22. *Id.*

23. World Intellectual Property Organization, *WIPO Copyright Treaty*, *available at* http://www.wipo.int/treaties/en/documents/pdf/s-wct.pdf (last visited Sept. 24, 2004).

24. Europa, *The EU at a Glance—European Treaties*, *at* http://europa.eu.int/abc/governments/index_en.htm#members (last visited Nov. 2, 2004).

25. Public Prosecutor v. Johansen, [2003] E.C.D.R. 28, *317 (quoting section 145).

26. 17 U.S.C.A. § 1201(b)(2) (West 1999).

27. The statute provides in relevant part: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(a)(1)(A).

28. Likewise, "No person shall . . . traffic in any technology that is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(a)(2)(A).

29. Similarly, "No person shall . . . traffic in any technology . . . that is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title . . ." 17 U.S.C. § 1201(b)(1)(A).

sure preventing or even limiting their complete duplication (recall that CSS is merely an authentication-encryption security measure and only limits access), the anti-trafficking provision relating to *copy control devices* is inapplicable.

The DMCA contains seven exemptions from liability, three of which are raised as DeCSS-related defenses. They are: (1) encryption research, (2) reverse engineering, and (3) security testing.[30] The encryption research exemption requires a lawful copy of the copyrighted work and a good faith effort to obtain authorization before circumvention for a legitimate study in encryption and/or to advance the state of knowledge in this area.[31] The reverse engineering exemption permits an individual to circumvent an access-control measure for the sole purpose of achieving interoperability with another computer program.[32] For instance, a claim that DeCSS was created in order to play a DVD on a Linux-based operating system would fall under this exemption of the DMCA. (However, the fact that DeCSS enables Windows-based computers to decrypt a DVD is contradictory evidence.) The security testing exemption is narrowly construed to apply only to a computer, computer system, or a computer network, thus likely excluding from its purview the decryption of DVDs.[33]

At least one court determined that a plaintiff must satisfy six elements to establish a *prima facie* case under the DMCA.[34] The plaintiff must prove: (1) ownership of a copyright in a work; (2) that is controlled by an effective technological measure; (3) which, because of a means of circumvention, a third party can access; (4) without authorization; (5) that infringes or facilitates the infringement of a right protected by the Copyright Act; (6) because the defendant either designed or produced a product primarily for the purpose of circumvention, or made such a product available despite limited commercial significance, or marketed the product for circumvention purposes.[35]

IV. Anti-Circumvention Case Law

The *Johansen* case was the most recent Norwegian case tried under section 145 of the Penal Code. The *321 Studios* case, which was heard in the Northern District of California, is one of the more recent DMCA DeCSS cases tried in the United States. The U.S. District Court relied heavily upon the 2000 *Reimerdes* case and the subsequent 2001 appeal, *Universal City Studios, Inc. v. Corley*.[36]

A. The Case Against Jon Johansen

Although Johansen was credited with the creation of DeCSS, the translated opinion makes it clear that much of DeCSS was created by two other individuals who were not parties to the suit.[37] Johansen was responsible, however, for mistakenly posting the program

30. *Reimerdes*, 111 F. Supp. 2d at 319-21.
31. *Id.* at 320-21.
32. *Id.* at 321.
33. *Id.*
34. Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004).
35. *Id.*
36. *See Corley*, 273 F.3d at 429.
37. *See* Public Prosecutor v. Johansen, [2003] E.C.D.R. 28, *314.

on the Internet briefly on October 6, 1999.[38] This mistake caught the attention of the MPAA and the DVD CCA, who eventually approached the Norwegian authorities about the matter.

Johansen was not charged with any violation of the then-existing Norwegian copyright law despite the fact that his confiscated computer contained 200 megabytes of the movie *The Matrix*, which was copied using the DeCSS technology without the prior consent of the copyright holder.[39] This is most likely because Johansen, who copied only a small portion of the copyrighted movie and did not subsequently offer it for sale, had a statutory defense under copyright law immunizing him from suit. Johansen was entitled to create a single copy of any work provided it was not done for the purposes of financial gain.[40] Additionally, Johansen could have defended copying the movie and the subsequent alteration of CSS under a provision that permits the copying of protected subject matter to "obtain the information necessary to achieve the interoperability of an independently created computer program with other programs . . . ."[41] Indeed, Johansen stated that his purpose for helping to create the DeCSS was to create a DVD player operable on his Linux Operating System, which at the time, was not a CSS licensee like its primary competitor, Windows OS.[42] Thus, only the access of the protected data—as opposed to the actual copying of the data—would be a sufficient basis upon which to predicate any cause of action.

Johansen was ultimately charged with violation of Norwegian Penal Code section 145, which prohibits the unauthorized and illegal access of electronic data by circumventing an active security measure.[43] The court's opinion focused on two issues: the definition of "data" and the definition of "illegal."[44] In briefly addressing the first issue, the court held that the encrypted movie and the accompanying CSS keys, both contained on the DVD, were "data" as defined by section 145.[45]

On the second issue, the court was required to consider whether Johansen's access of the aforementioned data was illegal. As to the CSS keys, the court found this access was not illegal under section 145 of the code.[46] The court's rationale was that section 145 forbids the access of data by means of circumventing a security measure; consequently, CSS as a form of data was not protected under the statute since it was not protected by any security measure.[47] As to the movie, the court determined that the applicability of the statute depended upon the manner in which the data was procured. Legal acquisition (e.g. purchase of a DVD) necessarily resulted in authorized access regardless of the actual manner in which the data was accessed. Conversely, illegal acquisition (e.g., theft of a DVD) would apparently result in unauthorized access actionable under section 145 even if it were played on a legally purchased DVD player.

38. *Id.* at 315.
39. Public Prosecutor v. Johansen [2004] E.C.D.R. 17 at *199.
40. Act No. 2 of 1961 Relating to Copyright in Literary, Scientific and Artistic Works, ch.1, § 12, *available at* http://www.jus.uio.no/iri/forskning/lib/laws/copyright.html (last modified Oct. 5, 2001).
41. *Id.* § 39i.
42. Public Prosecutor v. Johansen [2004] E.C.D.R. 17 at *200.
43. *Id.* at 196.
44. *Id.* at 200.
45. *Id.*
46. *Id.* at 204-05.
47. *Id.*

The Norwegian Court's focus on the manner in which the DVD is acquired as being indicative of the outcome of a violation of the anti-circumvention legislation is not shared by the United States, which consistently favors a strong protection of the rights of copyright holders.

B. The Case Against 321 Studios

In 2002, Plaintiff 321 Studios (321) filed a declaratory relief complaint against members of the MPAA, seeking to establish, *inter alia*, that its sale of DVD-copying software was not a violation of the DMCA.[48] The software, which was marketed as a means to create backup copies of legally purchased DVDs, permitted the user to create unencryptedcopies of the DVDs without using CSS.[49] In its complaint, 321 defended its actions on the grounds that CSS, as a meager 40-bit encryption system, was too easily cracked to make it an "effective security measure" under the purview of the DMCA.[50] Alternatively, it argued that it did not "circumvent" CSS since it used an authorized key, albeit belonging to another licensee, to access the underlying movie.[51] Furthermore, 321 argued that even if its software did circumvent CSS, it was implicitly authorized since a purchaser of a DVD is permitted to view it by means of decryption.[52]

Ultimately, the Court found against 321 on these arguments. It first determined that an "effective control" as defined by the DMCA was not to be based upon the ease at which the measure could be circumvented.[53] Rather, the Court held that if such a measure in its ordinary operation was meant to restrict access to copyrighted work, then it "effectively controlled" that access, thereby placing CSS within the scope of the DMCA.[54] Next, the court determined that use of an authorized key for decryption in the absence of express permission from the DVD CCA was still actionable circumvention.[55] Lastly, the Court determined that the implicit authorization to view a DVD is separate and distinct from any authorization to decrypt that movie for viewing.[56]

Further, 321 asserted in its defense that the intended use of the copying software did not violate any rights of the copyright holder, and similarly, the software was not primarily designed to circumvent CSS in light of its intended use. The court disagreed on both counts. The intended use of the software was held irrelevant in determining whether the software was primarily designed for the purposes of circumventing a technological measure.[57] The sale of software that circumvents CSS for the stated purpose of enabling the creation of a legal backup copy is thus a violation of the anti-trafficking provision of access control devices.[58] Likewise, the court responded by stating that the primary intended use of the software is irrelevant to a finding of an actionable circumvention under the DMCA.[59] The

48. *See* 321 Studios v. Metro Goldwyn Mayer Studios Inc., 307 F. Supp. 2d 1085 (N.D. Cal. 2004).
49. *Id.* at 1089.
50. *Id.* at 1095.
51. *Id.* at 1098.
52. *Id.* at 1096.
53. *Id.* at 1095.
54. *Id.* at 1094-95.
55. *Id.* at 1098.
56. *Id.* at 1096.
57. *Id.* at 1098.
58. *Id.*
59. *Id.* at 1097.

court succinctly stated that "[i]t is the technology itself at issue, not the uses to which the copyrighted material may be put" which determines liability.[60] Lastly, the court made a questionable finding that DeCSS imports liability under the anti-trafficking provision of copy control devices. Despite admissions that "321 is technically correct that CSS controls access to encrypted DVDs," they erroneously concluded that "encrypted DVDs cannot be copied unless they are accessed."[61]

Thus, the court in *321 Studios* adopted a liberal interpretation of the DMCA and held 321 liable for illegal circumvention and the trafficking of both access control devices and copy control devices. Initially, an appeal was planned, but diminishing financial resources and increased legal pressure from some of the largest and most influential industries in the world, namely the movie and electronic gaming industries, forced a premature settlement.[62]

V. Conclusion

The difference of opinion on the practical effect of a legally purchased DVD on a subsequent circumvention is the primary reason the courts of Norway and the United States found oppositely on the issue of circumvention. For the Norwegian courts, a legally acquired DVD precludes a finding of actionable anti-circumvention, whereas such an acquisition in the United States, according to the *321* Court, is irrelevant under the DMCA. Although it is likely that the United States' position will arguably never align itself with the views of their Norwegian counterparts, 321's overly broad interpretation of the DMCA will most likely be modified and limited by successive opinions. For instance, while the court in *321* was quick to dismiss the argument that the use of an authorized key precluded a finding of actionable circumvention under the DMCA, another federal court considered a similar issue on a more recent case and found oppositely.[63] Specifically, that court determined that the use of an authorized password by a third party not having authority to use that particular password to access a protected website was not actionable under the DMCA's anti-circumvention provision since the accused merely "avoided and bypassed the permission to engage and move through the technological measure from the measure's author."[64] Similarly, the *321* court's determination that the legal downstream uses are irrelevant to the determination of a DMCA violation could be seen as contradicted by another, more recent court opinion that requires the circumvention to aid or permit the violation of a copyright holder's right in order for liability to attach under the DMCA.[65] Given time, the courts of both Norway and the United States will provide more educated and consistent opinions that fully flesh out the limits of their respective anti-circumvention statutes and that more adequately balance the interests of the copyright holder against that of the consumer.

60. *Id.*

61. *Id.*

62. BBC News, *Film industry hails 'piracy win,' available at* http://news.bbc.co.uk/1/hi/entertainment/film/3552500.stm (last updated Aug. 10, 2004).

63. I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., 307 F. Supp. 2d 521, 532 (S.D.N.Y. 2004).

64. *Id.*

65. *See* Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, at 1200-01 (Fed. Cir. 2004).