

Foreword

Gerard M. Stegmaier¹

WILSON SONSINI GOODRICH & ROSATI
RESTON, VIRGINIA

Copyright © 2005, IOMA, Inc. Published by Pike & Fischer, publishers of *Internet Law & Regulation* (www.ilrweb.com). This work originally appeared in *THE DIGITAL MILLENNIUM COPYRIGHT ACT – 2005 SUPPLEMENT*, available at <http://www.pf.com/dmca2005.asp>. Reprinted with permission. Send editorial inquiries to msmith@pf.com.

Since the publication of *The Digital Millennium Copyright Act: Text, History, and Caselaw*,² courts have continued to refine their interpretation of the online service provider liability and anti-circumvention provisions of the Digital Millennium Copyright Act (“DMCA”). While earlier interpretations appeared to tip heavily in favor of those holding copyrights, as in *Universal City Studios v. Reimerdes*³ and *Sony Computer Entertainment America, Inc. v. Gamemasters*,⁴ recent decisions interpreting the DMCA appear to have somewhat tempered those early victories. The judicial, administrative, and legislative developments contained in this Supplement represent the ongoing efforts by courts, agencies, and lawmakers to grapple with the technological innovation that has occurred since the passage of the DMCA as well as the continuing evolution of electronic commerce. The Constitution makes clear in Article I, Section 8 that promotion of “the Progress of Science and useful Arts”⁵ depends on an equilibrium between property rights and the free exchange of information. While the DMCA attempts to strike an appropriate balance between those goals, the continuing debate over the DMCA’s meaning and application demonstrates that the proper balance may not have yet been reached in the eyes of many stakeholders.

Online Service Provider Liability

Title II of the DMCA provides online service providers with liability limitations, or “safe harbors,” for providing certain features. The safe harbors extend to (1) transmitting, routing, or providing connections for infringing material; (2) system caching; (3) information stored by a user; or (4) linking or directing users to infringing material (e.g. search engines).⁶ In order to qualify for these safe harbors, service providers must meet certain criteria and requirements. One provision that has received considerable judicial attention pertains to the subpoena process for identifying alleged infringers.⁷

¹ The author is an attorney with Wilson Sonsini Goodrich & Rosati, P.C. in Reston, Virginia. He also serves as an adjunct professor teaching various technology and intellectual property-related courses at George Mason University School of Law and as a member of the Privacy Advisory Committee of the Virginia Legislature’s Joint Commission on Technology and Science. The author wishes to thank Eion Murdock, a 2006 candidate for the juris doctorate degree at George Mason for his research assistance and the National Center for Technology and Law at George Mason for its continued support of the author’s research efforts. The author may be reached by e-mail at gstegmaier@wsgr.com. The views expressed herein are entirely the author’s and do not represent the views of any organization with which he may be affiliated.

² Pike & Fischer, 2003 (hereinafter cited as “*DMCA (2003 Ed.)*”).

³ *Universal City Studios v. Reimerdes*, 111 F Supp 2d 294, 6 ILR (P&F) 1 (SD NY 2000), *DMCA (2003 Ed.)*, p. 1037.

⁴ *Sony Computer Entertainment America, Inc. v. Gamemasters*, 87 F Supp 2d 976, 1999 ILRWeb (P&F) 3001 (ND Cal 1999), *DMCA (2003 Ed.)*, p.973.

⁵ U.S. CONST. art. I, § 8, cl. 8.

⁶ 17 USC §512(a) (2000)

⁷ *Id.* at §512(h)(5).

Initially, courts appeared willing to enforce DMCA subpoenas that sought the identities of subscribers who stored infringing material on their own—rather than service providers’—computers.⁸ However, in December 2003 the U.S. Court of Appeals for the District of Columbia Circuit overturned an earlier ruling to that effect and quashed such subpoenas.⁹ Verizon, the service provider at issue in the case, successfully argued that the provisions of §512(h) of the DMCA do not apply to service providers who act as mere conduits for data transferred between end-users. The appeals court thus interpreted §512(h) to authorize only the issuance of subpoenas against service providers that store infringing material on their servers.¹⁰ This interpretation was based on the requirements for obtaining a subpoena set forth in §512(h).

Section 512(h) by its terms requires the copyright holder to file along with the subpoena request “a notification of claimed infringement” as described in §512(c)(3)(A). That notification must identify material “to be removed or access to which is to be disabled” by the service provider.¹¹ However, because infringing material obtained or distributed via peer-to-peer file sharing may be located on the computer of an individual user, service providers that act as mere conduits arguably have no power to remove or disable access to such materials other than by disabling each individual user’s access to the Internet. The court thus held that disabling an individual user’s access to the Internet was intended to be a separate remedy, and that effective notification of alleged infringement under §512(c)(3)(A) was not possible if the target of the desired subpoena was acting merely as a conduit.¹² Because proper notification was not possible under this reasoning, the court concluded that copyright holder could not meet the requirements of §512(h) and granted Verizon’s motion to quash the subpoenas.¹³

In early 2005 the U.S. Court of Appeals for the Eighth Circuit in *In re Charter Communications Subpoena Enforcement Matter*¹⁴ closely followed D.C. Circuit’s analysis and reasoning, perhaps signaling the emergence of a prevailing view on this issue. Nonetheless, in April 2004 an Illinois federal district court denied standing to an Internet service provider that sought to quash subpoenas on behalf of its customers in *Fatwallet v. Best Buy Enterprise Services*.¹⁵ The *Fatwallet* court concluded that it was “difficult to see the harm that would befall the plaintiff as opposed to its subscribers” from enforcement of the subpoenas.¹⁶ *Fatwallet* differed somewhat from the facts in *Verizon Internet Services* and *Charter Communications* in that Best Buy had “asserted to th[e] court that it ha[d] no intention of [enforcing the subpoena].”¹⁷

In order to qualify for any of the safe harbors under §512, service providers must also reasonably implement a policy to deal with repeat infringers. In *Ellison v. Robertson*, plaintiff Ellison alleged that America Online had infringed his copyright by copying and redistributing material that had been posted without Ellison’s authorization to a Usenet newsgroup by Robertson.¹⁸ The district court held that America Online qualified for the 17 USC §512(a) safe harbor, despite the fact that America Online had changed its contact e-mail address for copyright infringement claims without configuring its mail system to forward e-mails sent to the old address.¹⁹ The Ninth Circuit reversed, ruling that America Online’s actions had created a “triable issue of material fact regarding [its] eligibility for the safe harbor limitations of liability” under §512(i).²⁰ In the court’s words, “AOL allowed notices of potential copy-

⁸ See *In re Verizon Internet Servs. Inc. Subpoena Enforcement Matter*, 240 F Supp 2d 24, 12 ILR (P&F) 640 (D DC 2003), p. 948, *infra*.

⁹ See *Recording Indus. Ass’n of Am. v. Verizon Internet Servs.*, 351 F3d 1229, 15 ILR (P&F) 1, 359 US App DC 85 (2003), p. 895, *infra*.

¹⁰ See *id.* 359 US App DC at 89.

¹¹ 17 USC §512(c)(3)(A)(iii).

¹² See *Verizon Internet Servs.*, 359 US App DC at 91-92.

¹³ See *id.* at 92, 95.

¹⁴ *In re Charter Communications Subpoena Enforcement Matter*, 393 F3d 771, 17 ILR (P&F) 54 (8th Cir 2005), p. 654, *infra*.

¹⁵ *Fatwallet, Inc. v. Best Buy Enter. Servs.*, 15 ILR (P&F) 678, Copyright L Rep (CCH) ¶ 28,799, at 30,006 (ND Ill April 12, 2004), p. 750, *infra*.

¹⁶ *Id.*, 15 ILR (P&F) at 679, Copyright L Rep (CCH) at 37,008.

¹⁷ *Id.*

¹⁸ See *Ellison v. Robertson*, 357 F3d 1072, 15 ILR (P&F) 175 (9th Cir 2004), p. 741, *infra*.

¹⁹ See *id.* 357 F3d at 1077.

²⁰ *Id.* at 1080.

right infringement to fall into a vacuum and go unheeded; that fact is sufficient for a reasonable jury to conclude that AOL had not reasonably implemented its policy against repeat infringers.”²¹

The court in *Ellison* noted three factors—based upon the statute’s language—that an Internet service provider must satisfy in order to fulfill the statutory prerequisite laid out in §512(i)(1)(A). First, it must adopt a policy that provides for the termination of access for repeat copyright infringers. Second, it must implement that policy in a reasonable manner. And finally, the Internet service provider must inform its clients of the policy.²²

The *Perfect 10 v. CCBill* court²³ subsequently relied upon the reasoning set forth in *Ellison* to determine the applicability of the §512 safe harbors to defendants who provided billing and age verification services.²⁴ The *Perfect 10* court held that imperfect implementation of a company’s DMCA policy did not vitiate a defendant’s efforts to qualify for §512 safe harbor protection so long as the implementation was reasonable; individual instances of failure to terminate repeat infringers were not necessarily unreasonable.²⁵ The court concluded that the defendants were entitled to the relevant §512 safe harbor protections, and granted CCBill’s motion for summary judgment, thereby dismissing underlying copyright infringement claims.²⁶

The *Perfect 10* holding was followed by the court in *Corbis v. Amazon.com*.²⁷ Corbis, a copyright holder in stock images, sued Amazon.com, the well-known Internet retailer, for direct and vicarious copyright infringement, alleging that individual vendors had used Amazon’s services to sell infringing products.²⁸ Amazon asserted a §512 safe harbor defense, and the court relied upon the *Ellison* factors to determine if §512 applied.²⁹ The court held that the §512 safe harbors did indeed apply to Amazon—following *Perfect 10* in finding that isolated failure to terminate repeat infringers did not constitute a failure to reasonably implement a DMCA policy—and granted summary judgment to Amazon.³⁰

In *Hendrickson v. Amazon.com*,³¹ the question before the court was whether notification of potential infringement before the subsequent infringement took place would preclude use of the §512 safe harbors. Hendrickson notified Amazon.com that any DVD copies of his copyrighted motion picture were infringing.³² When a third party subsequently sold infringing copies of his motion picture using Amazon’s services, Hendrickson sued.³³ Amazon claimed that it was protected by the safe harbor despite Hendrickson’s notification.³⁴ The court agreed, holding that “if at the time the notice is received, the infringing material is not posted, the notice does not enable the service provider to locate infringing material that is not there, let alone do it expeditiously.”³⁵

The online service provider liability provisions of the DMCA also provide sanctions for those who knowingly make material misrepresentations in sending or responding to takedown notices.³⁶ The use of this provision was put to test in *Online Policy Group v. Diebold*.³⁷ Online Policy Group (OPG) had acquired one of Diebold’s internal e-mail archives that contained messages acknowledging problems with Diebold’s products—principally electronic voting machines—and posted the contents of the archive on a web site.³⁸ In response, Diebold sent takedown no-

²¹ *Id.*

²² *Id.*

²³ *Perfect 10, Inc. v. CCBill, LLC*, 340 F Supp 2d 1077, 16 ILR (P&F) 127 (CD Cal 2004), p. 865, *infra*.

²⁴ *See id.* 340 F Supp 2d at 1087.

²⁵ *See id.* at 1090.

²⁶ *See id.* at 1102-03, 1112.

²⁷ *Corbis v. Amazon.com, Inc.*, 351 F Supp 2d 1090, 17 ILR (P&F) 238 (WD Wash 2004), p. 674, *infra*.

²⁸ *See id.* 351 F Supp 2d at 1093.

²⁹ *See id.* at 1099.

³⁰ *See id.* at 1110.

³¹ *Hendrickson v. Amazon.com, Inc.*, 298 F Supp 2d 914, 15 ILR (P&F) 22 (CD Cal 2003), p. 758, *infra*.

³² *See id.* 298 F Supp 2d at 915.

³³ *See id.*

³⁴ *See id.*

³⁵ *Id.* at 917.

³⁶ 17 USC §512(f) (2000).

³⁷ *Online Policy Group v. Diebold*, 337 F Supp 2d 1195, 16 ILR (P&F) 636 (ND Cal 2004), p. 818, *infra*.

³⁸ *See id.* 337 F Supp 2d at 1197.

tices to OPG's Internet service providers pursuant to 17 USC §512(c), who subsequently demanded that OPG remove the archive.³⁹ OPG alleged that these notices violated §512(f) because Diebold "'knowingly materially misrepresented' that publication of the e-mail archive constituted copyright infringement."⁴⁰

The U.S. District Court for the Northern District of California confronted the issue as to what standard should be applied when determining whether a knowing material misrepresentation had occurred.⁴¹ The court held that "'[k]nowingly' means that a party actually knew, should have known if it acted with reasonable care or diligence, or would have no substantial doubt had it been acting in good faith, that it was making misrepresentations" and that "'[m]aterial' means that the misrepresentation affected the ISP's response to a DMCA letter."⁴² After applying this standard, the court concluded that Diebold was liable under §512(f).⁴³

Anti-Circumvention Provisions

Inasmuch as the DMCA also addresses the concerns of content owners and producers, it affords significant protection to rights holders in the anti-circumvention provisions found in Section 1201 of Title I of the DMCA. Recent years have seen several litigation developments as courts have interpreted the scope and meaning of these provisions.

Early in 2002, the United States brought criminal charges against Elcom, a Russian software company that allegedly distributed software that removed copy-protection mechanisms built into electronic books, for violations of 17 USC §§ 1201(b)(1)(A) and (C).⁴⁴ Elcom responded by claiming that §1201(b) was unconstitutional on First Amendment, Fifth Amendment vagueness, and Commerce Clause grounds.⁴⁵

The court dismissed the vagueness argument, stating that "there [was] no ambiguity in what tools are allowed and what tools are prohibited because the statute bans trafficking in or the marketing of *all* circumvention devices" (emphasis added), and so the statute was not unconstitutionally vague.⁴⁶

As to its First Amendment arguments, Elcom first argued that the DMCA as applied to the sale of its product was unconstitutional because its product was a form of speech, and the government was prohibiting this speech based on its content.⁴⁷ The government argued that the product was not speech (an argument the court rejected out of hand) and that §1201 did not refer to the expressive content of speech, but rather the function divorced of the message.⁴⁸ This distinction was important because content-based speech regulation must meet strict scrutiny by being the least restrictive means to achieve a compelling state interest in order to pass constitutional muster, whereas content-neutral speech regulation only needs to be narrowly tailored to further a substantial and legitimate government interest.⁴⁹ The court, finding no congressional intent "to target speech because of its expressive content" and observing that "[o]n its face, the statute does not target speech," found that §1201 was content neutral.⁵⁰ Prevention of digital piracy was found by the court to be "both [a] legitimate and substantial" government interest, and the exceptions included in §1201 suggested that the statute was indeed narrowly tailored.⁵¹

Elcom further argued that §1201(b) burdened the §107 fair use rights of third party users of copy-protected materials.⁵² The court disagreed, saying that §1201(b) merely prohibited the distribution of tools that third parties could use to circumvent access restrictions (as opposed to §1201(a), which banned the use of such tools subject to certain fair use restrictions). Because "the DMCA does not eliminate fair use or substantially impair the fair use

³⁹ *See id.* at 1198.

⁴⁰ *Id.* at 1204.

⁴¹ *See id.*

⁴² *Id.*

⁴³ *See id.* at 1206.

⁴⁴ *See United States v. Elcom Ltd.*, 203 F Supp 2d 1111, 10 ILR (P&F) 611 (ND Cal 2002), *DMCA (2003 Ed.)* p. 1001.

⁴⁵ *See id.* at 203 F Supp 2d 1122, 1123.

⁴⁶ *See id.* at 1125.

⁴⁷ *See id.*

⁴⁸ *See id.* at 1126.

⁴⁹ *See id.* at 1127.

⁵⁰ *See id.* at 1128.

⁵¹ *See id.* at 1130, 1131, 1132.

⁵² *See id.* at 1133.

rights of anyone,” the court found that the DMCA was not rendered unconstitutionally overbroad.⁵³ The court also rejected Elcom’s challenge to the DMCA on Commerce Clause and Intellectual Property Clause grounds and finally denied Elcom’s motion to dismiss.⁵⁴

The anti-circumvention provisions were similarly found constitutional in *321 Studios v. MGM Studios*,⁵⁵ where 321 Studios sought a declaratory judgment that its DVD back-up software was permissible under §1201 and alleged that the DMCA’s anti-circumvention provisions were unconstitutional.⁵⁶ MGM claimed that 321’s product did in fact violate the DMCA. The district court granted MGM’s motion for partial summary judgment, ruling that because 321’s product used an unauthorized key (a special secret code used by authorized DVD players to read encoded DVDs), “it therefore avoids and bypasses CSS” and so the relevant provisions of the DMCA applied to its software.⁵⁷

In 2004 two major anti-circumvention cases were decided. These cases arguably suggest a treatment of §1201 claims by courts in a fashion that makes it more difficult for rights holders to control technology and competition under the auspices of copyright.

The first of these cases was *Chamberlain Group v. Skylink Technologies*.⁵⁸ Skylink manufactured a replacement garage door opener that was capable of opening Chamberlain’s garage doors. However, Chamberlain’s garage doors included a computerized encryption system to prevent criminals from opening a garage using a stolen code.⁵⁹ Chamberlain alleged that by selling a garage door opener capable of interacting with its security system, Skylink had circumvented the measures controlling access to the copyrighted garage door opening program.⁶⁰ The district court rejected this construction of the DMCA and Chamberlain appealed.⁶¹

The Federal Circuit upheld the district court’s decision, observing that “Chamberlain’s proposed construction would allow copyright owners to prohibit exclusively fair uses even in the absence of any feared foul use” and that “§1201 prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners.”⁶²

The Federal Circuit noted that §1201(a)(2) is violated when a plaintiff establishes that it owns a valid copyright effectively controlled by a technological measure that had been circumvented such that third parties could have unauthorized access to the work in a manner infringing or facilitating infringing of a right protected by the Copyright Act.⁶³ The circumvention must also have been made possible because of a product that the defendant either designed or produced primarily for circumvention and made available despite only limited commercial significance other than circumvention or alternatively had been marketed for use in circumventing the controlling technological measure.⁶⁴ In order to demonstrate a violation, a plaintiff must establish the circumvention as well as one of the two elements related to the motives for circumvention.⁶⁵ Chamberlain failed to meet the requirements of this test, and therefore summary judgment for Skylink was proper.⁶⁶

*Lexmark International v. Static Control Components*⁶⁷ represents another significant case development. Lexmark, a manufacturer of laser printers, sued to prevent Static Control from selling cartridges compatible with Lex-

⁵³ See *id.* at 1134.

⁵⁴ See *id.* at 1138-42.

⁵⁵ *321 Studios v. MGM Studios*, 307 F Supp 2d 1085, 15 ILR (P&F) 347 (ND Cal 2004), p. 543, *infra*.

⁵⁶ See *id.* at 307 F Supp 2d 1089, 1090.

⁵⁷ See *id.* at 1097, 1098.

⁵⁸ *Chamberlain Group v. Skylink Techs.*, 381 F3d 1178, 16 ILR (P&F) 256 (Fed. Cir 2004), p. 634, *infra*.

⁵⁹ See *id.* 381 F3d at 1183-85.

⁶⁰ See *id.* at 1182.

⁶¹ See *id.* at 1186-88.

⁶² *Id.* at 1202.

⁶³ See *id.* at 1203.

⁶⁴ See *id.*

⁶⁵ See *id.*

⁶⁶ See *id.* at 1204.

⁶⁷ *Lexmark Int’l v. Static Control Components*, 387 F3d 522, 16 ILR (P&F) 611 (6th Cir 2004), p. 774, *infra*.

mark printers.⁶⁸ Lexmark included a computerized authentication system in its printers and printer cartridges so that both the printer and printer cartridge contained embedded computer code.⁶⁹ The printer program authenticated the printer cartridge by checking that the cartridge contained an authorized program and, if so, the printer would operate.⁷⁰ Static Control included a copy of Lexmark's cartridge program with its own cartridges so that its cartridges would operate in Lexmark printers.⁷¹ Lexmark sued, alleging that defendant's inclusion of the cartridge program constituted circumvention of plaintiff's authentication scheme in violation of the anti-circumvention provisions of the DMCA.⁷² The district court agreed and issued a temporary injunction. Static Control appealed.⁷³ The appellate court reversed and vacated the preliminary injunction, holding that Lexmark's scheme did not control access to the work because the work could still be read from the printer—the scheme merely controlled use of the printer.⁷⁴ The court also said that the §1201(f) statutory exemption for interoperability to the anti-circumvention provisions of the DMCA could apply to Static Control's cartridges.⁷⁵

Although the *Chamberlain* and *Lexmark* decisions provide a narrower alternative interpretation of §1201, it remains to be seen whether other courts will follow this more recent line of cases.

Copyright Management Information

The Digital Millennium Copyright Act also contains provisions aimed at preventing the removal or falsification of copyright management information.⁷⁶ Generally claims under these provisions have not succeeded, most likely due to the statutory requirements that the defendant must have intentionally removed or falsified the information and known or had reason to know that its actions would have facilitated infringement.

Courts have interpreted intentional removal or falsification to mean that defendants must know or have reason to know that the work is copyrighted.⁷⁷ Even a subjective belief that the work is not copyrighted may be enough to escape liability.⁷⁸ Several cases have established a *de minimis* defense to actions brought under §1202.⁷⁹

In addition, courts have found that “to be actionable under §1202(b), a defendant must remove copyright management information from the ‘body’ of, or area around, plaintiff’s work itself.”⁸⁰

Legislation

Since 2002 there have been several attempts to further refine the Copyright Act, partly in response to the continued increase in illicit peer-to-peer file sharing over the Internet. The DMCA was enacted before *Napster* and its progeny, and rights holders have argued that the DMCA does not give them the means to adequately enforce their rights in this new environment.

In response, two bills were introduced in the 108th Congress: the Protecting Intellectual Rights Against Theft and Expropriation (PIRATE) Act of 2004⁸¹ and the Inducing Infringement of Copyrights (IICA, also known as INDUCE) Act of 2004.⁸²

⁶⁸ See *id.* 387 F3d at 529.

⁶⁹ See *id.* at 529, 530.

⁷⁰ See *id.* at 530-31.

⁷¹ See *id.*

⁷² See *id.* at 531.

⁷³ See *id.*

⁷⁴ See *id.* at 546-48.

⁷⁵ See *id.* at 550-51.

⁷⁶ 17 USC §1202.

⁷⁷ See, e.g., *Ward v. National Geographic Soc’y*, 208 F Supp 2d 429, 15 ILR (P&F) 62 (SD NY 2002), p. 972, *infra*.

⁷⁸ See *Schiffer Publ’g v. Chronicle Books*, 17 ILR (P&F) 294, 73 USPQ2d 1090 (ED Pa. 2004), p. 914, *infra*.

⁷⁹ See *Ward*, 208 F Supp 2d 429, 15 ILR (P&F) 62 (SD NY 2002); *Gordon v. Nextel Communications*, 345 F3d 922, 2003 ILRWeb (P&F) 2855 (6th Cir 2003), p. 753, *infra*.

⁸⁰ *Schiffer Publ’g*, 17 ILR (P&F) 294, 73 USPQ2d 1090 (ED Pa. 2004).

⁸¹ Protecting Intellectual Rights Against Theft and Expropriation (PIRATE) Act of 2004, S. 2237, 108th Cong. (2004), p. 185, *infra*.

⁸² Inducing Infringement of Copyrights Act of 2004, S. 2560, 108th Cong. (2004), p. 193, *infra*.

The PIRATE Act would amend Chapter 5 of Title 17 to give the Attorney General standing to bring civil suits on behalf of individual copyright owners. The individual copyright owners would receive restitution from the Attorney General's suit, but also would be able to bring their own suits. Any restitution an individual copyright owner received from the Attorney General would be offset against any damage award in a suit brought by the copyright owner.

The PIRATE Act faced criticism for shifting the cost of file-sharing lawsuits from the music and movie industry to the taxpayer; however, it passed the Senate and moved to a House subcommittee.

The INDUCE Act would amend 17 USC §501 to include intentional inducement to infringe copyright, much like the similar inducement provision in the Patent Act. Anyone who "intentionally aids, abets, induces, or procures" infringing acts would be liable as an infringer. However, the Act was by its terms not intended to alter the doctrines of contributory and vicarious liability.

The INDUCE Act was controversial from the outset and ultimately died in committee. Future congressional action may well depend on the outcome of the Supreme Court's decision in *MGM Studios v. Grokster*,⁸³ a case which seeks to clarify and refine the doctrines of contributory and vicarious infringement as they apply to peer-to-peer file sharing. The Supreme Court has yet to hear oral arguments in *Grokster* as of this writing.

On the other hand, users' rights groups contended that the DMCA upset the traditional balance of copyright law by impairing their fair use rights. The Digital Media Consumers' Rights Act of 2002⁸⁴ and the Benefit Authors without Limiting Advancement or Net Consumer Expectations (BALANCE) Act of 2003⁸⁵ were responses to these concerns.

The Digital Media Consumers' Rights Act and the BALANCE Act both sought to amend the anti-circumvention provisions of the DMCA to exempt circumventions that did not result in copyright infringement and circumventions undertaken for scientific investigation, and to exempt devices that would be necessary for such circumventions from the anti-trafficking provisions of 17 USC §1201. The BALANCE Act would also have added specific limitations on exclusive rights for digital works and would have amended the first sale doctrine to explicitly cover works stored in a digital format. Neither the Digital Media Consumers' Rights Act nor the BALANCE Act was ultimately enacted. Recent case law softening the anti-circumvention provisions of DMCA appears to make it less likely that legislation similar to the BALANCE Act will garner the required support to ensure future passage.

In the 109th Congress, the Family Entertainment and Copyright Act⁸⁶ would criminalize the unauthorized recording of movies in a movie theatre, strengthen and broaden the criminal copyright infringement provisions in Title 17, and improve protection for unreleased works historically prone to piracy before release (such as music CDs). The bill would also provide an exemption from infringement for home users who create temporary derivative works by using censorship technology to effectively remove content from copyrighted works. The Family Entertainment and Copyright Act passed the Senate and is currently in House committee.

Given the continued rise of peer-to-peer copyright infringement, the law concerning liability for those who provide the systems used for such infringement is sure to change. At this point, it remains unclear whether that change will come in the form of a Supreme Court ruling in *Grokster* or by way of congressional action.

⁸³ *MGM Studios v. Grokster*, 380 F3d 1154, 16 ILR (P&F) 361 (9th Cir 2004), cert. granted, 125 S. Ct. 686 (2004), p. 808, *infra*.

⁸⁴ Digital Media Consumers' Rights Act of 2002, H.R. 5544, 107th Cong. (2002), p. 3, *infra*.

⁸⁵ Benefit Authors without Limiting Advancement or Net Consumer Expectations (BALANCE) Act of 2003, H.R. 1066, 108th Cong. (2003), p. 175, *infra*.

⁸⁶ Family Entertainment and Copyright Act of 2005, H.R. 357, 109th Cong. (2005), p. 195, *infra*.