No. 04-3654

IN THE UNITED STATES COURT OF APPEALS
FOR THE EIGHTH CIRCUIT

DAVIDSON & ASSOCIATES, INC.,
d/b/a BLIZZARD ENTERTAINMENT, *et al.*,

Plaintiffs/Appellees,

v.

INTERNET GATEWAY, INC., *et al.*,

Defendants/Appellants.

On appeal from a final judgment of the United States District Court for the Eastern District of Missouri

BRIEF OF *AMICI CURIAE* ENTERTAINMENT SOFTWARE ASSOCIATION, RECORDING INDUSTRY ASSOCIATION OF AMERICA, AND MOTION PICTURE ASSOCIATION OF AMERICA IN SUPPORT OF APPELLEES AND AFFIRMANCE

Frederic Hirsch
Chun T. Wright
ENTERTAINMENT SOFTWARE ASSOCIATION
1211 Connecticut Avenue, N.W.
Suite 600
Washington, DC 20036
tel. (202) 223-2400
fax. (202) 223-2401

Counsel for Amicus Curiae the Entertainment Software Association

Paul M. Smith
Katherine A. Fallow
David Fagundes
JENNER & BLOCK LLP
601 13th Street NW, Suite 1200
Washington, DC 20005
tel. (202) 639-6000
fax (202) 639-6066

Counsel for Amici Curiae

[additional counsel listed on inside cover]

March 3, 2005

Stanley Pierre-Louis
RECORDING INDUSTRY ASSOCIATION
OF AMERICA, INC.
1330 Connecticut Avenue, N.W.
Suite 300
Washington, DC 20036
tel. (202) 857-9641
fax. (202) 775-7253

Counsel for Amicus Curiae the
Recording Industry Association of America

CORPORATE DISCLOSURE STATEMENT

Amicus the **Entertainment Software Association** ("ESA") is a nonprofit trade association dedicated to serving the business and public affairs needs of companies that publish video games for game consoles, personal computers, handheld devices, and the Internet. The ESA has no parent corporation. The ESA has issued no stock to the public and hence has no shareholders.

Amicus the **Recording Industry Association of America** ("RIAA") is the trade association that represents the United States sound recording industry. Its members are record companies in the United States that collectively create, manufacture or distribute approximately ninety percent (90%) of all legitimate sound recordings that are produced and sold in the United States. The RIAA has no parent corporation. The RIAA has issued no stock to the public and hence has no shareholders.

Amicus the Motion Picture Association of America, Inc. ("MPAA"), is a not-for-profit trade association founded in 1922 to address issues of concern to the United States motion picture industry. The MPAA has no parent corporation. The MPAA has issued no stock to the public and hence has no shareholders.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIALS

MISCELLANEOUS

STATEMENT OF INTEREST OF *AMICI CURIAE*

The companies represented by *amici* include the leading creators and providers of copyrighted works in the United States, and indeed the world. *Amici*'s members create a wide range of copyrighted works, including entertainment software, sound recordings, and audio-visual works. *Amici*'s members invest an enormous amount of time and resources in their intellectual property. For example, to bring one video game to market typically requires a team of twenty to as many as several hundred highly skilled professionals (including writers, animators, musicians, sound engineers, software engineers, and programmers) to work together for two to three years. Today, the average cost to develop a high-end game can easily range from $20 million to more than $40 million. On top of these costs, successful marketing and distribution efforts require an additional outlay of millions of dollars per title.

Amici, like the rest of the copyright industries, make an enormous contribution to the nation's culture and economy. Overall, copyright industries contributed 6% of the United States' gross domestic product in 2002, an amount roughly equal to the total expenditures and investments of the entire federal government in that same year. *See* Stephen E. Siwek, International Intellectual Property Association, *Copyright Industries in the*

U.S. Economy: The 2004 Report, iii, iv (2004) (available at http://www.iipa.com/pdf/2004_SIWEK_FULL.pdf). Copyright industries have created hundreds of thousands of highly skilled jobs in both the technology and creative sectors, generating an employment growth rate between 1997 and 2002 that was 130% greater than the U.S. employment growth rate during the same period. *Id.* at v.

Since the enactment of the Digital Millennium Copyright Act ("DMCA"), *amici* have made an ever-expanding variety of copyrighted materials available in digital format. As a result, more copyrighted materials, including computer programs, entertainment software, sound recordings, and audio-visual works are available to the public than ever before. The video game industry has seen the introduction of major new home and handheld game platforms, and significant growth in online games. The use of DVDs had grown exponentially, with a DVD player in nearly 50 million American households. And various online services now offer vast catalogs of sound recordings for legal downloading.

This enormous and rapid growth in digital distribution of copyrighted material could not have occurred without technological measures to protect *amici*'s intellectual property. Those measures, in turn, would have no meaning without the legal backing of the DMCA's anti-circumvention

provisions. In this case, the Defendants seek an exemption from the anti-circumvention provisions that, if recognized, would lead to exactly the type of digital piracy and resulting harm the DMCA was enacted to prevent. *Amici* thus have a strong interest in the outcome of this case.

Amici file this brief with the consent of the parties.

BACKGROUND

A. Technological Protection Measures, Backed by the DMCA, Are Critical to *Amici*'s Ability to Distribute their Copyrighted Works to the Public in a Digital Format.

The digital revolution that sparked the extraordinary growth in copyright industries also created the tools for undermining it. Increasingly, content owners such as *amici* have sought to make their works available to the public through new and innovative means, such as streaming music and video, and the interactive online gaming involved in this case. But the ease with which copyrighted works can be accessed and sold via digital media has led to a correlative growth in the ease with which they can be stolen. In the absence of effective security protections, works created by *amici* can be copied without degradation of quality, and their content distributed virtually instantaneously over the Internet to millions of people around the globe.

Though difficult to measure, the scope of Internet piracy is vast and growing rapidly. For example, billions of dollars worth of illegal

entertainment software products currently exist in the global marketplace. *International and Domestic Intellectual Property Enforcement Hearing Before a Subcomm. of the Senate Comm. on Appropriations*, 108th Cong. at 17 (Apr. 29, 2004) (Statement of Douglas Lowenstein, President, Entertainment Software Association). Indeed, an online monitoring program undertaken by *amici* the Entertainment Software Association ("ESA") identified 130,000 violations of its members' copyrights in the year 2003 alone. *Id.* at 21. Faced with the steep costs imposed by digital piracy, many content providers who would otherwise engage in a profitable creative enterprise may simply choose not to invest in the creation of intellectual property at all.

To counter the threat of piracy, *amici*'s members employ a variety of technological protection measures to prevent unauthorized access to their intellectual property. These include password protection, encryption, digital locks, and digital rights management tools. Like the Plaintiffs in this case, many of *amici*'s members use CD keys and digital "secret handshakes" to protect against unauthorized access to their copyrighted works.

The use of technological measures to protect copyright owners' exclusive rights under the Copyright Act is not enough. Mindful "that the digital environment poses a unique threat to the rights of copyright owners,

and as such, necessitates protection against devices that undermine copyright interests," Congress passed the DMCA in 1998. H.R. Rep. No. 105-551 (II), at 25 (1998) ("H. Rep."). Congress recognized the enormous potential of the Internet to enhance commerce, stimulate job creation, and provide a previously unrealized wealth of information through innovative means to individuals worldwide. *See* S. Rep. No. 105-190, at 8 (1998) ("S. Rep."); *see also* H. Rep. at 21, 35-36. At the same time, however, Congress understood that the digital revolution sowed the seeds of its own potential destruction via piracy. "Due to the ease with which digital works can be copied and distributed worldwide virtually instantaneously, *copyright owners will hesitate to make their works readily available on the Internet without reasonable assurance that they will be protected against massive piracy*." S. Rep. at 8 (emphasis added).

"The DMCA therefore backed with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 435 (2d Cir. 2001). Two of those legal sanctions are relevant here. Section 1201(a)(1) prohibits any person from "circumvent[ing] a technological measure that effectively controls access to a work protected under" the Copyright Act. 17 U.S.C. § 1201(a)(1)(A).

Section 1201(a)(2) – an anti-trafficking provision – prohibits distribution of a product that is "primarily designed" for, "has only limited commercially significant purpose or use other than," or is marketed for, circumventing a technological measure that effectively controls access to a copyrighted work. *Id.* § 1201(a)(2).

The anti-circumvention provisions, like the rest of the DMCA, were designed to serve twin goals: "promoting the continued growth and development of electronic commerce; and protecting intellectual property rights." H. Rep. at 23. Congress expected these provisions to encourage copyright owners to make their works available online, which, in turn, would enrich the amount of such material available to the public:

> A thriving electronic marketplace provides new and powerful ways for the creators of intellectual property to make their works available to legitimate consumers in the digital environment. And a plentiful supply of intellectual property – whether in the form of software, music, movies, literature, or other works – drives the demand for a more flexible and efficient electronic marketplace.

Id.

B. Private Contracts Complement the DMCA's Provisions in Protecting Digitally Distributed Copyrighted Works.

Amici and other copyright owners supplement technological protection measures with another essential means of protecting digital copyright: private contracts that define the scope of the license granted by

the owner to the user. Private license agreements are critical to the ability of *amici* and the copyright industries generally to distribute their works to the public using digital means. These contracts – sometimes referred to as "clickwrap" or "shrinkwrap" agreements – set forth the terms and limitations under which the customer may use the copyrighted materials. The End User License Agreement ("EULA") and Term of Use Agreement ("TOU") used by Blizzard are typical of these agreements.

As with technological means for protecting copyrighted materials, *amici*'s private contracts are effective only to the extent that they are backed by meaningful legal enforcement. Courts have consistently upheld the validity of "clickwrap" and "shrinkwrap" licenses where there is a clear indication that users were aware of and consented to the terms of those licenses. *E.g.*, *ProCD v. Zeidenberg*, 86 F.3d 1447, 1449 (7th Cir. 1996); *I.Lan Sys., Inc., v. Netscout Serv. Level Corp.*, 183 F. Supp. 2d 328, 338 (D. Mass. 2002); *Hotmail Corp. v. Van$ Money Pie, Inc.*, No. C-98 JW PVT ENE, C98-20064 JW, 1998 WL 388389, *1 (N.D. Cal. Apr. 16, 1998); *Forrest v. Verizon Communications, Inc.*, 805 A.2d 1007, 1010-11 (D.C.

2002) (enforcing a clickwrap agreement and stressing that "[a] contract is no less a contract simply because it is entered into via a computer").[1]

C. The bnetd Project.

Like *amici*, Plaintiffs have invested substantial amounts of time, money, and resources into developing their copyrighted works. Plaintiffs' games may be played over the Internet in "Battle.net mode" by connecting to Blizzard's Battle.net servers. *Davidson & Assocs., Inc. v. Internet Gateway, Inc.*, 334 F. Supp. 2d 1164, 1168 (E.D. Mo. 2004). A user who plays Blizzard's games over the Internet accesses a number of features in the game software that are available only in Battle.net mode, such as the ability to join multiplayer games, participate in tournaments, record wins and losses, create password-protected accounts, and chat with other players. *Id.* The online features of Blizzard's games are critical to the games' value. In addition, Blizzard gains additional revenue from the online features through the display of ad banners to users during online play. *See id.* at 1172.

To protect this valuable intellectual property, Plaintiffs assigned each Blizzard CD-ROM a "CD Key," and designed a protocol under which the game software and the Battle.net server exchange a "secret handshake" each

---

[1] Courts may not enforce clickwrap agreements where the agreement does not provide the user an opportunity to manifest express assent to the terms of the licensing agreement. *See, e.g., Specht v. Netscape Communications Corp.*, 306 F.3d 17, 30-31 (2d Cir. 2002).

time a user attempts to access the online features of the games. *Id.* at 1169. The secret handshake, which is a type of authentication sequence commonly used in the industry, is designed to ensure that only individuals with authorized copies of Blizzard's games are allowed to access their online features. *Id.*

Defendants circumvented Plaintiffs' secret handshake and distributed the tools for doing the same to the public via the Internet. Known as the "bnetd" project, Defendants reverse engineered Plaintiffs' game software to create a program that allows individuals to play Blizzard's games over the Internet without connecting to Plaintiffs' Battle.net servers, by bypassing the secret handshake. *Id.* at 1173. Defendants reverse engineered Blizzard's games despite expressly agreeing not to reverse engineer when they assented to the terms of Blizzard's EULA and TOU. *Id.* at 1172-73. Defendants then created the bnetd "emulator" to supplant the means for online play of Blizzard games. Critically, by its very design the bnetd emulator *always* allows a user to bypass the "secret handshake." *Id.* at 1173.[2] As a result, individuals can play unauthorized Blizzard games online by accessing the

[2] In normal operation of the secret handshake, the Battle.net server "asks" the game software to provide a valid CD Key. If the CD Key is valid, the server will return an "OK" message to the software, and the player will be allowed to access the game's online features. *Id.* at 1169. By contrast, the bnetd emulator *always* sends an "OK" message to the software, regardless of whether the individual has supplied a valid CD Key. *Id.* at 1173.

bnetd emulator. Moreover, "[o]nce game play starts there is no difference between Battle.net and the bnetd emulator from the standpoint of a user who is actually playing the game." *Id.* at 1172.

SUMMARY OF ARGUMENT

This case implicates two critical tools – private user agreements and technological protection measures – that *amici* employ to protect their valuable copyrighted works and ensure the continued distribution of those works in a variety of innovative digital formats. The District Court concluded that Plaintiffs' private contracts with their users are fully enforceable, and not preempted by the Copyright Act. The District Court also held that Defendants violated the DMCA when they created a program that circumvented Plaintiffs' technological protection measures and enabled widespread piracy of Plaintiffs' games. Those decisions are correct and should be affirmed. Acceptance of Defendants' arguments to the contrary would threaten the ability of *amici* to protect their copyrighted works in a digital environment that is beset by piracy. Such an outcome would be plainly contrary to Congress' purpose in enacting the DMCA, and would undermine a system of private licensing agreements that is widely used by a multitude of industries. *Amici* thus urge the Court to affirm the district court's judgment.

1. Defendants' actions were barred by the plain terms of Blizzard's EULA and TOU, to which they expressly agreed. Plaintiffs' clickwrap agreements are of the type widely employed by *amici*, and courts across the country have held that such contracts are valid and enforceable. There is no support for Defendants' argument that the Copyright Act preempts Plaintiffs' contract claims. This Court has recognized that there is no general rule holding that the Copyright Act preempts state contract claims arising out of copyright licensing agreements, and there is no reason to hold Plaintiffs' agreements to a different standard. *See Nat'l Car Rental Sys., Inc. v. Computer Assocs. Int'l, Inc.*, 991 F.2d 426, 431-32 (8th Cir. 1993); *Bowers v. Baystate Techs., Inc.*, 320 F.3d 1317, 1323-26 (Fed. Cir.), *cert. denied*, 539 U.S. 928 (2003). These types of contracts allow *amici* to control the terms under which they license their intellectual property, and the enforceability of such contracts thus is critical to *amici*'s ability to distribute their works to the public digitally.

2. Even if Defendants' actions were not barred by the independent force of Plaintiffs' private contracts, they would be prohibited by the anti-circumvention provisions of the DMCA. Defendants' development of the bnetd project violates both the letter and spirit of the DMCA. The DMCA was enacted to facilitate a thriving electronic marketplace and to encourage

copyright owners such as *amici* to make their works available to the broadest sector of the public through digital means. To combat the digital piracy that threatened those statutory goals, the DMCA made it illegal to circumvent the technological means employed by copyright owners to protect their intellectual property.

Under a straightforward application of the law, Defendants violated the anti-circumvention and anti-trafficking provisions of the DMCA. 17 U.S.C. §§ 1201(a)(1), 1201(a)(2). Defendants circumvented the encrypted secret handshake used by Plaintiffs to control access to their copyrighted games, and made the means for circumventing Plaintiffs' protection measures available to the world over the Internet.

Defendants fall far short of qualifying for the narrow exemption to liability contained in § 1201(f). That section was designed to allow legitimate reverse engineering for the "sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability with an independently created computer program." *Id.* § 1201(f)(1). Intended to foster "innovation and competition," the exemption does not apply where, as here, the Defendants have engaged in reverse engineering to create a program that does nothing more than supplant Plaintiffs' copyrighted work, and enables wide-scale piracy of

Plaintiffs' games. Applying the exemption to Defendants here would eviscerate the DMCA's anti-circumvention provisions. Congress surely did not intend that result when it adopted the narrow exemption in § 1201(f).

ARGUMENT

I. PLAINTIFFS' END USER AGREEMENTS, TYPICAL OF THE PRIVATE CONTRACTS WIDELY USED BY *AMICI*, ARE NOT PREEMPTED BY THE COPYRIGHT ACT.

As explained above, *amici's* members depend on user agreements such as the EULA and TOU at issue here as a critical means of protecting their intellectual property. Courts have consistently upheld these contracts where, as here, they provide users a full opportunity to assent. *See supra* at 7-8. Defendants argue nevertheless that the provisions in Blizzard's EULA and TOU restricting the ability to engage in reverse engineering and prohibiting emulators and matchmaking services are preempted by the Copyright Act. That argument is meritless. By assenting to the terms of Blizzard's EULA and TOU, Defendants agreed to certain contractual rights and obligations that are separate from – but consistent with – federal copyright law, and are therefore fully enforceable.

This Court has squarely rejected the contention that contract claims arising from a copyright license agreement are preempted by the Copyright Act as a general matter. *Nat'l Car Rental Sys.*, 991 F.2d at 431-32. In

National Car Rental, the Court held that the Copyright Act preempts only those state law claims that are "equivalent to the exclusive rights under copyright." *Id.* at 431. If, however, a contract adds an "extra element" to the copyright rights, a claim for breach of that contract is not preempted. *Id.*; *see also, e.g., Wrench LLC v. Taco Bell Corp.*, 256 F.3d 446, 457 (6th Cir. 2001); *ProCD, Inc.*, 86 F.3d at 1454; *Taquino v. Teledyne Monarch Rubber*, 893 F.2d 1488, 1501 (5th Cir. 1990); *Acorn Structures, Inc. v. Swantz*, 846 F.2d 923, 926 (4th Cir. 1988).

Applying the "extra element" test in a case virtually indistinguishable from this one, the Federal Circuit held that the Copyright Act does not preempt a prohibition on reverse engineering contained in a software shrinkwrap agreement. *Bowers*, 320 F.3d at 1323-26 (citing *Nat'l Car Rental*, among others, for the proposition that the Copyright Act "does not preempt contractual constraints on copyrighted" works).[3] The Federal Circuit held that "mutual assent and consideration" required by the plaintiff's shrinkwrap agreement rendered its claims "qualitatively different from copyright infringement." *Id.* at 1325. In so holding, the *Bowers* court noted that individuals could, by contract, waive affirmative defenses and

[3] *Amici* disagree with *Bowers*, however, to the extent it suggests that running a program in the ordinary intended manner and observing how it works constitutes reverse engineering. *See id.* at 1326.

statutory rights. *Id.* The court thus concluded that "private parties are free to contractually forego the limited ability to reverse engineer a software product under the exemptions of the Copyright Act." *Id.* at 1325-26.

There is no merit whatsoever to Defendants' attempts to distinguish *Bowers*. Defendants argue that the *Bowers* court addressed only statutory preemption, and failed to consider the conflict preemption argument they advance here. Appellants' Br. at 32-33. But the court in *Bowers* carefully considered whether its decision would frustrate the federal policies underlying fair use more generally, and concluded that it would not. 320 F.3d at 1325 (emphasizing that the decision to enforce private contractual agreements not to engage in reverse engineering leaves "untouched" the general principle that some reverse engineering constitutes fair use).

Nor does the Fifth Circuit's decision in *Vault Corp. v. Quaid Software, Ltd.*, 847 F.2d 255, 268-69 (5th Cir. 1988), countenance a different result. In *Vault Corp.*, the court invalidated a license agreement that was drafted in accordance with a Louisiana law prohibiting *all* copying of a computer program. *Vault Corp.* dealt with a provision of public law that, because of its generally applicable character, could reasonably be understood to be in tension with federal policy. By contrast, clickwrap and shrinkwrap agreements are private contracts that by their nature cannot

frustrate the objectives of federal law because they create no generally applicable law and thus do not affect nonparties. *Bowers*, 320 F.3d at 1325 (holding *Vault Corp.* inapplicable to shrinkwrap agreements because its holding does not "extend . . . to include private contractual arrangements supported by mutual assent and consideration"); *accord ProCD*, 86 F.3d at 1454 ("A copyright is a right against the world. Contracts, by contrast, generally affect only their parties; strangers may do as they please, so contracts do not create 'exclusive rights.'").

This Court should adopt the reasoning in *Bowers*, which is consistent with this Court's decision in *National Car Rental*, and in line with the overwhelming majority of courts to have considered similar preemption arguments. On the other hand, rejecting *Bowers* and invalidating the licensing agreements on federal preemption grounds would create an anomaly in federal law, which routinely permits private parties to engage in waivers of rights through contract. *E.g.*, *Trinity Universal Ins. Co. v. Smithwick*, 222 F.2d 16, 22 (8th Cir. 1955) ("Generally speaking, . . . a person may by contract waive a right given to him by law . . . ."); *Metropolitan Edison Co. v. NLRB*, 460 U.S. 693, 705-06 (1983) (holding that unions may contractually waive members' statutory rights); *Curtis*

Publishing Co. v. Butts, 388 U.S. 130, 142-44 (1967) (permitting waiver of First Amendment speech rights).

A holding that reverse engineering, unlike other federal statutory rights, cannot be waived by private contract would not only be out of step with longstanding precedent, but would render *amici* uncertain of the extent to which courts will enforce the EULAs and TOUs on which they depend for protection of their intellectual property. As a result of this uncertainty, *amici* and other copyright owners who rely on such agreements would be reluctant to make their works available in a universe that is so prone to piracy and abuse of copyright licenses.

II. DEFENDANTS VIOLATED THE DMCA.

A. The Bnetd Project Is Precisely What the DMCA's Anti-Circumvention Measures Were Designed to Prevent.

Defendants circumvented the encrypted "secret handshake" that Blizzard uses to control access to the Battle.net version of its copyrighted games. Defendants then made available to the public the tools for circumventing Blizzard's technological protection measures. Defendants' programs enable individuals who have unlawfully copied Blizzard's games to access the online features of the games in an environment that is indistinguishable from Battle.net. This is exactly the conduct the DMCA's anti-circumvention provisions were designed to prevent.

The encrypted "secret handshake" used by Blizzard – *typical of the digital locks* used by *amici* – is precisely the kind of access control protected by the DMCA's anti-circumvention measures. *See RealNetworks, Inc. v. Streambox, Inc.*, No. 2:99CV02070, 2000 WL 127311, *7 (W.D. Wash. Jan. 18, 2000) (holding that secret handshake is a device that controls access within the meaning of § 1201); *Sony Computer Entm't Am., Inc. v. Gamemasters*, 87 F. Supp. 2d 976, 987 (N.D. Cal. 1999) (concluding that mechanism that verifies encrypted data from CD-ROM before allowing game to play on console was a technological measure that "effectively controls access" under § 1201(a)(2)); *Corley*, 273 F.3d at 436-37 (finding breach of DMCA where defendants circumvented authentication sequence used by movie studios to permit playing of DVDs only on authorized devices); *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1095 (N.D. Cal. 2004) (same). Bnetd, by providing a way for unauthorized users to access Blizzard's games in Battle.net mode, bypassed the secret handshake, and in so doing committed an archetypal violation of the DMCA's anti-circumvention provisions.

Defendants attempt to avoid this straightforward analysis with a pair of unconvincing arguments. Defendants first argue that Blizzard's secret handshake does not control access to a work protected by copyright.

Appellants' Br. at 52-57. But as Plaintiffs have made clear, the authentication sequence controls access to their copyrighted games in online play. "[I]n the ordinary course of its operation," 17 U.S.C. § 1201(a)(3)(B), Blizzard's authentication sequence controls the circumstances under which an individual is able to access the features of Blizzard games available on online mode – *e.g.*, the audio and visual manifestations accompanying multiple player games and tournaments, the password-protected accounts, and the icons unique to Battle.net mode. Thus, as in *Corley*, *321 Studios*, and *Gamemasters*, the copyrighted work being protected is the expressive content of the video game or DVD.

When Plaintiffs' DMCA claim is correctly understood, it becomes clear that the authority on which Defendants rely so heavily, *Lexmark International, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004), is inapposite. In *Lexmark*, the defendant developed a microchip that enabled third party toner cartridges to interoperate with plaintiff's printers, and included in that chip a means of circumventing the secret handshake used by plaintiff's printers to prevent use of such unapproved cartridges. *Id.* at 530-31. Finding that plaintiff's secret handshake protected computer code that was solely functional, the court held that the defendant did not circumvent the technological protection measure in order to access

any copyrighted expression, but only to access the printer *functions* enabled by the underlying computer code. *Id.* at 547-49.[4] Here, by contrast, Defendants' circumvention of Blizzard's authentication sequence directly accessed copyrighted expression that Blizzard intended to protect: the online features of Blizzard games. Indeed, the court in *Lexmark* was careful to distinguish its holding from those instances in which the technological measure protects computer code that produces "protected expression." *Id.* at 548 ("*Unlike the code underlying video games or DVDs*, 'using' or executing the Printer Engine Program does not in turn create any protected expression.") (emphasis added). As the court explained, "[i]n the essential setting where the DMCA applies, the copyright protection operates on two planes: in the literal code governing the work and in the visual or audio manifestation generated by the code's execution." *Id.* Where, as here, a technological measure guards computer software that "translate[s] into some

[4] Defendants' argument is based on a fundamental misreading of the *Lexmark* decision. Defendants assert that *Lexmark* stands for the proposition that a *secret handshake* is a "lock-out code" that is not protected by the Copyright Act. *See* Appellants' Br. at 55-57. But the Sixth Circuit's holding with respect to the "lock-out code" involved the Toner Loading Program, not the separate secret handshake; and the "lock-out code" discussion dealt with Lexmark's copyright infringement claim, not the DMCA claim at issue here. *Lexmark*, 387 F.3d at 537-41. Having concluded that the Toner Loading Program was not protected by copyright, the Sixth Circuit held that the secret handshake, to the extent it was designed to protect the Toner Loading Program, did not control access to a protected work, and thus did not qualify for protection under § 1201(a)(2). *Id.* at 550.

other visual and audio manifestation," the DMCA's anti-circumvention measures plainly apply. *Id.*

Defendants' other argument – that the secret handshake does not "effectively control[] access" to its copyrighted works because the object code for Blizzard games can be read directly from the game CD-ROMs – is similarly misplaced. Although licensees of Blizzard software may have access to the object code of games because it is written onto the CD-ROMs sold to licensees, that is irrelevant because the copyrighted work to which the secret handshake controls access is not merely the code itself but instead the distinctive images, action, and sounds of Blizzard games when played in Battle.net mode. As the Sixth Circuit explained in *Lexmark*, where "the program commands in software for video games or computers translate into some other visual and audio manifestation[,] . . . restricting 'use' of the work means restricting customers from making use of the copyrightable expression in the work." *Id.*

Defendants' cramped reading of what constitutes a measure that "effectively controls" access to a copyrighted work simply cannot be squared with the statutory language. The DMCA specifies that a measure effectively controls access "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." 17 U.S.C. § 1201(a)(3)(B). Here, "in the ordinary course of its operation," Blizzard's authentication sequence requires "the application of information," "or a process or a treatment," in order to gain access to the audio and visual manifestations of the online features of Blizzard's games. A user ordinarily cannot access these expressive features without successfully engaging in the secret handshake. Therefore, it makes no difference for purposes of the DMCA that the games' object code could conceivably be read from the CD-ROMs – what matters is that the secret handshake controls access to the copyrighted expression.[5]

B. Defendants' Actions Do Not Qualify for the Narrow Statutory Exemption for Reverse Engineering.

Despite having distributed a program that enables widespread piracy of Blizzard's games, Defendants argue that they are nevertheless exempt from liability under the DMCA's statutory exemption for reverse

---

[5] Properly read, *Lexmark* stands for the proposition that an authentication sequence that controls access to readable object code, which produces only a non-copyrighted function (*e.g.*, running a printer), does not qualify for protection under the DMCA. 387 F.3d at 546-48. To the extent that *Lexmark* can be read to hold, as Defendants argue, that a technological measure that controls access to copyrighted expression, but allows access to the literal code that produces the expression, is not entitled to protection under the DMCA, then it should be rejected by this Court as wrongly decided and inconsistent with what even the Sixth Circuit recognized was the "essential setting" of the DMCA – protection of the digital distribution of video games, music, video, and business software.

engineering. Defendants' argument, if accepted, would undermine the very purpose of the anti-circumvention provisions, and would discourage *amici* from making a rich array of copyrighted works available in digital format. Where, as here, the Defendants engaged in reverse engineering to create and distribute a program that allows individuals to play unauthorized copies of Plaintiffs' games in an online format that to the user is indistinguishable from Plaintiffs' proprietary one, the narrow exemption found in § 1201(f) is unavailable.

1. The Reverse Engineering Provision.

Section § 1201(f) sets forth the very limited circumstances under which an individual may engage in circumvention, notwithstanding the prohibitions of § 1201(a). Section 1201(f)(1) provides an exception to the anti-circumvention provision of § 1201(a)(1). Thus, an individual

> 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 the interoperability 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.

17 U.S.C. § 1201(f)(1). Sections 1201(f)(2) and (f)(3) allow individuals to develop circumvention tools notwithstanding the anti-trafficking provisions, and in certain very limited circumstances allow an individual to share

circumvention tools with third parties "for the sole purpose" of achieving legitimate interoperability. *Id.* § 1201(f)(2) & (f)(3).

The reverse engineering exceptions to the DMCA were "intended to allow legitimate software developers to continue engaging in certain activities for the purpose of achieving interoperability . . . ." House Comm. on the Judiciary, 105th Cong., Section-by-Section Analysis of H.R. 2281 as Passed by the House on Aug. 4, 1998 14 (Comm. Print Sept. 1998) ("H.R. Comm"). However, the product that results from the reverse engineering "must be a new and original work, not infringing the original computer program." *Id.* "Finally, the goal of this section is to ensure that current law is not changed, and not to permit infringement." *Id.* at 15.

Congress did not intend for § 1201(f)(3) to create the kind of loophole to liability sought by Defendants. *See* Appellants' Br. at 41 (invoking the protections of § 1201(f)(3)). The legislative history makes clear that the scope of § 1201(f)(3) is quite narrow. That subsection:

> allows developers of independently created software to rely on third parties either to develop the necessary circumvention tools or to identify the necessary information to achieve interoperability. The ability to rely on third parties is particularly important for small software developers who do not have the capability of performing these functions in-house. This provision permits such sharing of information and tools.

H.R. Comm. at 15. Thus, there is no support for the argument that in adopting § 1201(f)(3), Congress intended to create an exception to the anti-trafficking provisions that would essentially swallow the rule. Indeed,

> [r]ecognizing, however, that making circumvention information or tools generally available would undermine the objectives of this Act, the provision imposes strict limitations. Sharing information and tools is permitted solely for the purpose of achieving interoperability of an independently created computer program with other programs. If a person makes this information available for another purpose, he is not covered by this exemption.

Id.

2. The Bnetd Project – Which Merely Supplants Blizzard's Copyrighted Works and Enables Rampant Piracy of Blizzard's Games – Does Not Meet the Statutory Definition of Reverse Engineering.

Defendants' actions fundamentally do not qualify for the narrow statutory exception for reverse engineering. By creating and distributing a program that allows anyone to circumvent Blizzard's secret handshake – in other words, distributing the means to pick Blizzard's digital lock – Defendants violated the plain meaning and underlying principles of the DMCA. As noted above, the DMCA was enacted to encourage the distribution of copyrighted works through digital means, and the anti-circumvention provisions serve this statutory purpose by protecting copyright owners against digital piracy. Congress exempted from DMCA liability legitimate reverse engineering that contributes to competition and

innovation in the computer software industry. Defendants' bnetd project – which facilitates piracy and contributes nothing to competition and innovation in the industry – undermines the statutory goals, and therefore cannot qualify as legitimate reverse engineering under § 1201(f).[6]

a. Creation of a program, like the bnetd project, that knowingly enables wide-scale piracy of copyrighted works, does not satisfy the requirements of § 1201(f).

Defendants created a program that will always allow individuals to bypass Blizzard's secret handshake and enable them to play Blizzard's games without using Battle.net – and without, for example, being exposed to the banner ads displayed to users of Battle.net. The program created by Defendants incorporated copyrighted elements from the Battle.net server program (such as copyrighted icons). Defendants then distributed that program to the world via the Internet. Taken together, these various goals show that Defendants did not reverse engineer Blizzard's authentication sequence for the "sole purpose of identifying and analyzing those elements

---

[6] Defendants cannot take advantage of the reverse engineering exemption for the additional reason that Defendants incorporated Blizzard's copyrighted materials, such as copyrighted icons unique to Battle.net mode, into their circumvention program. *See* Consent Decree ¶ 1 ("Copyrighted materials created by Blizzard, including code, files and images from Blizzard's Battle.net server and game clients, were duplicated and incorporated into Defendants' bnetd server program without Blizzard's authorization[.]");17 U.S.C. § 1201(f) (permissible reverse engineering must "not constitute infringement under this title").

of the program that are necessary to achieve the interoperability of an independently created computer program with other programs." 17 U.S.C. § 1201(f)(1); *Davidson & Assocs.*, 334 F. Supp. 2d at 1185.

Defendants' contrary interpretation of the § 1201(f) exemption would, if accepted, eviscerate the anti-circumvention provisions. Defendants essentially argue that the "sole purpose" test is limited to scrutiny of the individual's immediate motivation for engaging in reverse engineering. *See* Appellants' Br. at 45-48. But under that reading, anyone who sought to create and/or distribute software that circumvented technological protection measures could escape liability under the DMCA merely by stating that his intent was to achieve interoperability of the circumvention tool. Indeed, under Defendants' reading, the reverse engineering provision would exempt the DVD-copying software that courts repeatedly have held violate the DMCA, simply because the developers of such software could argue that they reverse engineered the DVD protection measures in order to play DVDs on a non-authorized software player. *See Corley*, 273 F.3d at 443-45, 459-60.[7]

---

[7] *See also Universal Studios, Inc. v. Remeirdes*, 111 F. Supp. 2d 294, 319, 320 (S.D.N.Y. 2000) (§ 1201(f) did not exempt development of "DeCSS" software, which circumvented DVD protection measures, even though developers claimed they sought only to enable interoperability with Linux operating system; fact that developers were aware that DeCSS could enable

The legislative history surrounding § 1201(f) demonstrates, moreover, that in allowing software developers to share circumvention tools and information with certain "third parties," Congress did not intend to adopt a wholesale exception to the anti-circumvention and anti-trafficking provisions. In fact, the right to distribute the results of such study is limited to situations where the purpose of the distribution is itself to enable interoperability as opposed to enabling circumvention. 17 U.S.C. § 1201(f)(3).

Endowing Defendants with immunity under the DMCA's reverse engineering exemption would undermine the statute's primary goals of protecting against digital piracy and encouraging innovation. Far from enriching the digital marketplace, emulators such as bnetd threaten to attenuate this marketplace by providing free substitutes to the intellectual property created by online digital businesses. If courts permit such alternatives to exist, *amici* and others in the copyright industries will have far fewer incentives to make their works available in the digital marketplace because the existence of emulators will significantly diminish their ability to earn a profit from their work. This was precisely the risk to Internet commerce that Congress created the DMCA to prevent. S. Rep. at 8; *see*

---

interoperability with other, unauthorized systems, demonstrated that analyzing elements for interoperability was not developers' "sole purpose").

also S. Rep. at 65 (additional statement of Mr. Leahy) ("The future growth of computer networks like the Internet and of digital, electronic communications requires [protection of technological protection measures]. Otherwise, owners of intellectual property will be unwilling to put their material online. If there is no content worth reading online, the growth of this medium will be stifled, and public accessibility will be retarded.").

b. The bnetd project is not an "independently created computer program" for purposes of § 1201(f).

As the District Court found, the bnetd program was designed to act as a mere substitute for the Battle.net service, not as a new and original work. *See Davidson & Assocs.*, 334 F. Supp. 2d at 1185. Therefore, the District Court correctly concluded, the bnetd project was not an "independently created computer program" within the meaning of § 1201(f).

The District Court's conclusion is consistent with the language and purpose of the DMCA. The purpose of the reverse engineering provision, like the statute's overall purpose, was to "foster competition and innovation in the computer and software industry." S. Rep. at 13. The section therefore includes the phrase "independently created" to ensure that only reverse engineering that led to devices with some basic quantum of originality would merit an exemption from the DMCA's anti-circumvention and anti-

trafficking provisions. Thus, "[t]he resulting product [of reverse engineering] must be a *new and original* work" to qualify for the exemption. S. Rep. at 32 (emphasis added). Works such as the bnetd program, which merely supplants the means for online play of Blizzard's games, can stake no claim to "contribut[ing] significantly to the growth of markets for works of the imagination." H. Rep. at 24.

This interpretation of § 1201(f) is consistent with the balance struck by Congress in enacting the anti-circumvention provisions and their limited exceptions. Congress recognized the possible tension between the statute's twin goals of "promoting the continued growth and development of electronic commerce; and protecting intellectual property rights." H. Rep. at 23. Congress sought to balance these goals by protecting the investments of intellectual property owners while also permitting enough access to information to assure that the Internet would continue to function as an engine of growth. *Id.* at 21. Where, as here, Defendants have engaged in reverse engineering to create nothing more than a mere imitation of the

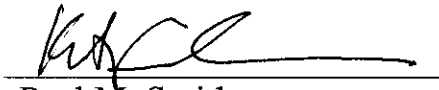
copyright owner's works, their actions fall outside the statutory exemption created by Congress to achieve this careful balance.[8]

[8] Defendants' arguments about reverse engineering as fair use are inapposite, because Plaintiffs are claiming violations of the DMCA, not copyright infringement. In any event, Defendant's reverse engineering would not qualify as fair use under *Sega Enterprises, Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992), or *Sony Computer Entertainment, Inc. v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000). Unlike in *Sega*, where the Ninth Circuit held that the defendant's reverse engineering constituted fair use because the video games that resulted presented a saleable alternative to defendant's products and thereby enriched the variety of creative works available to the public, 977 F.2d at 1522-23, bnetd merely supplants Blizzard's product, allowing individuals to play Blizzard games in Battle.net mode without performing the secret handshake – indeed, without even purchasing Blizzard's games. Bnetd thus undermines rather than enhances competition. Likewise, the bnetd project does not even meet the minimum standard of originality set by *Connectix*, which required that for an emulator to be original it at least had to enable game play through a distinctive medium. 203 F.3d at 606.

CONCLUSION

For the foregoing reasons, the decision of the District Court should be affirmed.

Respectfully submitted,



Paul M. Smith
Katherine A. Fallow
David Fagundes
JENNER & BLOCK LLP
601 Thirteenth Street, NW
Suite 1200 South
Washington, DC 20005
tel. (202) 639-6000
fax (202) 639-6066

Counsel for Amici Curiae

Frederic Hirsch
Chun T. Wright
ENTERTAINMENT SOFTWARE ASSOCIATION
1211 Connecticut Avenue, N.W.
Suite 600
Washington, DC 20036
tel. (202) 223-2400
fax. (202) 223-2401

Counsel for Amicus Curiae the Entertainment Software Association

Stanley Pierre-Louis
RECORDING INDUSTRY ASSOCIATION OF AMERICA, INC.
1330 Connecticut Avenue, N.W., Ste. 300
Washington, DC 20036
tel. (202) 857-9641
fax. (202) 775-7253

Counsel for Amicus Curiae the Recording Industry Association of America

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the type-volume limitation set forth in Fed. R. App. P. 32(a)(7)(B) because it contains 6,820 words, not including the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief also complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6), because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 1997-2002 in 14-point Times New Roman.

I certify that the file containing the foregoing Brief for Amici Curiae, which was copied to a CD-ROM disk and filed and served, has been scanned for viruses and that it is virus-free.

Katherine A. Fallow

ADDENDUM

International and Domestic Intellectual Property Enforcement Hearing Before a Subcomm. of the Senate Comm. on Appropriations, 108th Cong. at 17 (Apr. 29, 2004) (Statement of Douglas Lowenstein, President, Entertainment Software Association).

S. HRG. 108–632

INTERNATIONAL AND DOMESTIC INTELLECTUAL PROPERTY ENFORCEMENT

HEARING

BEFORE A

SUBCOMMITTEE OF THE

COMMITTEE ON APPROPRIATIONS

UNITED STATES SENATE

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

SPECIAL HEARING

APRIL 29, 2004—WASHINGTON, DC

Printed for the use of the Committee on Appropriations

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

93–984 PDF WASHINGTON : 2004

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON APPROPRIATIONS

TED STEVENS, Alaska, *Chairman*

THAD COCHRAN, Mississippi	ROBERT C. BYRD, West Virginia
ARLEN SPECTER, Pennsylvania	DANIEL K. INOUYE, Hawaii
PETE V. DOMENICI, New Mexico	ERNEST F. HOLLINGS, South Carolina
CHRISTOPHER S. BOND, Missouri	PATRICK J. LEAHY, Vermont
MITCH McCONNELL, Kentucky	TOM HARKIN, Iowa
CONRAD BURNS, Montana	BARBARA A. MIKULSKI, Maryland
RICHARD C. SHELBY, Alabama	HARRY REID, Nevada
JUDD GREGG, New Hampshire	HERB KOHL, Wisconsin
ROBERT F. BENNETT, Utah	PATTY MURRAY, Washington
BEN NIGHTHORSE CAMPBELL, Colorado	BYRON L. DORGAN, North Dakota
LARRY CRAIG, Idaho	DIANNE FEINSTEIN, California
KAY BAILEY HUTCHISON, Texas	RICHARD J. DURBIN, Illinois
MIKE DEWINE, Ohio	TIM JOHNSON, South Dakota
SAM BROWNBACK, Kansas	MARY L. LANDRIEU, Louisiana

JAMES W. MORHARD, *Staff Director*
LISA SUTHERLAND, *Deputy Staff Director*
TERRENCE E. SAUVAIN, *Minority Staff Director*

SUBCOMMITTEE ON COMMERCE, JUSTICE, AND STATE, THE JUDICIARY, AND RELATED AGENCIES

JUDD GREGG, New Hampshire, *Chairman*

TED STEVENS, Alaska	ERNEST F. HOLLINGS, South Carolina
PETE V. DOMENICI, New Mexico	DANIEL K. INOUYE, Hawaii
MITCH McCONNELL, Kentucky	BARBARA A. MIKULSKI, Maryland
KAY BAILEY HUTCHISON, Texas	PATRICK J. LEAHY, Vermont
BEN NIGHTHORSE CAMPBELL, Colorado	HERB KOHL, Wisconsin
SAM BROWNBACK, Kansas	PATTY MURRAY, Washington
	ROBERT C. BYRD, West Virginia (ex officio)

Professional Staff
SCOTT GUDES
KATHERINE HENNESSEY
DENNIS BALKHAM
JILL SHAPIRO LONG
SHANNON O'KEEFE
LILA HELMS *(Minority)*
KATE ELTRICH *(Minority)*
CHAD SCHULKEN *(Minority)*

Administrative Support
JESSICA ROBERTS

CONTENTS

STATEMENT OF DOUGLAS LOWENSTEIN, PRESIDENT, ENTERTAINMENT SOFTWARE ASSOCIATION

Mr. LOWENSTEIN. Thank you, Mr. Chairman. I would like to start, I think I have testified over the years about 10 or 15 times on a panel with Jack Valenti and I am fearful that this may be the last time, so I just want to say what a privilege it has been to follow you all the time. And the problem with following Jack is one tends to simply want to say, I agree with what he said, and move on, and he usually says it better, so indulge me if I say some of the same things but perhaps not as articulately.

I do appreciate the opportunity to share the views of the American video game industry on the U.S. Government's efforts to control intellectual property piracy. Worldwide video game revenues now exceed $25 billion and the industry has been the fastest growing of all entertainment sectors since the late 1990s. With the average age of game players now 29, the industry is poised to sustain double-digit growth in the next 5 years, and the growth potential is even greater if we can begin to open up the vast expanses of markets currently closed due to rapid piracy.

The typical video game now costs between $5 and $10 million to make, often double that, and 2 or 3 years of development time. But the opportunity to recover this investment through sales in Asia, Eastern Europe, the Middle East, and Central and South America is virtually nonexistent. Piracy rates in these regions are at 80 percent and sometimes 90 percent or even higher, and they serve as an effective barrier to entry, let alone to the establishment of a viable, legitimate market.

The value of pirated products circulating in these markets is easily in the billions. Piracy in these regions includes illegal optical disk and video game cartridge replication and manufacturing facilities, the mass exporting of pirated games, Internet piracy, and so-called burn-to-order operations. In many cases, organized criminal enterprises are at the center of the global piracy and counterfeit rings.

Our members are aggressive and proactive on the anti-piracy front, but unfortunately, our efforts alone are not enough. For this reason, we have been grateful for the engagement of the Congress and in particular this subcommittee and several executive branch agencies, including the State Department, the Commerce Department, the U.S. Trade Representative, and the Department of Justice in the global anti-piracy campaign.

But I submit to you that the investment our Government makes in protecting the intellectual property assets of America's creative industries ultimately enhances this Nation's economic growth and vitality. For every dollar invested to protect entertainment software or movies or music or business software, every dollar invested to protect those products from piracy promotes export sales, contributes to a positive balance of trade, and the continued creation by our industry of highly skilled, well-paying jobs right here in the United States. In fact, about 40 to 50 percent of the revenue of a typical game company comes from overseas sales.

Let me briefly highlight some recommendations that we think would build on the good work done to date by this committee, the

subcommittee, and the Government agencies engaged in the fight to protect U.S. intellectual property.

First, we recommend that the subcommittee provide additional resources for USTR to hire personnel dedicated to monitoring and enforcing compliance by signatory countries with the multilateral agreements and recent bilateral agreements, such as the new FTAs with Australia, Singapore, Morocco, and so forth. It is critical to recognize—critical—that negotiating agreements is only the beginning of the process, not the end.

Second, we recommend that the subcommittee provide additional resources dedicated to intellectual property investigations by the Department of Justice, including the Computer Fraud and Intellectual Property Section and the various CHIPs units in several U.S. Attorneys' offices. DOJ's announcement last week, as we have said, Operation Fastlink, offers impressive evidence of the value of this kind of investment. Fastlink was an investigation whose roots actually involved game piracy and it resulted in the take-down of more than 200 computers in the United States and 10 other countries.

Third, we recommend additional resources for the FBI to train more agents to pursue intellectual property investigations into the larger-scale Internet and hard goods piracy operations. Such investigations are the key to smashing the global piracy syndicates.

Finally, we recommend that the subcommittee provide resources for U.S. law enforcement agencies to coordinate investigative operations against criminal organizations involved in large-scale factory-level manufacturing of pirated game product in Asia and Eastern Europe.

Given America's leadership in the field of law enforcement in this area and the inadequate capabilities in many countries where piracy flourishes, the simple fact is that if the United States does not lead this enforcement effort against the organized criminal syndicates that are at the root of the global piracy problem, genuine long-term progress will be difficult to achieve.

Mr. Chairman, the U.S. Government has been a strong and effective partner in the battle against global entertainment software piracy, but it is equally clear that the global piracy problem remains deeply entrenched and that it directly endangers America's economic security, as U.S. companies' survival in potential markets close off due to the proliferated of pirated and counterfeit goods. We need your continued help. We thank you for your continued interest and support.

Senator GREGG. Thank you.

[The statement follows:]

PREPARED STATEMENT OF DOUGLAS LOWENSTEIN

INTRODUCTION

Mr. Chairman and members of the Subcommittee, thank you for the opportunity to discuss international and domestic intellectual property enforcement as it relates to the entertainment software industry. Our industry values its working relationship with Congress, the Office of the United States Trade Representative, and the Departments of Commerce, Justice, State, and Homeland Security, as we work cooperatively to ensure that one of America's greatest assets—its intellectual property—receives adequate protection, domestically and abroad.

I appear on behalf of the members of the Entertainment Software Association (ESA). The ESA serves the business and public affairs interests of companies that publish video and computer games, including games for video game consoles, per-

sonal computers, handheld devices, and the Internet. ESA members produced more that 90 percent of the $7 billion in entertainment software sold in the United States in 2003. In addition, ESA's member companies produced billions more in exports of American-made entertainment software, helping to power the $20 billion global game software market. The entertainment software industry is one of the nation's fastest growing economic sectors, more than doubling in size since the mid-1990s and in so doing, has generated thousands of highly skilled jobs in the creative and technology fields.

Our industry makes a tremendous investment in its intellectual property. For an ESA member company to bring a top game to market, it often requires a team of 20 to 30 professionals—sometimes twice that number—working for two or three years to fuse together the work of writers, animators, musicians, sound engineers, software engineers, and programmers into an end product which, unlike any other form of entertainment, is interactive, allowing the user to direct and control the outcome of the experience. On top of these research and development costs, publishers will invest at least $5 to $10 million to market and distribute the game. The reality is that only a small percentage of these titles actually achieve profitability, and many more never recover their front-end R&D costs. In this type of market, it is easy to understand how devastating piracy can be as it siphons the revenue required to sustain the enormously high creative costs necessary to produce successful products.

In this testimony, I would like to focus on a number of domestic and international intellectual property challenges we face today, including, most formidably, from large-scale, for-profit piracy of industry products. I will share with you what ESA and its member companies are doing to combat these problems, how government has responded, and what we all must do protect our industry and the nation.

THE PIRACY PROBLEM

Entertainment software piracy is an international problem occurring both in the United States and abroad. It takes many forms, which fall into two basic types: hard goods piracy and Internet piracy. Billions of dollars worth of pirated entertainment software products—including some produced by organized criminal syndicates—are present in worldwide markets today.

Hard Goods Piracy

Entertainment software programs are produced for a variety of platforms, including video game consoles, personal computers, handheld devices, and the Internet. Hard goods piracy involves the illegal manufacturing of counterfeit optical discs for use in personal computers (PCs) and consoles for the home, such as Microsoft Xbox, the Sony PlayStation2, as well as counterfeit cartridge manufacturing for handheld devices such as the Nintendo Game Boy.

Optical media piracy is a growing problem for the industry. In many parts of the world, especially Malaysia, China, Thailand, and Russia, pirate optical disc factories produce huge numbers of illegal copies of popular games. In its Special 301 report to the United States Trade Representative this February, the International Intellectual Property Alliance (IIPA) (of which ESA is a member) reported a "staggering" growth in the number and capacity of these optical disc factories across the globe. The "burning" or copying of compact discs and DVDs is also a global problem, not only in Asia, but in Europe and Central and South America as well. In addition, console game publishers are victimized by the growing prevalence of so-called "mod chips"[1] and other devices designed to circumvent technological protection measures built into entertainment software products.

As with optical discs and mod chips, there is large-scale piracy of game cartridges used for handheld units. This piracy is committed in factories as well as smaller workshops which produce huge numbers of illegal products.

The extent of this problem cannot be overemphasized. In some nations, these large pirate enterprises operate in the open, raking in millions in illegal profits. For example, Professor Daniel Chow of Ohio State University said in recent congressional testimony that the intellectual property piracy problem in China has reached a crisis level, with virtually the entire economy of the Chinese city of Yiwu in Zhejiang Province now based on the trade of pirated products. The problem is widespread in China. As I testified before a House Subcommittee last month, enforcement undertaken by just one ESA member, Nintendo, resulted in the seizure of 4.7 million counterfeit items in China during 2003.

[1] "Mod chips" are a particular type of circumvention device that are installed into video game consoles chiefly for the purpose of rendering the console capable of playing pirated games.

Internet Piracy

While pirate factories tend to be an offshore problem, Internet piracy is a problem both domestically and internationally. Internet piracy has been a problem for several years, but is becoming an ever more serious threat due to advancing technology. While broadband Internet communication has created tremendous opportunities for consumers to enjoy high-speed communication and entertainment, it has also been a boon to pirates. High-speed Internet has given pirates the ability to readily distribute entertainment software around the globe. Some of the main Internet piracy problems include so-called "warez" sites, "cracker" groups, and peer-to-peer (P2P) distribution.

There are a number of ways in which the Internet is used to facilitate piracy of entertainment software products. It is a highly efficient distribution tool for the software and video games themselves. Each day, our investigators uncover hundreds of instances in which unauthorized copies of our members' products are made available through the use of virtually all popular Internet protocols, including through websites, FTP sites, chat sessions and, increasingly, through a growing number of peer-to-peer protocols. The Internet is also used as an advertising vehicle for services that offer pirated hard copies of disc and cartridge-based games, circumvention devices, and circumvention services.

"Warez" is a name given to sites where software and other content is distributed illegally. Often, these warez sites are operated by teams of software "crackers," individuals and groups skilled in "cracking" technological protection measures, thus allowing infringers to distribute unlimited copies of the games around the world. These sites represent a major threat to our industry. We have been extremely gratified with the Justice Department's aggressive enforcement actions against these warez groups, including last week's announcement of Operation Fastlink, an internationally coordinated investigation which resulted in the closing of warez servers and the seizure of pirated products. The Department of Justice reported that Operation Fastlink resulted in the seizure of more than 200 computers in the United States and 10 other countries. We are most appreciative for these actions that have effectively shut off illegal access to approximately $50 million of pirated works.

Internet piracy also fuels hard goods piracy by serving as an early source of the "cracked" version of game titles. Internet pirates generally obtain legitimate copies of games on the day of release or, in some cases, even prior to the commercial release of a game title. These copies are then farmed out to crackers, who, within 12 to 24 hours are often able to bypass the access and copy protection technologies included in the game software and produce a "cracked" version of the game, i.e., one stripped of these protection technologies. These cracked versions are immediately made available throughout the Internet and often are sold directly to different criminal organizations, which dominate the global trade in pirated entertainment software through a network of replication facilities in Southeast Asia and Eastern Europe. These organized crime syndicates are able to use these "cracked" versions of game software obtained illegally from the Internet to manufacture and sell pirated games on the streets, either in competition with legitimate versions or, as in most countries around the world, two to three weeks in advance of the time that legitimate goods are available.

Internet cafes offering computers for temporary use have become ubiquitous fixtures around the world. They provide a quick and easy way for people to check e-mail or use the web. Unfortunately, they also provide a quick and easy vehicle for piracy. For example, in countries throughout Asia, many Internet cafes buy only one licensed copy for use by hundreds of users in the cafe, while the cafe owner is making a profit from each and every user. In addition, many cafe operators turn a blind eye to customers who use their facilities to commit further infringements, such as burning software and other copyrighted works onto CDs.

Piracy and Organized Criminal Syndicates

Many organizations, including law enforcement agencies such as Interpol, have concluded that organized criminal enterprises are involved in intellectual property piracy. In its February Special 301 report, the IIPA reported that because of the immense profits that pirates can make by stealing intellectual property, criminal organizations have taken over pirating operations in many countries. In addition, the relatively weak penalties for intellectual property crimes in many nations make it an attractive funding source for organized criminal enterprises. Noting that intellectual property piracy gives organized criminal enterprises far greater profits and much less risk than dealing narcotics, the IIPA report cited organized crime involvement in intellectual property piracy in numerous nations, including Malaysia, Taiwan, Russia, Mexico, and Spain. Indeed, the cross-border nature of organized crime's involvement in software piracy presents an additional challenge.

ESA AND MEMBER COMPANY RESPONSES TO THE PIRACY PROBLEM

The entertainment software industry has taken the initiative to protect its intellectual property with a variety of anti-piracy measures, including international enforcement programs, online monitoring efforts, civil litigation, support and assistance to law enforcement and border control agents, technological measures, policy interaction, training of law enforcement and intellectual property education programs.

International Enforcement

Internationally, ESA and its members companies have targeted game piracy through the establishment of local enforcement programs in countries across the world. For its foreign programs, ESA typically will engage local attorneys and investigators to work with and support local law enforcement and customs officials in pursuing enforcement actions against local individuals and entities engaged in game piracy. In Asia, ESA established programs in Hong Kong and Singapore several years ago to address burgeoning game piracy in those countries. These programs have successfully curtailed the spread of street-level and retail piracy, with the Hong Kong program now focused on addressing upstream targets which are involved in the import/export of pirated goods to other markets. In South America, ESA initiated an industry program in Brazil two years ago as a joint effort with a local software industry association. This program is quite active, with monthly actions against retail venues in Sao Paulo and other major Brazilian cities as well as actions against local labs that routinely burn copies of games for distribution in the local market place. More recently, ESA has begun work on launching new enforcement programs in Canada and Mexico to address growing piracy situations there.

ESA's programs complement local enforcement programs established by some of our larger members, including Electronic Arts, Microsoft, Nintendo, Sony Computer Entertainment, and Vivendi Universal Games. These member programs similarly involve the retention of local attorneys and investigators who focus on the pirate trade in that member's game products, and work with local police and customs officials to seize pirate game product and arrest and prosecute the responsible parties. Periodically, member companies will also undertake civil actions against pirate groups. Collectively, these member companies have programs operating in more than 30 countries.

Online Monitoring and Enforcement

ESA has implemented an online monitoring program to enforce its members' intellectual property rights against Internet piracy. Under the online monitoring program, ESA has tracked an average of 400,000 new incidents of infringements per month and, over the last year, issued more than 130,000 takedown notices to Internet service providers (ISPs) under the provisions of the Digital Millennium Copyright Act (DMCA) and related authorities. These notices were addressed to ISPs both in the United States and abroad regarding instances of infringing activity engaged in by their users.

In addition to its online monitoring activities, ESA and its members have availed themselves of civil remedies available under law—including cease and desist notices, and when necessary, civil litigation—in enforcing member company rights against individuals engaging in online piracy.

U.S. Law Enforcement Support and Assistance

ESA and its member companies cooperate with United States customs and law enforcement officials on a number of levels, including preliminary investigative work, examination of seized products, and the preparation and submission of relevant documentation and affidavits in support of criminal prosecutions. ESA also assists law enforcement by providing trial testimony, identifying infringing game material found on servers, and assisting in high-level investigations of criminal organizations involved in game piracy. The U.S. Attorney's Office for the Eastern District of Virginia cited the entertainment software industry's assistance in obtaining a conviction of a member of the highly organized "DrinkorDie" piracy group targeted in "Operation Buccaneer." Last week, Attorney General Ashcroft credited ESA and other associations with providing vital assistance in "Operation Fastlink," an investigation that resulted in the coordinated takedown of more than 200 computers, including more than 30 servers that acted as storage and distribution hubs for warez groups, including Fairlight, Kalisto, Echelon, Class, and Project X.

Technological Measures

The entertainment software industry uses an array of technological protection measures (TPMs) to protect its various products, including those for personal com-

puter, console, and handheld games. These self-help protection methods act as "digital locks," preventing unauthorized access to the game content. However, criminal enterprises manufacture, create, and distribute illegal circumvention devices to disable or bypass these games' TPMs, and use the Internet to advertise and distribute these tools as well as the "cracked" (unprotected) products.

However, it has become clear that technology is not enough. We must have laws that protect not only the intellectual property, but the technological protection measures that facilitate distribution while safeguarding industry products. Furthermore, we must have meaningful enforcement of these laws in order to deter the often highly organized criminal enterprises from engaging in the piracy.

Policy Engagement

The entertainment software industry is also engaged—at both the association and member company levels—in legal and policy reform. In this capacity, we work closely with U.S. and foreign government officials to help provide an effective legal and commercial framework for the healthy growth of the industry and to promote the increased availability of entertainment software products.

Training of Law Enforcement

The entertainment software industry has assisted government in the area of intellectual property enforcement by having ESA conduct training sessions across the nation and internationally to help educate law enforcement on intellectual property issues. Over the past year, in over 70 training sessions involving approximately 1,400 officials and agents in the United States and three foreign countries, ESA provided training on methods of detection and identification of pirated game products.

Intellectual Property Education

Recently, the ESA and its member companies have undertaken a number of different initiatives to educate different segments of the public, in particular, younger age groups, regarding the importance of intellectual property, the harm that game piracy and other forms of intellectual property infringement can cause, as well as the risks inherent in engaging in pirate activities. Most of these efforts have focused on providing children a deeper appreciation of the value and importance of intellectual property such as copyright and trademarks.

GOVERNMENT'S RESPONSE TO THE PIRACY PROBLEM

USTR and other key offices in the Departments of Commerce and State tasked with enforcing U.S. trade law and—as part of the trade agenda—intellectual property law, have consistently demonstrated their strong and continuing commitment to creators generally and the entertainment software industry specifically, pressing for the highest attainable standards of protection for intellectual property rights through the successful negotiation of multilateral and bilateral agreements with other nations. These agencies have also stood firm in monitoring, rewarding, and in notable instances, penalizing countries for failing to achieve compliance with U.S. trade law and international intellectual property norms.

One especially valuable tool has been the "Special 301" review process, which the U.S. government utilizes effectively to target countries that must improve their efforts to protect intellectual property. In addition to Special 301, by requiring countries in the Generalized System of Preferences (GSP) program to ensure adequate and effective protection of intellectual property rights as a condition of obtaining the program's tariff free status for their exports to the United States, the United States has also raised awareness of intellectual property rights as a national policy priority.

Several U.S. agencies also monitor and help to dismantle market access barriers that hinder the flow of U.S. products to overseas markets. The market access problems facing the entertainment software industry include compliance with legitimate product identification formalities (such as so-called "stickering" regimes), protracted content review periods, and other trade or import restrictions against U.S. computer and video game products. These regimes not only increase the cost incurred by U.S. publishers in getting legitimate product to market but also add considerable delay before products are actually made available for sale. This delay, in turn, works to the advantage of pirates who bypass processes required of legitimate publishers.

The Department of Commerce, through its International Trade Administration (ITA), has made it a priority to gather information from our industry on trade barriers and other impediments to commerce, chief among them being endemic piracy, and to bring these barriers to the attention of U.S. and foreign officials. We are similarly appreciative of the resources dedicated year-round by the Department in support of the government's international negotiations (such as the recently con-

cluded Joint Commission on Commerce and Trade with China), and steps taken by the Department's Trade Compliance Center to ensure that American exporters overcome foreign trade barriers.

The Commerce Department's Patent and Trademark Office also contributes immensely to the work of USTR, by providing, for instance, the necessary technical expertise and advice during free trade negotiations and discussions of intellectual property issues at the multilateral level. In addition, the PTO provides training and technical assistance programs, not only to promote intellectual property protection, but also to foreign governments to improve their intellectual property laws and to train their law enforcement agencies to better address intellectual property infringement.

With respect to domestic enforcement, intellectual property rightsholders have been increasingly better served by the efforts of the investigative arms of the Departments of Justice and Homeland Security and the prosecutorial capabilities of the Department of Justice. Investigative agencies contributing to this mission include the FBI and Customs' Bureau of Investigations and Criminal Enforcement (ICE), as well as its Bureau of Customs and Border Protection (CBP). The prosecutorial offices contributing to the success of this mission include the Computer Hacking and Intellectual Property (CHIPs) units within several key U.S. Attorneys' offices and the Computer Crime and Intellectual Property Section (CCIPS) of the Department of Justice.

The Department of Justice has recently taken two important actions in the fight against piracy. First, it has established the Intellectual Property Task Force to coordinate the department's intellectual property enforcement activities. Second, as mentioned earlier, the Attorney General last week announced Operation Fastlink, a coordinated effort with law enforcement agencies around the world to stop Internet piracy. Operation Fastlink is an important example of the positive results that can be achieved when our government works together with other governments to coordinate response to piracy problems. With the global nature of the Internet, this type of international cooperation is vital.

In sum, we are extremely grateful that so many U.S. government agencies have taken action in the fight against global piracy. We believe, overall, that existing roles and responsibilities are allocated appropriately to assure that agencies with the greatest subject-matter expertise are on the job. That said, we believe there are a few actions that this Subcommittee can take to strengthen the U.S. Government's ability to strike additional blows that weaken the global pirate trade.

RECOMMENDATIONS

The entertainment software industry will continue to use technological and legal measures to protect its intellectual property, but private efforts are not enough. It is imperative that the U.S. government remain firm in its commitment to fight the rampant international and domestic piracy of intellectual property. The various government agencies responsible for the protection of intellectual property are doing a remarkable job in many ways, but can be hindered in their efforts to focus on enforcing the intellectual property provisions of international treaties and domestic laws due to insufficient resources and personnel. Following are some concrete steps we believe will arm our government with additional tools and authorities to win the war on piracy.

Office of the U.S. Trade Representative

In recent years, the Office of the U.S. Trade Representative (USTR) has done a tremendous job of successfully negotiating free trade agreements that raise intellectual property protection standards to the highest levels. We thank the Subcommittee for the $5 million that Congress added to the fiscal year 2004 budget for USTR, and acknowledge USTR's efforts to reorganize its China office in order to make best use of these resources. However, with the increasing burden of broadening the free trade sphere, USTR has not had the resources or personnel to devote to its other mission: monitoring compliance with and enforcing U.S. trade law and bilateral trade agreements.

USTR, to its benefit, relies on personnel from other federal agencies to perform its monitoring duties. Moreover, intellectual property rights issues are currently included in an office within USTR that also covers services and investment issues. Given the enormous importance of intellectual property to our economy, ESA recommends that the Subcommittee create a stand-alone intellectual property office with dedicated and adequate staff to conduct multilateral and bilateral negotiations and also to ensure that our trading partners comply with their intellectual property-related obligations to the United States. Additionally, the Subcommittee could consider creating a special ambassador for intellectual property and provide that official

with adequate staff and resources dedicated to the enforcement of existing agreements.

Whatever approach is taken, the addition of new staff dedicated to enforcement of agreements will materially strengthen USTR's ability to monitor WTO/TRIPS compliance, and to fulfill the potential of the 301 program by more aggressive use of out-of-cycle reviews. Similarly, dedicated intellectual property staff could help ensure that the GSP program is used as effectively as possible to induce foreign nations to better protect American intellectual property rights. (A reinvigoration of the GSP review process would be much desired as the prospect of losing tariff-free trade benefits that reach into the billions for certain nations would certainly prove to be a great incentive to improving intellectual property protections.)

Department of State

The State Department is playing a critical role in providing funds to foreign countries to help improve their law enforcement against copyright piracy. During this fiscal year, Congress provided a one-year allocation of funds to the State Department and directed it to spend the $2.5 million on building the capacity of foreign law enforcement agencies to better enable certain countries to comply with their obligations under the international intellectual property treaties.

ESA believes it is critical to sustain and grow this funding in the new fiscal year to help ensure that foreign enforcement programs will become fully developed and effective. The United States can only do so much, and this program recognizes that an investment in enhancing the ability of other nations to assume a greater role in enforcement may reduce demands on our own government in future years.

Furthermore, as helpful as the State Department has been, the fact remains that it is responsible for a broad range of foreign policy issues. Understandably, intellectual property issues often do not take priority. We believe the Subcommittee should consider elevating the State Department's Intellectual Property Division to "Office-level" status, thereby granting this unit greater authority to advocate for enforcement of intellectual property protections with other offices within the State Department.

Department of Justice

As noted elsewhere, the Justice Department has been increasingly aggressive and effective in the fight against piracy. Therefore, we recommend strongly that the Subcommittee allocate sufficient funds for Justice to continue its recent efforts and undertake new initiatives, such as the Intellectual Property Task Force and Operation Fastlink. We believe that the investigative capabilities of the FBI and the prosecutorial resources of the Department of Justice, including the Computer Crime and Intellectual Property Section (CCIPS) and the Computer Hacking and Intellectual Property (CHIPs) sections of the U.S. Attorneys' Offices should be fully funded to accomplish their vital missions.

We thank the Subcommittee for the support it has already given to the Department by setting aside a portion of the DOJ's appropriation for cybercrime and intellectual property crime enforcement. However, we recommend that Congress provide additional resources to the Justice Department to expand these efforts. Specifically, we recommend additional funding for the investigation of intellectual property crimes by the FBI. We believe that additional agents specifically trained in online investigations are essential to fighting domestic intellectual property piracy. This will enhance and support the efforts of U.S. Attorneys engaged in prosecuting intellectual property offenses.

CONCLUSION

Mr. Chairman and members of the Subcommittee, it is clear from my testimony that our industry has in the U.S. Government a strong and effective partner in the battle against global entertainment software piracy. Your Subcommittee's commitment to fighting piracy is well-documented. We are grateful for your commitment, especially at a time when our nation faces so many other threats to our security. But it is equally clear that the global piracy problem remains deeply entrenched, and that it directly endangers America's economic security as U.S. companies see viable potential markets closed-off due to the proliferation of pirated and counterfeit products. We need your continued help, and we appreciate the opportunity to share some ideas on additional steps that can be taken to protect America's greatest export: our creative and intellectual property. Working together, I believe we can fight piracy to protect what is one of America's most dynamic and fastest growing creative industries.

Senator GREGG. Mr. Holleyman.

UNPUBLISHED CASES

Hotmail Corp. v. Van$ Money Pie, Inc., No. C-98 JW PVT ENE, C98-20064 JW, 1998 WL 388389, *1 (N.D. Cal. Apr. 16, 1998).

RealNetworks, Inc. v. Streambox, Inc., No. 2:99CV02070, 2000 WL 127311, *7 (W.D. Wash. Jan. 18, 2000).

Not Reported in F.Supp.
1998 WL 388389 (N.D.Cal.), 47 U.S.P.Q.2d 1020
(Cite as: 1998 WL 388389 (N.D.Cal.))

Motions, Pleadings and Filings

United States District Court, N.D. California.
HOTMAIL CORPORATION, Plaintiff,
v.
VAN$ MONEY PIE INC.; ALS Enterprises, Inc.; LCGM, Inc.; Christopher Moss d/b/a the Genesis Network, Inc.; Claremont Holdings Ltd.; Consumer Connections; Palmer & Associates; and Financial Research Group; and Darlene Snow d/b/a Visionary Web Creations and/or d/b/a Maximum Impact Marketing, Defendants.
No. C-98 JW PVT ENE, C 98-20064 JW.

April 16, 1998.

Nicole A. Wong, Hosie, Wes, Sacks & Brelsford, LLP, Menlo Park, CA, for Plaintiff.

William R. Mitchell, Tustin, CA, LCGM, Madison Heights, MI, Palmer & Associates, San Diego, CA, Financial Research Group, El Cajon, CA, James Polyzois, Detroit, MI, Darlene Snow, Mission Viejo, CA, for Defendants.

ORDER GRANTING PRELIMINARY INJUNCTION

WARE, J.

*1 THIS MATTER was submitted on the papers by the Court on the Motion of plaintiff Hotmail Corporation ("Hotmail") for Preliminary Injunction to enjoin defendants ALS Enterprises, Inc. ("ALS"); LCGM, Inc. ("LCGM"); Christopher Moss d/b/a Genesis Network ("Moss"); Palmer & Associates ("Palmer"); Financial Research Group ("Financial") and Darlene Snow d/b/a Visionary Web Creations and/or d/b/a Maximum Impact Marketing ("Snow") from infringing Hotmail's HOTMAIL trade name and service mark, diluting this mark, engaging in acts of unfair competition, violating the Computer Fraud and Abuse Act, breaching a contract, and violating California law. 15 U.S.C. §§ 1125(a) & (c); 18 U.S.C. § 1030; Cal. Bus. & Prof.Code §§ 14330, 17200; Cal. Civ.Code §§ 1709-10; and 3420-22. Having reviewed the entire court record pertaining to this Motion, and having considered the evidence and argument of counsel in support of Hotmail's Motion, the Court enters the following Findings of Fact and Conclusions of Law:

FINDINGS OF FACT

1. Plaintiff Hotmail is a Silicon Valley company that provides free electronic mail ("e-mail") on the World Wide Web. Hotmail's online services allow its over ten million registered subscribers to exchange e-mail messages over the Internet with any other e-mail user who has an Internet e-mail address throughout the world. Every e-mail sent by a Hotmail subscriber automatically displays a header depicting Hotmail's domain name "hotmail.com" and a footer depicting Hotmail's "signature" at the bottom of the e-mail which reads "Get Your Private, Free Email at http://www.hotmail.com." Every e-mail received by a Hotmail subscriber also automatically displays a header depicting Hotmail's domain name. Thus, plaintiff's HOTMAIL mark--contained within its domain name and signature--appears on millions of e-mails transmitted worldwide daily.

2. In or about 1996, Hotmail developed the mark HOTMAIL and obtained the Internet domain name "hotmail.com" which incorporates its mark. Hotmail is the sole and exclusive holder of that domain name.

3. In or about 1996, Hotmail began using its HOTMAIL mark in various forms and styles, continuously in commerce in association with its online services as a means of identifying and distinguishing Hotmail's online services from those of others. Thus Hotmail's mark has appeared in the headers and footers of e-mail sent from and received by Hotmail subscribers, on Hotmail's homepage and on nearly every page of its Website, on letterhead and envelopes, on business cards, in promotional materials and in press releases.

4. Hotmail has spent approximately $10 million marketing, promoting, and distributing its services in association with its HOTMAIL mark. Hotmail does not authorize any other e-mail service provider to use its HOTMAIL mark, or Hotmail's domain name or signature.

5. "Spam" is unsolicited commercial bulk e-mail akin to "junk mail" sent through the postal mail. The transmission of spam is a practice widely condemned in the Internet Community and is of significant concern to Hotmail.

***2** 6. Hotmail has invested substantial time and money in efforts to disassociate itself from spam and to protect e-mail users worldwide from receiving spam associated in any way with Hotmail.

7. To become a Hotmail subscriber, one must agree to abide by a Service Agreement ("Terms of Service") which specifically prohibits subscribers from using Hotmail's services to send unsolicited commercial bulk e-mail or "spam," or to send obscene or pornographic messages. Hotmail can terminate the account of any Hotmail subscriber who violates the Terms of Service.

8. In or about the Fall of 1997, Hotmail learned that defendants were sending "spam" e-mails to thousands of Internet e-mail users, which were intentionally falsified in that they contained return addresses bearing Hotmail account return addresses including Hotmail's domain name and thus its mark, when in fact such messages did not originate from Hotmail or a Hotmail account. Such spam messages advertised pornography, bulk e-mailing software, and "get-rich-quick" schemes, among other things.

9. In addition, Hotmail learned that defendants had created a number of Hotmail accounts for the specific purpose of facilitating their spamming operations. Such accounts were used to collect responses to defendants' e-mails and "bounced back" messages in what amounted to a "drop box" whose contents were never opened, read or responded to. It was these Hotmail accounts that were used as return addresses by defendants in lieu of defendants' actual return addresses when defendants sent their spam e-mail.

10. As a result of the falsified return addresses described above, Hotmail was inundated with hundreds of thousands of misdirected responses to defendants' spam, including complaints from Hotmail subscribers regarding the spam and "bounced back" e-mails which had been sent by defendants to nonexistent or incorrect e-mail addresses. This overwhelming number of e-mails took up a substantial amount of Hotmail's finite computer space, threatened to delay and otherwise adversely affect Hotmail's subscribers in sending and receiving e-mail, resulted in significant costs to Hotmail in terms of increased personnel necessary to sort and respond to the misdirected complaints, and damaged Hotmail's reputation and goodwill.

11. In particular, Hotmail discovered a spam e-mail message advertising pornographic material that was sent by ALS. While this spam originated from ALS and was transmitted through an E-mail Provider other than Hotmail, ALS falsely designated a real Hotmail e-mail address as the point of origin. The e-mail address chosen for this purpose was "geri748@hotmail.com."

12. Hotmail also discovered a number of spam e-mail messages advertising pornographic material that were sent by LCGM. While these spam e-mails originated from LCGM and were transmitted through an E-mail Provider other than Hotmail, LCGM falsely designated a number of real Hotmail e-mail address as the points of origin. The e-mail addresses chosen for this purpose were " becky167 @hotmail.com;" "deena54@hotmail.com;" "marisa104@hotmail.com;" "shelly345 @hotmail.com;" "sonnie67@hotmail.com;" "ashley_113@hotmail.com;" "grace44 @hotmail.com;" "jess_59@hotmail.com;" "kristina17@hotmail.com;" "nellie24 @hotmail.com;" and, "tyrona56@hotmail.com."

***3** 13. Hotmail also discovered a spam e-mail message advertising pornographic material that was sent by Moss. While this spam originated from Moss and was transmitted through an E-mail Provider other than Hotmail, Moss falsely designated a real Hotmail e-mail address as the point of origin. The e-mail address chosen for this purpose was "rebecca_h19@hotmail.com."

14. Hotmail also discovered a spam e-mail message advertising a cable descrambler kit that was sent by

Palmer. While this spam originated from Palmer and was transmitted through an E-mail Provider other than Hotmail, Palmer falsely designated two real Hotmail e-mail addresses as the points of origin. The e-mail addresses chosen for this purpose were "kelCA@hotmail.com" and "angiCA@hotmail.com."

15. Hotmail also discovered a spam e-mail message advertising a service that matches people seeking cash grants that was sent by Financial. While this spam originated from Financial and was transmitted through an E-mail Provider other than Hotmail, Financial falsely designated a real Hotmail e-mail address as the point of origin. The e-mail address chosen for this purpose was "order_desk66 @hotmail.com."

16. Hotmail also discovered a number of spam e-mail messages advertising pornography that were sent by Snow. While this spam originated from Snow and was transmitted through an E-mail Provider other than Hotmail, Snow falsely designated several real Hotmail e-mail address as the point of origin. The e-mail addresses chosen for this purpose were "bettyharris123@hotmail.com;" "annharris123@hotmail.com;" "cindyharris123@hotmail.com;" "wilmasimpson @hotmail.com;" "rw3570@hotmail.com;" "rw3560@hotmail.com;" and, "jw2244 @hotmail.com."

CONCLUSIONS OF LAW

Jurisdiction and Venue

17. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331. This Court has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367. This Court has personal jurisdiction over the defendants ALS, LCGM, Moss, Palmer, Financial, and Snow, who have engaged in business activities in or directed in California.

18. Venue is proper in this district pursuant to 28 U.S.C. § 1391 because a substantial portion of the events giving rise to the claims pled herein occurred in this judicial district and defendants do business in this judicial district.

Standard For Granting Preliminary Injunction

19. The standard for preliminary injunction relief in trademark infringement cases and related actions is well-settled. Hotmail must show either: (a) a likelihood of success on the merits and the possibility of irreparable injury; or (b) the existence of serious questions going to the merits and the balance of hardships tips in Hotmail's favor. *Apple Computer. Inc. v. Formula Int'l, Inc.,* 725 F.2d 521, 523 (9th Cir.1984).

Plaintiff's Legal Claims

20. Hotmail seeks preliminary injunctive relief in this Motion for false designations of origin, federal and state dilution, violation of the Computer Fraud and Abuse Act, state and common law unfair competition, breach of contract, fraud and misrepresentation, and trespass to chattel, pursuant to 15 U.S.C. §§ 1116, 1125(a) & (c); 18 U.S.C. § 1030; Cal. Bus. & Prof.Code §§ 14330, 17203; and Cal Civ.Code §§ 1709-10.

Plaintiff's Likelihood Of Success On Its Claims

False Designation Of Origin And Unfair Competition

*4 21. The core element of a cause of action for false designation of origin under 15 U.S.C. § 1125(a) as well as other unfair competition is "likelihood of confusion, i.e., whether the similarity of the marks is likely to confuse customers about the source of the products." *E. & J. Gallo Winery v. Gallo Cattle Co.,* 967 F.2d 1280, 1290 (9th Cir.1992); *Academy of Motion Picture Arts & Sciences v. Creative House Promotions, Inc.,* 944 F.2d 1446, 1454 (9th Cir.1991).

22. Courts will consider the following factors, among others, as relevant to a determination of the likelihood of confusion for claims under 15 U.S.C. § 1125(a) and related other unfair competition claims: (a) strength or weakness of plaintiff's mark; (b) the degree of similarity with defendant's mark; (c) class of goods; (d) marketing channels used; (e) evidence of actual confusion; and (f) intent of the defendant. *Americana Trading Inc. v. Russ Berrie & Co.,* 966 F.2d 1284, 1287 (9th Cir.1992). However, there is not a mandated test for likelihood of confusion applied by the courts in this Circuit, and the appropriate time for full consideration of all

relevant factors is when the merits of the case are tried. *Apple Computer,* 725 F.2d at 526.

23. The majority of these factors supports a finding that Hotmail is likely to succeed on the merits of its claims that defendants' use of the HOTMAIL mark is likely to cause consumer confusion or mistake as to the origin, sponsorship, or approval of defendants' spam e-mails and spam e-mail business, and that there are at least serious questions going to the merits of plaintiff's claims.

24. Plaintiff's mark is strong. The "strength" of a mark depends in part on whether it is arbitrary or fanciful, suggestive, merely descriptive, or generic. *Chronicle Pub. Co. v. Chronicle Publications, Inc.,* 733 F.Supp. 1371, 1375 (N.D.Cal.1989). In addition, a company's "extensive advertising, length of time in business, public recognition, and uniqueness" all strengthen its trademarks. *Century 21 Real Estate Corp. v. Sandlin,* 846 F.2d 1175, 1179 (9th Cir.1988). While the second part of the mark--"mail"--may be suggestive by conveying some aspect of the e-mail process, the mark as a whole is arbitrary and fanciful because it neither describes nor suggests that Hotmail is a provider of electronic mail as a Web-based service on the Internet. Moreover, plaintiff has spent substantial sums of money to advertise and market its services in association with the mark and has extensively featured the mark in its promotions.

25. Defendants' "mark" is not only confusingly similar to plaintiff's mark, it is identical to it. A comparison of defendants' and plaintiff's uses shows such striking similarity that a jury could not help but find that defendants' use is confusing. Indeed, there has been actual confusion among consumers regarding the marks. This factor alone may be determinative. *See E. Remy Martin & Co., S.A. v. Shaw-Ross International Imports, Inc.,* 756 F.2d 1525, 1529, 1530 (11th Cir.1985) (it is "well-settled" that "evidence of actual confusion is not necessary to a finding of likelihood of confusion, although it is the best such evidence;" indeed, "a sufficiently strong showing of likelihood of confusion may be itself constitute a showing of substantial likelihood of prevailing on the merits and/or a substantial threat of irreparable harm"); *World Carpets, Inc. v. Dick Littrell's New World Carpets,* 438 F.2d 482, 489 (5th Cir.1971) ("[t]here can be no more positive or substantial proof of likelihood of confusion than proof of actual confusion").

***5** 26. The class of goods and services distributed by defendants--e-mails-- which bear a mark identical to plaintiff's, are the same as the class of goods and services distributed by plaintiff--e-mails.

27. The marketing channels through which the parties sell their goods and services are the same--via e-mail over the Internet. Their consumer audience is likewise the same. Moreover, because e-mail is specifically designed for the rapid exchange of information, consumers are unlikely to exercise a great deal of care in distinguishing between marks on e-mails they receive.

28. Defendants' intent further supports possible confusion. *Levi Strauss & Co. v. Blue Bell,* 632 F.2d 817, 822 (9th Cir.1981); *Pacific Telesis Group v. International Telesis Communications,* 994 F.2d 1364, 1369 (9th Cir.1993). Here, the evidence supports an inference that defendants intended to emulate plaintiff's trademark, given their knowing falsification of e-mail return addresses, their fraudulent creation of Hotmail mailboxes, as well as their attempts to circumvent plaintiff's efforts to prevent its subscribers from receiving spam.

Dilution

29. The core elements of a cause of action under the federal dilution statute are plaintiff's ownership of a famous mark and dilution of the distinctive quality of plaintiff's mark, regardless of whether consumers are confused about the parties' goods. 15 U.S.C. § 1125(c)(1). Under the California dilution statute as well, actual injury or likelihood of confusion need not be shown; plaintiff need only show its business reputation is likely to be injured or the distinctive value of its mark is likely to be diluted. Cal. Bus. & Prof.Code § 14330; *Academy,* 944 F.2d at 1457.

30. In determining whether a mark is distinctive and famous so as to support a claim for federal dilution, the Court has considered the following factors; (a) the degree of inherent or acquired distinctiveness of the mark; (b) the duration and extent of use of the mark in connection with the

goods or services with which the mark is used; (c) the duration and extent of advertising and publicity of the mark; (d) the geographical extent of the trading area in which the mark is used; (e) the channels of trade for the goods or services with which the mark is used; (f) the degree of recognition of the mark in the trading areas and channels of trade used by the mark's owner and the person against whom the injunction is sought; and (g) the nature and extent of use of the same or similar marks by third parties. 15 U.S.C. § 1125(c)(1).

31. Under California's anti-dilution statute, the plaintiff need only show the "[l]ikelhihood of injury to business reputation or of dilution of the distinctive quality of a mark." Cal. Bus. & Prof.Code § 14330.

32. Here, the evidence supports a finding that plaintiff will likely prevail on its federal and state dilution claims and that there are at least serious questions going to the merits of these claims. First, there is sufficient evidence to lead to a finding that plaintiff's trademark is "famous" within the meaning of 15 U.S.C. § 1125(c)(1) and also that it is entitled to state dilution protection. Plaintiff's mark is distinctive, has been advertised and used extensively both nationally and internationally in connection with plaintiff's services, and has established considerable consumer recognition. Moreover, the use of identical marks by defendants who are sending e-mails to thousands of e-mail users across the country and the world through identical trade channels threatens to dilute the distinctiveness of plaintiff's trademark and threatens to harm plaintiff's business reputation.

Violation Of Computer Fraud And Abuse Act

***6** 33. The Computer Fraud and Abuse Act prohibits any person from knowingly causing the transmission of information which intentionally causes damage, without authorization, to a protected computer. 18 U.S.C. § 1030.

34. The evidence supports a finding that plaintiff will likely prevail on its Computer Fraud and Abuse Act claim and that there are at least serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that defendants knowingly falsified return e-mail addresses so that they included, in place of the actual sender's return address, a number of Hotmail addresses; that such addresses were tied to Hotmail accounts set up by defendants with the intention of collecting never-to-be-read consumer complaints and "bounced back" e-mails; that defendants knowingly caused this false information to be transmitted to thousands of e-mail recipients; that defendants took this action knowing such recipients would use the "reply to" feature to transmit numerous responses to the fraudulently created Hotmail accounts, knowing thousands of messages would be "bounced back" to Hotmail instead of to defendants, and knowing that numerous recipients of defendants' spam would e-mail complaints to Hotmail; that defendants took such actions knowing the risks caused thereby to Hotmail's computer system and online services, which include risks that Hotmail would be forced to withhold or delay the use of computer services to its legitimate subscribers; that defendants' actions caused damage to Hotmail; and that such actions were done by defendants without Hotmail's authorization.

Breach Of Contract

35. The evidence supports a finding that plaintiff will likely prevail on its breach of contract claim and that there are at least serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that defendants obtained a number of Hotmail mailboxes and access to Hotmail's services; that in so doing defendants agreed to abide by Hotmail's Terms of Service which prohibit using a Hotmail account for purposes of sending spam and/or pornography; that defendants breached their contract with Hotmail by using Hotmail's services to facilitate sending spam and/or pornography; that Hotmail complied with the conditions of the contract except those from which its performance was excused; and that if defendants are not enjoined they will continue to create such accounts in violation of the Terms of Service.

Fraud And Misrepresentation

36. The cause of action for fraud includes willfully deceiving another with intent to induce him to alter his position to his injury or risk by asserting, as a fact, that which is not true, by one who has no

reasonable ground for believing it to be true; or by suppressing a fact, by one who is bound to disclose it, or who gives information of other facts which are likely to mislead for want of communication of that fact; or by making a promise without any intention of performing it. Civ.Code §§ 1709-10.

*7 37. The evidence supports a finding that plaintiff will likely prevail on its fraud and misrepresentation claim and that there are at least serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that defendants fraudulently obtained a number of Hotmail accounts, promising to abide by the Terms of Service without any intention of doing so and suppressing the fact that such accounts were created for the purpose of facilitating a spamming operation, and that defendants' fraud and misrepresentation caused Hotmail to allow defendants to create and use Hotmail's accounts to Hotmail's injury. In addition, the evidence supports a finding that defendants' falsification of e-mails to make it appear that such messages and the responses thereto were authorized to be transmitted via Hotmail's computers and stored on Hotmail's computer system--when defendants knew that sending such spam was unauthorized by Hotmail--constitutes fraud and misrepresentation, and that Hotmail relied on such misrepresentations to allow the e-mails to be transmitted over Hotmail's services and to take up storage space on Hotmail's computers, to Hotmail's injury.

Trespass To Chattel

38. "Trespass to chattel ... lies where an intentional interference with the possession of personal property has proximately caused injury." *Thrifty-Tel, Inc. v. Bezenek,* 46 Cal.App.4th 1559, 1566, 54 Cal.Rptr.2d 468 (1996).

39. The evidence supports a finding that plaintiff will likely prevail on its trespass to chattel claim and that there are serious questions going to the merits of this claim in that plaintiff has presented evidence of the following: that the computers, computer networks and computer services that comprise Hotmail's e-mail system are the personal property of Hotmail; that defendants obtained consent to create Hotmail accounts within the limitations set forth in the Terms of Service: no spamming and no pornography; that defendants intentionally trespassed on Hotmail's property by knowingly and without authorization creating Hotmail accounts that were used for purposes exceeding the limits of the Terms of Service; that defendants trespassed on Hotmail's computer space by causing tens of thousands of misdirected e-mail messages to be transmitted to Hotmail without Hotmail's authorization, thereby filling up Hotmail's computer storage space and threatening to damage Hotmail's ability to service its legitimate customers; and that defendants' acts of trespass have damaged Hotmail in terms of added costs for personnel to sort through and respond to the misdirected e-mails, and in terms of harm to Hotmail's business reputation and goodwill.

Irreparable Harm To Plaintiff

40. In cases where trademark infringement is shown, irreparable harm is presumed. *Apple Computer,* 725 F.2d at 525; *Charles Schwab & Co. v. Hibernia Bank,* 665 F.Supp. 800, 812 (N.D.Cal.1987).

41. Plaintiff has suffered and, if defendants are not enjoined, will continue to suffer irreparable harm from the distribution, promotion and use of e-mails bearing plaintiff's mark--particularly spam e-mails, some of which advertise pornography--because of the loss of goodwill and reputation arising from customer confusion about the source of defendants' spam e-mails and/or plaintiff's affiliation or sponsorship of them. This kind of harm is not easily quantified and not adequately compensated with money damages. Plaintiff thus has no adequate remedy at law.

Balance Of Hardships

***8** 42. The Court finds that the irreparable harm to plaintiff should injunctive relief not be granted outweighs any injury to defendants resulting from a temporary injunction. Plaintiff has introduced evidence that it has been involved in extensive distribution and promotion of its online services in association with its mark for years and has expended vast amounts of time and money developing and promoting its mark. Plaintiff also is a service mark owner entitled to avoid having its reputation and goodwill placed in jeopardy. In

contrast, if enjoined, defendants would not suffer harm in that they would be free to continue advertising by means of e-mail so long as they did not use Hotmail's mark or services to facilitate such advertising. Thus, the balance of hardships strongly tips in favor of plaintiff.

Conclusion

43. The Court therefore concludes that plaintiff is entitled to a preliminary injunction on the grounds that plaintiff is likely to succeed on the merits, that there is a possibility of irreparable injury, that there are serious questions going to the merits, and that the balance of hardships tips sharply in plaintiff's favor. It is therefore,

ORDERED AND ADJUDGED:

That defendants ALS, LCGM, Moss, Palmer, Financial, and Snow, their officers, agents, co-conspirators, servants, affiliates, employees, parent and subsidiary corporations, attorneys and representatives, and all those in privity or acting in concert with defendants are temporarily and preliminarily enjoined and restrained during the pendency of this action from directly or indirectly:

1. Using any images, designs, logos or marks which copy, imitate or simulate Hotmail's HOTMAIL mark, and/or Hotmail's "hotmail.com" domain name for any purpose, including but not limited to any advertisement, promotion, sale or use of any products or services;

2. Performing any action or using any images, designs, logos or marks that are likely to cause confusion, to cause mistake, to deceive, or to otherwise mislead the trade or public into believing that Hotmail and defendants, or any of them, are in any way connected, or that Hotmail sponsors defendants; or that defendants, or any of them, are in any manner affiliated or associated with or under the supervision or control of Hotmail, or that defendants and Hotmail or Hotmail's services are associated in any way.

3. Using any images, designs, logos or marks or engaging in any other conduct that creates a likelihood of injury to the business reputation of Hotmail or a likelihood of misappropriation and/or dilution of Hotmail's distinctive mark and the goodwill associated therewith;

4. Using any trade practices whatsoever, including those complained of herein, which tend to unfairly compete with or injure Hotmail, its business and/or the goodwill appertaining thereto;

5. Sending or transmitting, or directing, aiding, or conspiring with others to send or transmit, electronic mail or messages bearing any false, fraudulent, anonymous, inactive, deceptive, or invalid return information, or containing the domain "hotmail.com," or otherwise using any other artifice, scheme or method of transmission that would prevent the automatic return of undeliverable electronic mail to its original and true point of origin or that would cause the e-mail return address to be that of anyone other than the actual sender;

***9** 6. Using, or directing, aiding, or conspiring with others to use, Hotmail's computers or computer networks in any manner in connection with the transmission or transfer of any form of electronic information across the Internet, including, but not limited to, creating any Hotmail e-mail account, or becoming a Hotmail subscriber, for purposes other than those permitted by Hotmail's Terms of Services, including but not limited to, for purposes of participating in any way in sending spam e-mail or operating a spamming business, or sending or advertising or promoting pornography and/or sending e-mails for any commercial purpose.

7. Opening, creating, obtaining and/or using, or directing, aiding, or conspiring with others to open, create, obtain and/or use, any Hotmail account or mailbox;

8. Acquiring or compiling Hotmail member addresses for use in the transmission of unsolicited promotional messages to those Hotmail members; and,

9. Sending or transmitting, or directing, aiding, or conspiring with others to send or transmit, any unsolicited electronic mail message, or any electronic communication of any kind, to or through Hotmail or its members without prior written authorization.

IT IS FURTHER ORDERED AND ADJUDGED:

That plaintiff shall provide a bond in the amount of only $100.

1998 WL 388389 (N.D.Cal.), 47 U.S.P.Q.2d 1020

Motions, Pleadings and Filings (Back to top)

. 5:98CV20064 (Docket)
(Jan. 26, 1998)

END OF DOCUMENT

Not Reported in F.Supp.2d
2000 WL 127311 (W.D.Wash.)
(Cite as: 2000 WL 127311 (W.D.Wash.))

▷

Motions, Pleadings and Filings

Only the Westlaw citation is currently available.

United States District Court, W.D. Washington.
REALNETWORKS, INC., Plaintiff,
v.
STREAMBOX, INC., Defendant.
No. 2:99CV02070.

Jan. 18, 2000.

ORDER ON PLAINTIFF'S MOTION FOR PRELIMINARY INJUNCTION

PECHMAN, J.

INTRODUCTION

***1** Plaintiff RealNetworks, Inc. ("RealNetworks") filed this action on December 21, 1999. RealNetworks claims that Defendant Streambox has violated provisions of the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201 *et seq.*, by distributing and marketing products known as the Streambox VCR and the Ripper. RealNetworks also contends that another Streambox product, known as the Ferret, is unlawfully designed to permit consumers to make unauthorized modifications to a software program on which RealNetworks holds the copyright.

On December 21, 1999, RealNetworks applied for a temporary restraining order to bar Streambox from manufacturing, distributing, selling, or marketing the VCR, the Ripper, and the Ferret. On December 23, 1999, Chief Judge Coughenour of this Court entered a Temporary Restraining Order, finding RealNetworks was likely to succeed on the merits of its claims and that it was suffering irreparable harm from Streambox's conduct. The Court also ordered Streambox to show cause as to why the restraints contained in the Temporary Restraining Order should not be continued as a preliminary injunction.

After expedited briefing, a show cause hearing was held on January 7, 2000 before the Court. Both parties were permitted to submit overlength briefs in support of their arguments. The Court further requested that both parties submit and highlight portions of the legislative history of the DMCA that they believe to be relevant to interpreting the statute with respect to Plaintiff's claims under the statute.

The Court, having considered the papers and pleadings filed herein and having heard oral argument from the parties, concludes that a preliminary injunction should be entered to enjoin the manufacture, distribution, and sale of the Streambox VCR and the Ferret during the pendency of this action. The Court does not conclude that a preliminary injunction should be entered with respect to the Ripper. Pursuant to Fed.R.Civ.P. 52(a), the Court's findings of fact and conclusions of law are stated below.

FINDINGS OF FACT

RealNetworks

1. RealNetworks is a public company based in Seattle, Washington that develops and markets software products designed to enable owners of audio, video, and other multimedia content to send their content to users of personal computers over the Internet.

2. RealNetworks offers products that enable consumers to access audio and video content over the Internet through a process known as "streaming." When an audio or video clip is "streamed" to a consumer, no trace of the clip is left on the consumer's computer, unless the content owner has permitted the consumer to download the file.

3. Streaming is to be contrasted with "downloading," a process by which a complete copy of an audio or video clip is delivered to and stored on a consumer's computer. Once a consumer has downloaded a file, he or she can access the file at

will, and can generally redistribute copies of that file to others.

*2 4. In the digital era, the difference between streaming and downloading is of critical importance. A downloaded copy of a digital audio or video file is essentially indistinguishable from the original, and such copies can often be created at the touch of a button. A user who obtains a digital copy may supplant the market for the original by distributing copies of his or her own. To guard against the unauthorized copying and redistribution of their content, many copyright owners do not make their content available for downloading, and instead distribute the content using streaming technology in a manner that does not permit downloading.

5. A large majority of all Internet Web pages that deliver streaming music or video use the RealNetworks' format.

RealNetworks' Products

6. The RealNetworks' products at issue in this action include the "RealProducer," the "RealServer" and the "RealPlayer." These products may be used together to form a system for distributing, retrieving and playing digital audio and video content via the Internet.

7. Owners of audio or video content may choose to use a RealNetworks product to encode their digital content into RealNetworks' format. Once encoded in that format, the media files are called RealAudio or RealVideo (collectively "RealMedia") files.

8. After a content owner has encoded its content into the RealMedia format, it may decide to use a "RealServer" to send that content to consumers. A RealServer is software program that resides on a content owner's computer that holds RealMedia files and "serves" them to consumers through streaming.

9. The RealServer is not the only available means for distributing RealMedia files. RealMedia files may also be made available on an ordinary web server instead of a RealServer. An end-user can download content from an ordinary web server using nothing more than a freely available Internet browser such as Netscape's Navigator or Microsoft's Internet Explorer.

10. To download streaming content distributed by a RealServer, however, a consumer must employ a "RealPlayer." The RealPlayer is a software program that resides on an end-user's computer and must be used to access and play a streaming RealMedia file that is sent from a RealServer.

RealNetworks' Security Measures

11. RealNetworks' products can be used to enable owners of audio and video content to make their content available for consumers to listen to or view, while at the same time securing the content against unauthorized access or copying.

12. The first of these measures, called the "Secret Handshake" by RealNetworks, ensures that files hosted on a RealServer will only be sent to a RealPlayer. The Secret Handshake is an authentication sequence which only RealServers and RealPlayers know. By design, unless this authentication sequence takes place, the RealServer does not stream the content it holds.

13. By ensuring that RealMedia files hosted on a RealServer are streamed only to RealPlayers, RealNetworks can ensure that a second security measure, which RealNetworks calls the "Copy Switch," is given effect. The Copy Switch is a piece of data in all RealMedia files that contains the content owner's preference regarding whether or not the stream may be copied by end-users. RealPlayers are designed to read this Copy Switch and obey the content owner's wishes. If a content owner turns on the Copy Switch in a particular RealMedia file, when that file is streamed, an end-user can use the RealPlayer to save a copy of that RealMedia file to the user's computer. If a content owner does not turn on the Copy Switch in a RealMedia file, the RealPlayer will not allow an end-user to make a copy of that file. The file will simply "evaporate" as the user listens to or watches it stream.

*3 14. Through the use of the Secret Handshake and the Copy Switch, owners of audio and video content can prevent the unauthorized copying of their content if they so choose.

15. Content owners who choose to use the security measures described above are likely to be seeking

to prevent their works from being copied without their authorization. RealNetworks has proferred declarations from copyright owners that they rely on RealNetworks security measures to protect their copyrighted works on the Internet. Many of these copyright owners further state that if users could circumvent the security measures and make unauthorized copies of the content, they likely would not put their content up on the Internet for end-users.

16. Many copyright owners make content available on their Web site as a means to attract end-users to the Web site; that is, to drive "traffic" to the Web site. The more traffic a Web site generates, the more it can charge for advertisements placed on the Web site. Without RealNetworks' security measures, a copyright owner could lose the traffic its content generates. An end-user could obtain a copy of the content after only one visit and listen to or view it repeatedly without ever returning to the Web site. That end-user could also redistribute the content to others who would then have no occasion to visit the site in the first instance.

17. Copyright owners also use Real Networks' technology so that end-users can listen to, but not record, music that is on sale, either at a Web site or in retail stores. Other copyright owners enable users to listen to content on a "pay-per-play" basis that requires a payment for each time the end-user wants to hear the content. Without the security measures afforded by RealNetworks, these methods of distribution could not succeed. End-users could make and redistribute digital copies of any content available on the Internet, undermining the market for the copyrighted original.

18. RealNetworks' success as a company is due in significant part to the fact that it has offered copyright owners a successful means of protecting against unauthorized duplication and distribution of their digital works.

The RealPlayer Search Functionality

19. In addition to its content playing and content protection capabilities, the RealPlayer enables end-users to search the Internet for audio and video content. Currently, a company known as Snap! LLC supplies the search services available to end-users through the RealPlayer under a contract with RealNetworks.

20. Under RealNetworks' contract with Snap, the search bar on the bottom of the RealPlayer's graphical user interface (the screen end-users view and interact with) is emblazoned with Snap's logo. An end-user can input a search request by inserting "key words" into the search bar. The RealPlayer then uses Snap's search services to locate specific content corresponding to the search request from among the millions of media files available on the Internet. The RealPlayer then routes the end-user to a Web site maintained and co-branded by RealNetworks and Snap, where the names and locations of the files responsive to the search request are displayed.

***4** 21. Through this process, Snap garners visibility and visitors, enhancing Snap's ability to sell advertising and products. Snap compensates RealNetworks for the promotional value it receives based on the number of searches performed by users who are directed to the Snap search engine. RealNetworks maintains that it has earned several million dollars from its contract with Snap.

Streambox

22. Defendant Streambox, Inc. is a Washington corporation which provides software products for processing and recording audio and video content, including but not limited to content which is streamed over the Internet. Streambox also maintains a searchable database of Internet web addresses of various audio and video offerings on the Internet. The Streambox products at issue in this case are known as the Streambox VCR, the Ripper, and the Ferret.

Streambox VCR

23. The Streambox VCR enables end-users to access and download copies of RealMedia files that are streamed over the Internet. While the Streambox VCR also allows users to copy RealMedia files that are made freely available for downloading from ordinary web servers, the only function relevant to this case is the portions of the VCR that allow it to access and copy RealMedia files located on RealServers.

24. In order to gain access to RealMedia content located on a RealServer, the VCR mimics a

RealPlayer and circumvents the authentication procedure, or Secret Handshake, that a RealServer requires before it will stream content. In other words, the Streambox VCR is able to convince the RealServer into thinking that the VCR is, in fact, a RealPlayer.

25. Having convinced a RealServer to begin streaming content, the Streambox VCR, like the RealPlayer, acts as a receiver. However, unlike the RealPlayer, the VCR ignores the Copy Switch that tells a RealPlayer whether an end-user is allowed to make a copy of (i.e., download) the RealMedia file as it is being streamed. The VCR thus allows the end-user to download RealMedia files even if the content owner has used the Copy Switch to prohibit end-users from downloading the files.

26. The only reason for the Streambox VCR to circumvent the Secret Handshake and interact with a RealServer is to allow an end-user to access and make copies of content that a copyright holder has placed on a RealServer in order to secure it against unauthorized copying. In this way, the Streambox VCR acts like a "black box" which descrambles cable or satellite broadcasts so that viewers can watch pay programming for free. Like the cable and satellite companies that scramble their video signals to control access to their programs, RealNetworks has employed technological measures to ensure that only users of the RealPlayer can access RealMedia content placed on a RealServer. RealNetworks has gone one step further than the cable and satellite companies, not only controlling access, but also allowing copyright owners to specify whether or not their works can be copied by end-users, even if access is permitted. The Streambox VCR circumvents both the access control and copy protection measures.

***5** 27. The Streambox VCR can be distinguished from a third-party product sold by RealNetworks called GetRight. GetRight enables end-users to download RealAudio files that have been placed on a web server, but not RealAudio files placed on a RealServer.

28. A copyright owner that places a RealMedia file onto a web server instead of a RealServer does not make use of protections offered by the RealNetworks security system. Thus, when GetRight is used to obtain such a file, it need not and does not circumvent RealNetworks' access control and copyright protection measures. GetRight cannot access materials available from a RealServer because it cannot perform the requisite Secret Handshake. Unlike GetRight, the Streambox VCR circumvents the Secret Handshake and enables users to make digital copies of content that the copyright owner has indicated that it should not be copied.

29. Once an unauthorized, digital copy of a RealMedia file is created it can be redistributed to others at the touch of a button.

30. Streambox's marketing of the VCR notes that end-users can "[d]ownload RealAudio and RealMedia files as easily as you would any other file, then reap the benefits of clean, unclogged streams straight from your hard drive" and that the product can be used by "savvy surfers who enjoy taking control of their favorite Internet music/video clips."

31. The Streambox VCR poses a threat to RealNetworks' relationships with existing and potential customers who wish to secure their content for transmission over the Internet and must decide whether to purchase and use RealNetworks' technology. If the Streambox VCR remains available, these customers may opt not to utilize RealNetworks' technology, believing that it would not protect their content against unauthorized copying.

Streambox Ripper

32. Streambox also manufactures and distributes a product called the Streambox Ripper. The Ripper is a file conversion application that allows conversion (adaptation) of files from RealMedia format to other formats such as .WAV, . RMA, and MP3. The Ripper also permits conversion of files between each of these formats, i.e., .WAV to .WMA and .WAV to MP3.

33. The Ripper operates on files which are already resident on the hard disk of the user's computer. The Ripper permits users to convert files that they have already created or obtained (presumably through legitimate means) from one format to another.

34. Streambox has proferred evidence that one potential use of the Ripper would be to permit copyright owners to translate their content directly from the RealMedia format into other formats that they may wish to utilize for their own work. Streambox has provided examples of various content owner who need a way to convert their own RealMedia files into different formats, such as .WAV for editing, or .WMA to accommodate those users who wish to access the content with a Windows Media Player instead of a RealPlayer. In addition, content which is freely available, such as public domain material and material which users are invited and even encouraged to access and copy, may be converted by the Ripper into a different file format for listening at a location other than the user's computer.

Streambox Ferret

***6** 35. Streambox manufactures, markets, and distributes a third product called the Streambox Ferret. The Ferret may be installed as a "plug-in" application to the RealPlayer.

36. When a consumer installs the Ferret as a plug-in to the RealPlayer, the RealPlayer's graphical user interface is configured with an added button, which allows the user to switch between the Snap search engine and the Streambox search engine. The use of the Ferret may also result in replacement of the "Snap.Com" logo that appears on the RealPlayer's graphical user interface with a "Streambox" logo.

37. When consumers install the Ferret as a plug-in to the RealPlayer, the visual appearance and operation of the RealPlayer is altered.

CONCLUSIONS OF LAW

1. The Court has jurisdiction over this action under 28 U.S.C. §§ 1331 and 1338.

2. The Court finds that RealNetworks has standing to pursue DMCA claims under 17 U.S.C. § 1203, which affords standing to "any person" allegedly injured by a violation of sections 1201 and 1202 of the DMCA.

Preliminary Injunction Standard

3. To obtain a preliminary injunction, a party must show either (1) a combination of probable success on the merits and the possibility of irreparable harm, or (2) that serious questions are raised and the balance of hardships tips in its favor. *Apple Computer v. Formula Int'l, Inc.*, 725 F.2d 521, 523 (9 th Cir.1984). These are not separate tests, but rather "opposite ends of a single 'continuum in which the required showing of harm varies inversely with the required showing of meritoriousness." ' *Rodeo Collection v. West* Seventh, 812 F.2d 1215, 1217 (9 th Cir.1987); *Cadence Design Sys., Inc. v. Avant! Corp.*, 125 F.3d 824, 826 (9 th Cir.1997), *cert denied,* 118 S.Ct. 1795 (1998) (quotation omitted).

4. RealNetworks argues that a plaintiff who demonstrates a reasonable likelihood of success on claims under section 1201 of the DMCA is entitled to a presumption of irreparable harm. In support of this argument, RealNetworks cites cases in which such a presumption was afforded to plaintiffs who brought copyright *infringement* claims. *See Cadence Design Sys., Inc. v. Avant! Corp.*, 125 F.3d 824, 827 (9 th Cir.1997), *cert. denied,* 118 S.Ct. 1795, and *Triad Sys. Corp. v. Southeastern Express,* 64 F.3d 1330, 1335 (9 th Cir.1995).

5. RealNetworks' claims against the Streambox VCR and the Ripper, by contrast, arise under section 1201 of the DMCA, and thus do not constitute copyright "infringement" claims. *See* 1 *Nimmer on Copyright* (1999 Supp.), § 12.A17[B] (noting that section 1201 of the DMCA occupies "a niche distinct from copyright infringement" and that section 1201 is removed from the Act's definition of copyright infringement.) Because the DMCA is a recently-enacted statute, there appears to be no authority holding that a plaintiff seeking a preliminary injunction who shows a reasonable likelihood of success on a claim arising under section 1201 of the DMCA is entitled to a presumption of irreparable harm.

RealNetworks Has Demonstrated a Reasonable Likelihood of Success on its DMCA Claims With Respect to the Streambox VCR

***7** 6. The DMCA prohibits the manufacture, import, offer to the public, or trafficking in any technology, product, service, device, component, or part thereof that: (1) is primarily designed or

produced for the purpose of circumventing a technological measure that effectively "controls access to" a copyrighted work or "protects a right of a copyright owner;" (2) has only limited commercially significant purpose or use other than to circumvent such technological protection measures; or (3) is marketed for use in circumventing such technological protection measures. 17 U.S.C. §§ 1201(a)(2), 1201(b).

Parts of the VCR Are Likely to Violate Sections 1201(a)(2) and 1201(b)

7. Under the DMCA, the Secret Handshake that must take place between a RealServer and a RealPlayer before the RealServer will begin streaming content to an end-user appears to constitute a "technological measure" that "effectively controls access" to copyrighted works. *See* 17 U.S.C. § 1201(a)(3)(B) (measure "effectively controls access" if it "requires the application of information or a process or a treatment, with the authority of the copyright holder, to gain access to the work"). To gain access to a work protected by the Secret Handshake, a user must employ a RealPlayer, which will supply the requisite information to the RealServer in a proprietary authentication sequence.

8. In conjunction with the Secret Handshake, the Copy Switch is a "technological measure" that effectively protects the right of a copyright owner to control the unauthorized copying of its work. *See* 17 U.S.C. § 1201(b)(2)(B) (measure "effectively protects" right of copyright holder if it "prevents, restricts or otherwise limits the exercise of a right of a copyright owner"); 17 U.S.C. § 106(a) (granting copyright holder exclusive right to make copies of its work). To access a RealMedia file distributed by a RealServer, a user must use a RealPlayer. The RealPlayer reads the Copy Switch in the file. If the Copy Switch in the file is turned off, the RealPlayer will not permit the user to record a copy as the file is streamed. Thus, the Copy Switch may restrict others from exercising a copyright holder's exclusive right to copy its work.

9. Under the DMCA, a product or part thereof "circumvents" protections afforded a technological measure by "avoiding, bypassing, removing, deactivating or otherwise impairing" the operation of that technological measure. 17 U.S.C. §§ 1201(b)(2)(A), 1201(a)(2)(A). Under that definition, at least a part of the Streambox VCR circumvents the technological measures RealNetworks affords to copyright owners. Where a RealMedia file is stored on a RealServer, the VCR "bypasses" the Secret Handshake to gain access to the file. The VCR then circumvents the Copy Switch, enabling a user to make a copy of a file that the copyright owner has sought to protect.

10. Given the circumvention capabilities of the Streambox VCR, Streambox violates the DMCA if the product or a part thereof: (i) is primarily designed to serve this function; (ii) has only limited commercially significant purposes beyond the circumvention; or (iii) is marketed as a means of circumvention. 17 U.S.C. §§ 1201(a)(2)(A-C), 1201(b)(b)(A-C). These three tests are disjunctive. *Id.* A product that meets only one of the three independent bases for liability is still prohibited. Here, the VCR meets at least the first two.

***8** 11. The Streambox VCR meets the first test for liability under the DMCA because at least a part of the Streambox VCR is primarily, if not exclusively, designed to circumvent the access control and copy protection measures that RealNetworks affords to copyright owners. 17 U.S.C. §§ 1201(a)(2)(A), 1201(b)(c)(A).

12. The second basis for liability is met because portion of the VCR that circumvents the Secret Handshake so as to avoid the Copy Switch has no significant commercial purpose other than to enable users to access and record protected content. 17 U.S.C. § 1201(a)(2)(B), 1201(b)(d)(B). There does not appear to be any other commercial value that this capability affords.

13. Streambox's primary defense to Plaintiff's DMCA claims is that the VCR has legitimate uses. In particular, Streambox claims that the VCR allows consumers to make "fair use" copies of RealMedia files, notwithstanding the access control and copy protection measures that a copyright owner may have placed on that file.

14. The portions of the VCR that circumvent the secret handshake and copy switch permit consumers to obtain and redistribute perfect digital copies of

audio and video files that copyright owners have made clear they do not want copied. For this reason, Streambox's VCR is not entitled to the same "fair use" protections the Supreme Court afforded to video cassette recorders used for "time-shifting" in *Sony Corp. v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

15. The *Sony* decision turned in large part on a finding that substantial numbers of copyright holders who broadcast their works either had authorized or would not object to having their works time-shifted by private viewers. *See Sony*, 464 U.S. at 443, 446. Here, by contrast, copyright owners have specifically chosen to prevent the copying enabled by the Streambox VCR by putting their content on RealServers and leaving the Copy Switch off.

16. Moreover, the *Sony* decision did not involve interpretation of the DMCA. Under the DMCA, product developers do not have the right to distribute products that circumvent technological measures that prevent consumers from gaining unauthorized access to or making unauthorized copies of works protected by the Copyright Act. Instead, Congress specifically prohibited the distribution of the tools by which such circumvention could be accomplished. The portion of the Streambox VCR that circumvents the technological measures that prevent unauthorized access to and duplication of audio and video content therefore runs afoul of the DMCA.

17. This point is underscored by the leading treatise on copyright, which observes that the enactment of the DMCA means that "those who manufacture equipment and products generally can no longer gauge their conduct as permitted or forbidden by reference to the *Sony* doctrine. For a given piece of machinery might qualify as a stable item of commerce, with a substantial noninfringing use, and hence be immune from attack under *Sony*' s construction of the Copyright Act--but nonetheless still be subject to suppression under Section 1201." 1 *Nimmer on Copyright* (1999 Supp.), § 12A.18[B]. As such, "[e]quipment manufacturers in the twenty-first century will need to vet their products for compliance with Section 1201 in order to avoid a circumvention claim, rather than under *Sony* to negate a copyright claim." *Id.*

***9** 18. Streambox also argues that the VCR does not violate the DMCA because the Copy Switch that it avoids does not "effectively protect" against the unauthorized copying of copyrighted works as required by § 1201(a)(3)(B). Streambox claims this "effective" protection is lacking because an enterprising end-user could potentially use other means to record streaming audio content as it is played by the end-user's computer speakers. This argument fails because the Copy Switch, in the ordinary course of its operation when it is on, restricts and limits the ability of people to make perfect digital copies of a copyrighted work. The Copy Switch therefore constitutes a technological measure that effectively protects a copyright owner's rights under section. 1201(a)(3)(B).

19. In addition, the argument ignores the fact that before the Copy Switch is even implicated, the Streambox VCR has already circumvented the Secret Handshake to gain access to a unauthorized RealMedia file. That alone is sufficient for liability under the DMCA. *See* 17 U.S.C. § 1201(i)(e).

20. Streambox's last defense to liability for the VCR rests on Section 1201(c)(3) of the DMCA which it cites for the proposition that the VCR is not required to respond to the Copy Switch. Again, this argument fails to address the VCR's circumvention of the Secret Handshake, which is enough, by itself, to create liability under Section 1201(a)(2).

21. Moreover, Section 1201(c)(3) states that "[n]othing in this section shall require ... a response to any particular technological measure, so long as ... the product ... does not otherwise fall within the prohibitions of subsections (a)(2) or (b)(1)." 17 U.S.C. § 1201(c)(3). As the remainder of the statute and the leading copyright commentator make clear, Section 1201(c)(3) does not provide immunity for products that circumvent technological measures in violation of Sections 1201(a)(2) or (b)(1). *See* 17 U.S.C. § 1201(c)(3) (a product need not respond to a particular measure *"so long as such ... product ... does not otherwise fall within the prohibitions of subsections (a)(2) or (b)(1)."* (emphasis added); 1 *Nimmer on Copyright* (1999 Supp.), § 12A.05[C]. If the statute meant what Streambox suggests, any manufacturer of circumvention tools could avoid DMCA liability simply by claiming it chose not to

respond to the particular protection that its tool circumvents.

22. As set forth above, the Streambox VCR falls within the prohibitions of sections 1201(a)(2) and 1201(b)(1). Accordingly, Section 1201(c)(3) affords Streambox no defense.

RealNetworks is Likely to Suffer Irreparable Harm With Respect to the VCR

23. RealNetworks argues that because it has demonstrated a reasonable likelihood of success on its DMCA claims concerning the VCR, it is entitled to a presumption of irreparable harm. As noted above, however, this point is not settled.

24. Assuming that a plaintiff who demonstrates a reasonable likelihood of success with respect to claims arising under section 1201 of the DMCA is entitled to a presumption of irreparable harm, RealNetworks would be entitled to such a presumption.

***10** 25. In the event that such a presumption is not applicable, RealNetworks has demonstrated that it would likely suffer irreparable harm if the Streambox VCR is distributed. The VCR circumvents RealNetworks' security measures, and will necessarily undermine the confidence that RealNetworks' existing and potential customers have in those measures. It would not be possible to determine how many of RealNetworks' existing or potential customers declined to use the company's products because of the perceived security problems created by the VCR's ability to circumvent RealNetworks' security measures.

26. An injunction against the VCR also would serve the public interest because the VCR's ability to circumvent RealNetworks' security measures would likely reduce the willingness of copyright owners to make their audio and video works accessible to the public over the Internet.

RealNetworks Has Not Demonstrated that It Is Reasonably Likely to Succeed on its DMCA Claim With Respect to the Ripper.

27. RealNetworks also alleges that Streambox's marketing and distribution of the Ripper violates section 1201(b) (but not section 1201(a)(2)) of the DMCA.

28. RealNetworks maintains that the primary purpose and only commercially significant use for the Ripper would be to enable consumers to prepare unauthorized "derivatives" of copyrighted audio or video content in the RealMedia format in violation of 17 U.S.C. § 106(2).

29. The Ripper has legitimate purposes and commercially significant uses. For example, the Ripper may be used by content owners, including copyright holders, to convert their content from the RealMedia format to other formats. Streambox has submitted evidence that at least some content owners would use the Ripper for this legitimate purpose. The Ripper may also be used by consumers to convert audio and video files that they acquired with the content owner's permission from RealMedia to other formats. RealNetworks has not demonstrated that it is likely to succeed on its claims that the Ripper violates sections 1201(b)(1)(A) or (B) of the DMCA.

30. RealNetworks' DMCA claims with respect to the Ripper rely largely on its argument that the proprietary RealMedia format constitutes a technological measure that effectively protects a right of a copyright owner because it prevents end-users from making derivative works based on audio or video content that a consumer obtains in RealMedia format. RealNetworks did not offer this argument in any detail in its opening memorandum.

31. There is little evidence that content owners use the RealMedia format as a "technological measure" to prevent end-users from making derivative works. In any case, RealNetworks has not introduced evidence that a substantial number of content owners would object to having end-users convert RealMedia files that they legitimately obtain into other formats.

32. Similarly, RealNetworks has not submitted substantial evidence that the Ripper's alleged violations of section 1201(b) will cause RealNetworks injury. None of the numerous declarations submitted by RealNetworks' customers or recording industry employees express concern that the Ripper will permit RealMedia files to be

converted to other formats. Instead, persons who submitted these declarations indicate that they are concerned that unnamed Streambox products will permit consumers to acquire unauthorized copies of copyrighted works that are made available only in the streaming format. These concerns appear to relate to the functions of the Streambox VCR, not to the functions of the Ripper. The Ripper functions as a "converter," not as a copier. As such, these declarations do not suggest that the Ripper's alleged violations of section 1201(b) will result in any injury to RealNetworks in the form of lost customers or business.

***11** 33. RN further alleges that Streambox's marketing of the Ripper violates section 1201(b)(1)(C) of the DMCA. The brief quotes from Streambox's promotional materials that RealNetworks references do not appear to urge consumers to buy the Ripper in order to create derivative works in violation of the Copyright Act. The evidence submitted by RealNetworks is not sufficient to show a reasonable likelihood of success on its claims under section 1201(b)(1)(C).

34. In light of Streambox's demonstration that the Ripper has legitimate and commercially significant uses, RealNetworks has not shown that it is likely to succeed on its DMCA claims with respect to the product.

35. Even if RealNetworks had raised a "serious question" about the Ripper's alleged violation of the DMCA, RealNetworks has not demonstrated that the balance of hardships tips sharply in its favor. As noted above, RealNetworks has not submitted evidence that the sale of the Ripper would cause it to lose customers or goodwill. By contrast, enjoining the Ripper would deprive Streambox of the ability to market a potentially valuable product with legitimate uses.

RealNetworks Has Demonstrated that It Is Entitled to a Preliminary Injunction with Respect to the Ferret

36. Finally, RealNetworks claims that Streambox commits contributory and/or vicarious copyright infringement by distributing the Ferret product to the public. In order to prevail on such claims, RealNetworks must demonstrate that consumers who use the Ferret as a plug-in to the RealPlayer infringe RealNetworks' rights as a copyright owner. RealNetworks alleges that consumers who install the Ferret as a plug-in application to a RealPlayer create an unauthorized derivative of the RealPlayer, thus violating RealNetwork's rights under 17 U.S.C. § 106(2).

37. RealNetworks holds a valid copyright registration for version 7 of the RealPlayer, which constitutes prima facie evidence that RealNetworks is the owner of the copyright to the program. *See Apple Computer, Inc. v. Formula Int'l, Inc.*, 725 F.2d 521, 523 (9 th Cir.1984).

38. Streambox does not dispute that consumers who use the Ferret as a plug-in to a RealPlayer create a change the RealPlayer user interface by adding a clickable button that permits the user to access the Streambox search engine, rather than the Snap search engine.

39. Streambox claims that changes that the Ferret makes to the RealPlayer do not constitute the creation of a derivative work. To support this argument, Streambox cites generally the Ninth Circuit's decision in *Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.*, 964 F.2d 965 (9 th Cir.1992). As RealNetworks notes, however, the court in *Galoob* held that the manufacturer of a product that altered the audiovisual displays of a Nintendo game did not commit contributory copyright infringement because the "[t]he altered displays do not incorporate a portion of a copyrighted work in some concrete or permanent form." *Id.* at 968. Here, by contrast, the alterations to the RealPlayer assume a more concrete form that the altered displays at issue in *Galoob*.

***12** 40. However, the Court is not persuaded that RealNetworks has demonstrated that it is likely to succeed on its contributory/vicarious copyright infringement claims with respect to the Ferret. The facts and issues presented in the principal case that RealNetworks relies upon, *Micro Star v. Formgen, Inc.*, 154 F.3d 1107 (9 th Cir.1998), do not appear to be completely analogous to the situation here. In addition, RealNetworks' argument that consumers who install the Ferret breach a license agreement that they must agree to in order to obtain the RealPlayer was first raised in RealNetworks' reply

brief.

41. Nonetheless, the Court concludes that RealNetworks has raised serious questions going to the merits of its claim. It is undisputed that consumers who install the Ferret as a plug-in application to the RealPlayer cause the graphical interface of the RealPlayer to be modified, arguably creating a derivative work under 17 U.S.C. § 106(2) without the copyright owner's authorization. In addition, RealNetworks has proferred evidence that end users who install the Ferret are violating a license agreement with RealNetworks.

42. A plaintiff seeking a preliminary injunction who raises serious questions going to the merits of its claim is entitled to an injunction if the balance of hardships tips sharply in its favor. *See Micro Star v. Formgen, Inc.*, 154 F.3d 1107, 1109 (9 th Cir.1998).

43. The balance of hardships here clearly favors RealNetworks. The Ferret's ability to permit consumers to modify the RealPlayer jeopardizes RealNetworks' exclusive relationship with Snap. In addition, each time a consumer opts to use the Streambox search engine that is present on a modified RealPlayer rather than the Snap search engine that is present on an unmodified RealPlayer costs RealNetworks royalty payments from Snap, and it would be difficult if not impossible to calculate the lost revenue to RealNetworks.

44. By contrast, the hardship that Streambox would experience if an injunction issued against the product would not be nearly as severe. The Ferret plug-in simply provides consumers with a way to access the Streambox search engine through the RealPlayer. The Streambox search engine is already accessible to consumers in other places. If the Ferret is not available for distribution as a plug-in to the RealPlayer, consumers will still have the ability to conveniently access and use the Streambox search engine.

CONCLUSION

Consistent with the findings of fact and conclusions of law above, the Court hereby ORDERS that:

During the pendency of this action, Defendant Streambox, Inc. and its officers, agents, servants, employees and attorneys, and those persons in active concert and participation with Streambox, Inc. who receive actual notice of this Preliminary Injunction, are restrained and enjoined from manufacturing, importing, licensing, offering to the public, or offering for sale:

a) versions of the Streambox VCR or similar products that circumvent or attempt to circumvent RealNetworks' technological security measures, and from participating or assisting in any such activity;

***13** b) versions of the Streambox Ferret or similar products that modify RealNetworks' RealPlayer program, including its interface, its source code, or its object code, and from participating or assisting in any such activity.

Plaintiff's motion for a preliminary injunction with respect to the Streambox Ripper is DENIED.

This Order shall be effective immediately, on the condition that RealNetworks continues to maintain security with the Clerk in the amount of $1,000,000 for the payment of such costs and damages as may be incurred by Streambox if it is found that Streambox was wrongfully enjoined by this Order.

The TRO entered by Judge Coughenour on December 23, 1999, and extended by the Court until 5:00 p.m. on January 18, 2000, is hereby VACATED by this Order.

The clerk is directed to provide copies of this order to all counsel of record.

2000 WL 127311 (W.D.Wash.)

Motions, Pleadings and Filings (Back to top)

. 2:99CV02070 (Docket)
(Dec. 21, 1999)

END OF DOCUMENT

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the Brief of *Amici Curiae* ESA, RIAA, and MPAA in Support of Appellees and Affirmance was duly served upon the following, by forwarding two copies of the Brief via first class mail, postage prepaid, to:

Jonathan Band Matthew Schruers Morrison & Foerster LLP 2000 Pennsylvania Avenue NW Suite 5500 Washington, DC 20006 202.887.1500	Steven H. Rovak Kirill Y. Abramov Sonnenschein Nash & Rosenthal LLP One Metropolitan Square, Suite 3000 St. Louis, MO 63102 314.241.1800
Carol Anne Been Gerald E. Fradin Sonnenschein Nash & Rosenthal LLP 8000 Sears Tower Chicago, IL 60606 312.876.8000	Jennifer M. Urban Director, Intellectual Property Clinic Clinical Assistant Professor of Law The Law School, Rm. 410 University of Southern California Los Angeles, CA 90089-0071 213.740.1538
Mark S. Sableman Matthew Braunel Thompson Coburn LLP One US Bank Plaza St. Louis, MO 63101-1693 314.552.6000	Cindy A. Cohn Jason M. Schultz Electronic Frontier Foundation 454 Shotwell Street San Francisco, CA 94110 415.436.9333
Robert M. Galvin Paul S. Grewal Richard C. Lin Day & Casebeer 20300 Stevens Creek Boulevard Suite 400 Cupertino, CA 95014 408.873.0110	Karen Tokarz Clinical Education Program Washington University School of Law Anheuser-Busch Hall One Brookings Drive St. Louis, MO 63130 314.935.6414

Peter Jaszi Glushko-Samuelson Intellectual Property Law Clinic Washington College of Law American University 4800 Massachusetts Avenue, NW Washington, DC 20016 202.274.4216	Matthew J. Conigliaro Andrew C. Greenberg Carlton Fields, P.A. Corporate Center Three at International Plaza 4221 W. Boy Scout Blvd. Tampa, FL 33647-5736 813.223.7000
Deirdre K. Mulligan Director, Samuelson Law, Technology & Public Policy Clinic Acting Clinical Professor of Law University of California at Berkeley School of Law (Boalt Hall) 346 North Addition, Boalt Hall Berkeley, CA 94720-7200 510.642.0499	Raymond T. Nimmer Leonard Childs Professor of Law University of Houston Law Center 100 Law Center Houston, Texas 77004 713.743.2152
Laura M. Quilter Samuelson Law, Technology & Public Policy Clinic University of California at Berkeley School of Law (Boalt Hall) 389 North Addition, Boalt Hall Berkeley, CA 94720-7200	

This 3rd day of March, 2005.

Katherine A. Fallow