04-3654

IN THE

United States Court of Appeals

FOR THE EIGHTH CIRCUIT

——o0o——

DAVIDSON & ASSOCIATES, INC.,
D.B.A. BLIZZARD ENTERTAINMENT,
AND VIVENDI UNIVERSAL GAMES, INC.,

Plaintiffs-Appellees,

—against—

INTERNET GATEWAY, INC.,
TIM JUNG, ROSS COMBS
AND ROB CRITTENDEN,

Defendants-Appellants.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

Case No. 4:02CV498 CAS

Honorable Charles A. Shaw, United States District Judge

OPENING BRIEF OF DEFENDANTS-APPELLANTS INTERNET GATEWAY, INC., TIM JUNG, ROSS COMBS and ROB CRITTENDEN

Robert M. Galvin, *pro hac vice*
Paul S. Grewal, *pro hac vice*
Richard C. Lin, *pro hac vice*
DAY CASEBEER MADRID &
BATCHELDER LLP
20300 Stevens Creek Blvd. Suite 400
Cupertino, CA 95014
(408) 873-0110

Jason M. Schultz, *pro hac vice*
ELECTRONIC FRONTIER
FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

Mark Sableman (4244)
Matthew Braunel (109915)
THOMPSON COBURN LLP
One US Bank Plaza
St. Louis, MO 63101-1611
(314) 552-6000

Attorneys for Defendants-Appellants

SUMMARY OF THE CASE

Defendants-Appellants Internet Gateway, Incorporated, Tim Jung, Ross Combs, and Rob Crittenden ("Defendants") appeal the District Court's order granting Plaintiffs-Appellees Davidson & Associates, Incorporated, D.B.A. Blizzard Entertainment, and Vivendi Universal Games, Inc.'s ("Plaintiffs") motion for partial summary judgment and denying Defendants' summary judgment motion. This appeal will establish whether mass-market "shrinkwrap" and "clickwrap" licenses enforced under state law may outlaw fair use despite the explicit protections for fair use in the Copyright Act of 1976 and the Digital Millennium Copyright Act ("DMCA"). The appeal will also determine whether the public may rely upon the specific protections against liability included in the DMCA for fair use by reverse engineering.

Defendants request 30 minutes for oral argument (per side).

CORPORATE DISCLOSURE STATEMENT

No parent corporation or publicly held corporation owns 10% or more of the stock of Internet Gateway, Incorporated.

TABLE OF CONTENTS

PAGE NO.

TABLE OF CONTENTS (con'd)

PAGE NO.

TABLE OF CONTENTS (cont'd)

PAGE NO.

TABLE OF AUTHORITIES

PAGE NO.

CASES

TABLE OF AUTHORITIES (cont'd)

PAGE NO.

TABLE OF AUTHORITIES (cont'd)

PAGE NO.

TABLE OF AUTHORITIES (cont'd)

PAGE NO.

TABLE OF AUTHORITIES (cont'd)

PAGE NO.

STATUTES

OTHER AUTHORITIES

TABLE OF AUTHORITIES (cont'd)

PAGE NO.

JURISDICTION

The District Court exercised jurisdiction pursuant to the Copyright Act, 17 U.S.C. §§101 *et seq.*, 28 U.S.C. §1338(a) and (b), and 28 U.S.C. §1332. The September 30, 2004 Order entered by the District Court was a final order within the meaning of 28 U.S.C. §1291. Because Defendants filed a timely Notice of Appeal on October 28, 2004, Defendants invoke the jurisdiction of this Court under that statute.

ISSUES ON APPEAL

1. Did the District Court err in finding that Plaintiffs' copyright licenses could forbid all fair use and yet not conflict with and thus be preempted by federal copyright law's explicit protections for fair use?

Freightliner Corp. v. Myrick, 514 U.S. 280 (1995); *Sony Computer Entm't v. Connectix Corp.*, 203 F.3d 596 (9th Cir. 2000); *Sega Enterprises Ltd. v. Accolade, Inc.*, 977 F.2d 1510 (9th Cir. 1992); *Vault Corp. v. Quaid Software Ltd.,* 847 F.2d 255 (5th Cir. 1988); 17 U.S.C. §§107, 117; 17 U.S.C. §1201(f).

2. Did the District Court err in finding that the exemption from liability for circumvention set forth in 17 U.S.C. §1201(f) did not apply to Defendants' reverse engineering in developing a program that interoperates with Plaintiffs'

software?

Lexmark Int'l v. Static Control Components, 387 F.3d 522 (6th Cir. 2004); *Chamberlain Group, Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178 (Fed. Cir. 2004); *Sony*, 203 F.3d 596; *Sega*, 977 F.2d 1510; 17 U.S.C. §1201(f).

3. Did the District Court err in finding that despite Plaintiffs' failure to present any evidence of access to an effectively protected copyright work, Defendants had circumvented a copyright protection measure in Plaintiffs' computer software in violation of 17 U.S.C. §1201(a)(1) and had trafficked in circumvention technology in violation of 17 U.S.C. §1201(a)(2)?

Lexmark, 387 F.3d 522; *Sony,* 203 F.3d 596; *Sega*, 977 F.2d 1510; 17 U.S.C. §1201(a)(1); 17 U.S.C. §1201(a)(2).

INTRODUCTION

Since the first Copyright Act was passed over two hundred years ago, our copyright laws have always struck a balance. On the one hand, in recognition of the need to provide incentives to develop creative works, American copyright law rewards those who develop a work with the exclusive right to reproduce, distribute, perform, display and prepare derivatives of the work. These rights endure in most cases for a term no less than the life of the work's author plus 70 years. On the other hand, American copyright law also recognizes that previous creative works

can inspire new creative works. And so, notwithstanding a copyright owner's "exclusive" rights, our laws allow others to make certain uses of a developer's creative work even when the developer has withheld his consent to that use. *See* 17 U.S.C. §107 ("the fair use of a copyrighted work . . . is not an infringement of copyright"). These uses, known collectively as "fair use," enrich us all, by permitting the use of copyrighted works in criticism, comment, news reporting, teaching, scholarship, research and, most pertinent here, the creation of interoperable computer software.

All of this is at risk in this case. Only recently, in *Eldred v. Ashcroft*, 537 U.S. 186, 219 (2003), the Supreme Court reaffirmed that the fair use defense is an essential component of the copyright law framework, allowing "the public to use not only facts and ideas contained in a copyrighted work, but also expression itself in certain circumstances." This case will determine whether the Supreme Court's pronouncement in *Eldred* stands strong against efforts to defeat fair use or whether it gives way to Plaintiffs' legal attacks and end-runs. Specifically, it presents the question of whether developers of creative works may use contracts of adhesion and misguided claims brought under the DMCA to nullify the protections for fair use that Congress and the courts have long provided.

Defendants purchased computer videogames manufactured and sold by the Plaintiffs that are capable of being played over computer networks, including the internet. Inspired by their passion for these games and frustrated by the many problems and limitations of Plaintiffs' proprietary "Battle.net" online service, Defendants joined a non-profit, all-volunteer group of computer game hobbyists called the "bnetd" project. The bnetd project aimed to develop an alternative means of playing lawfully-purchased games online.

Reflecting the countless hours dedicated by its members, the bnetd project ultimately succeeded. Working together and without any compensation, the members of the bnetd project developed interoperable software — the "bnetd server" — that allowed players to play certain games sold by Plaintiffs over the internet and other computer networks in ways that were demonstrably different from and, in many cases, better than Plaintiffs' Battle.net service.

But rather than taking inspiration from its customers' efforts to improve the Battle.net service, Plaintiffs turned to the courts and filed this suit. Plaintiffs have argued that the bnetd project should be banned, and Defendants subject to crippling damages, because third parties unrelated to and unknown to Defendants who separately acquired unauthorized copies of Plaintiffs' games could more easily play those games online using the bnetd server than Plaintiffs' Battle.net service.

Yet while Plaintiffs cloak their claims in the rhetoric of piracy, this case has nothing to do with embracing or facilitating piracy. It has everything to do with Plaintiffs wanting to stifle competition in the market for internet game servers that work with its store-bought products via a pernicious combination of adhesion contracts in the form of "shrinkwrap" and "clickwrap" licenses and misguided claims under the DMCA. To the extent there has been any use of pirated videogames on Defendants' servers, Defendants have offered to address Plaintiffs' concerns, but Plaintiffs refused to cooperate by disclosing its methods for authenticating the games. Instead, Plaintiffs turned to adhesion contracts and the DMCA to force consumers to abandon an online gaming environment outside their control and instead use Plaintiffs' problem-ridden online service.

When the District Court granted Plaintiffs summary judgment and denied Defendants' motion for summary judgment, it concluded that Plaintiffs could use adhesion contracts and the DMCA to frustrate the balance struck by Congress between exclusive rights and fair use. In doing so, it ignored the plain language protecting fair use by reverse engineering in both the Copyright Act and the DMCA and the unavoidable conflict between these protections and state adhesion contracts that deny consumers these rights.

In section 107 of the Copyright Act, Congress provided explicit protections for fair use of copyrighted materials generally, declaring that the fair use of a copyrighted work is not an infringement even when it would otherwise violate the exclusive rights awarded to copyright owners under sections 106 and 106A of the Act. In section 1201(f) of the DMCA, Congress went further and specifically recognized the need to protect one particular form of fair use, fair use by reverse engineering for the purpose of making interoperable computer programs. In declaring fair use, and especially fair use by reverse engineering, off-limits to claims under the Copyright Act and the DMCA, Congress could not have been clearer.

There is no dispute that Defendants' reverse engineering was necessary to creating an interoperable computer program. The District Court acknowledged that:

- "reverse engineering as a fair use is firmly established," *Davidson & Assocs., Inc. v. Internet Gateway, Inc.*, 334 F.Supp.2d 1164, 1180 (E.D. Mo. 2004);
- "[r]everse engineering was necessary in order for the defendants to learn [Plaintiffs'] protocol language and to ensure that bnetd worked with [Plaintiffs'] games," *id.* at 1172;

- "compatibility required that bnetd speak the same protocol that the Battle.net service speaks," *id.*;
- "[i]t would not have been possible to create a workable bnetd server without reverse engineering [Plaintiffs'] software and protocols," *id.*;
- "[Plaintiffs] do[] not disclose the methods [they] use[] to generate CD Keys or to confirm the validity of CD Keys [that confirm the authenticity of a copy of Plaintiffs' videogames]," *id.* at 1173; and
- "there is no way that defendants could have implemented a check for CD Key validity [i.e. whether a copy of a game was authentic] in the bnetd program." *Id.* at 1173.

Despite these findings, the District Court refused to respect Congress's explicit protections for fair use by reverse engineering set forth in both 17 U.S.C. §§107 and 1201(f), as well as the opinions of several appellate courts recognizing the right to fair use by reverse engineering when necessary for computer program compatibility.

With respect to Plaintiffs' shrinkwrap and clickwrap adhesion contracts, the District Court ignored the clear conflict between the prohibitions on fair use by reverse engineering in those contracts and the protections afforded under 17 U.S.C.

§§107 and 1201(f). Instead, Defendants were held to have waived their rights to fair use of Plaintiffs' copyrighted works, even though the contracts fatally undermine Congress's intent to preserve public, as well as private, interests in access to the works. With respect to Plaintiffs' DMCA claims, the District Court ruled that Defendants could be held liable for circumvention even though they qualified for immunity under the reverse engineering exemption in 17 U.S.C. §1201(f) and even though Plaintiffs failed to establish that anything accessed by Defendants was protectable under federal copyright law. These extraordinary standards have never been the test for conflict preemption or DMCA liability in this or any other Circuit.

The decision below turns Congress's carefully crafted protections for fair use and especially fair use by reverse engineering on their heads. If affirmed, it will seriously threaten any meaningful possibility for not just fair use by reverse engineering, but any fair use. There is no genuine dispute that Plaintiffs' combination of adhesion contracts and DMCA claims attempt to prohibit any fair use of their copyrighted materials. The harm to Defendants is, and continues to be, enormous. The harm to the public at large is greater still. Through restrictions in "take it or leave it" shrinkwrap or clickwrap and the litigation of strategic claims brought under the DMCA, Plaintiffs or any other like-minded party could

effectively outlaw any fair use of their works, whether for the development of interoperable software, parody, criticism, or teaching.

Because review of a summary judgment is *de novo*, this Court considers afresh the law of fair use as applied to the facts. This review will demonstrate not only that the District Court erred in granting summary judgment for Plaintiffs, but that summary judgment should have been granted for Defendants.

STATEMENT OF THE CASE

On April 5, 2002, Plaintiffs filed suit for federal copyright infringement, federal trademark infringement, dilution, and false designation of origin, common law trademark infringement and unfair competition. On April 16, 2002, Plaintiffs amended their complaint to add a state law claim for breach of contract. On November 21, 2002, Plaintiffs further amended their complaint to add claims for circumvention of copyright protection systems and trafficking in circumvention technology.

On March 18, 2004, the District Court "entered a consent decree and permanent injunction which constituted the full and complete relief on plaintiffs' claims of copyright infringement, federal trademark infringement, federal false designation, and common-law trademark and infringement." 334 F.Supp.2d at 1167. On March 26, 2004, in accordance with the consent decree, the District

Court dismissed these claims with prejudice, leaving only Plaintiffs' circumvention, trafficking, and breach of contract claims as well as Defendants' related counterclaims for ruling on the summary judgment motions and briefs previously submitted by the parties.

On September 30, 2004, the District Court (1) granted "plaintiffs' motion for summary judgment as to Count VII of their second amended complaint for breach of contract and den[ied] defendants' motion for summary judgment as to the contract claim; (2) grant[ed] plaintiffs' motion for summary judgment as to the anti-circumvention claim in Count II and [denied] defendants' motion for declaratory judgment as to the anti-circumvention claim; and (3) grant[ed] plaintiffs' motion for summary judgment as to the trafficking in anti-circumvention technology in Count II and den[ied] defendants' motion for declaratory judgment regarding the trafficking in anti-circumvention technology claim." *Id.*

On October 28, 2004, Defendants filed a Notice of Appeal from the District Court's September 30 Order pursuant to 28 U.S.C. §1291.

STATEMENT OF THE FACTS

Internet Gateway, Inc. is a small, family-run business: its sole personnel are

Tim Jung and his wife Glorianne. DER195.[1] What the local coffee shop is to Starbucks, Tim and Glorianne Jung are to international giants like America Online (AOL) and Earthlink: they provide local internet service to their friends and neighbors in St. Peters, Missouri.

Like Ross Combs and Rob Crittenden, Mr. Jung purchased for his amusement computer videogames developed and sold by Plaintiffs. DER195, 201, 207. Soon after their purchases, the individual Defendants experienced a host of frustrations playing Plaintiffs' videogames over the internet using Plaintiffs' proprietary online Battle.net service. 334 F.Supp.2d at 1171-72; DER360-61. Among these frustrations were difficulties connecting to the service, mandatory exposure to advertising, rampant player profanity and cheating. *Id.* To address these frustrations, Defendants joined a non-profit volunteer group called the bnetd project. *Id.*

The goal of the bnetd project was simple: to develop an alternative for playing Plaintiffs' videogames online that addressed consumers' frustrations with Battle.net. 334 F.Supp.2d at 1172; DER362, 280. Working with like-minded computer enthusiasts across the country, the members of the bnetd project developed a program that could run on a computer server and facilitate

[1] Defendants' Excerpts of Record are cited "DER___."

communications between players of Plaintiffs' videogames. *Id.* Like other bnetd project members, Defendants participated as volunteers. DER364, 195, 201, 207. They were never paid anything for their work on the project. *Id.*

The "bnetd server" worked much like the software running the Plaintiffs' Battle.net service, by interoperating with the "Battle.net Mode" incorporated into the individual videogames. 334 F.Supp.2d at 1172. Although intended as a functional replacement for Battle.net, the bnetd server was written entirely from scratch and was developed using a scientific method known as "reverse engineering." 334 F.Supp.2d at 1172-73; DER168. As the Supreme Court has noted, reverse engineering is widely accepted and practiced in many technological fields and is nothing more than "starting with a known product and working backwards to divine the process which aided in its development or manufacture." *Kewanee Oil Co. v. Bicron Corp.*, 416 U.S. 470, 476 (1974).

Here, to allow purchasers of the games to play one another using the bnetd server, members of the bnetd project had to reverse engineer the communication protocols, that the Battle.net service speaks.[2] 334 F. Supp.2d at 1172; DER365. This was necessary because Plaintiffs' games expect to communicate using the

[2] Interactions between Plaintiffs' videogames and internet game servers like Battle.net are governed by a "protocol" — a language that two computer programs use to speak with each other. DER174-75.

Battle.net protocol, and will therefore be unable to work with a computer server that does not speak the protocol. *Id.* Using the protocol, their bnetd server could interact, or interoperate, with Plaintiffs' store-bought videogames in the same way that Plaintiffs' Battle.net server did. *Id.* As the District Court found, Defendants did not reverse engineer Plaintiffs' protocols as a short cut to building a program that could interoperate with Plaintiffs' videogames — they had no other choice:

> Reverse engineering was necessary in order for the defendants to learn Blizzard's protocol language and to ensure that bnetd worked with Blizzard games. ***It would not have been possible to create a workable bnetd server without reverse engineering [Plaintiffs'] software and protocols.***

334 F.Supp.2d at 1172 (emphasis added).

Although Defendants were able to implement much of the same functionality in the bnetd program as the Battle.net service, one feature that Defendants could not implement was Plaintiffs' "CD Key checking" mechanism. *Id.* at 1173. Plaintiffs' games are shipped to customers on CD-ROM disks. *Id.* at 1169; DER355, 237. These games come with a "CD Key," a unique sequence of alphanumeric characters that is printed on a sticker attached to the case in which the CD-ROM was packaged. *Id.* In order for the game to work on a computer, the user must type in the CD Key information when the game is first installed on the computer. *Id.*

As an additional security measure, the Battle.net service also checks the CD Key information of any game that attempts to connect to Battle.net. *Id.* To log on to the Battle.net service and access Battle.net Mode, the game initiates an authentication sequence between the game and the Battle.net server. *Id.* The game sends its CD Key information to the Battle.net server, which is in an encrypted form so that individuals cannot steal the information when it is transmitted over the Internet. *Id.* The Battle.net server then decrypts the CD Key information and determines whether or not the CD Key is valid, and whether it is currently being used by another player in the same "gateway," or geographic region. 334 F.Supp.2d at 1169; DER356, 238. If the CD Key is valid and not being used by another player in that gateway, the Battle.net server sends an "okay" signal to the game that allows the game to enter Battle.net Mode and use the Battle.net gaming services. *Id.* If the server sends any response other than "okay", the game will not play through the server and, eventually, the game will stop talking to the server entirely. DER178.

Because this communication between the Battle.net server and the game is encrypted, and because Plaintiffs do not disclose the methods it uses to generate CD Keys or to confirm the validity of CD Keys, there was no way for Defendants to implement the CD Key checking function in the bnetd program. 334 F.Supp.2d

at 1173; DER367-68. Instead, when a game attempts to connect with a server running the bnetd program and sends its CD Key information to the server, rather than determining whether or not the CD Key is valid or currently in use by another player, the bnetd program always has to send an "okay" signal to the game before the program can access the game's Battle.net Mode. *Id*. Just as with the Battle.net server, any other response from the bnetd server other than "okay" would prohibit game play. *Id.;* DER178.

Because Plaintiffs refused to disclose the information necessary to check for pirated games, the bnetd server had no way of validating whether the game copies with which it operated were authorized. *Id.* This created the potential for third parties to use bnetd servers with unauthorized game copies. However, Defendants never advised others to play unauthorized copies of Plaintiffs' videogames using the bnetd server. 334 F.Supp.2d at 1173; DER368, 197, 203. And in no way did the bnetd server help anyone to make an unlawful copy of any of Plaintiffs' games. *Id*.

Alarmed at the prospect of customers reverse engineering their own solution to Battle.net's many problems, Plaintiffs attempted to ban all reverse engineering of their products altogether. They did so by selling their videogames with an End User License Agreement ("EULA") that prohibits purchasers from engaging in any

reverse engineering of its software, including reverse engineering protected as fair use under the Copyright Act. 334 F.Supp.2d at 1169-71; DER257-73. The EULA is in the form of a "shrinkwrap" or "clickwrap" license, in that the terms of the license are not shown to the user until the user takes the game home and attempts to install the game onto his or her computer. 334 F.Supp.2d at 1169-70; DER356-58. The user cannot complete installation of the game unless he clicks on a button stating that he agrees to all of the terms of the EULA. *Id.* In addition, Plaintiffs' Battle.net service has a Terms of Use ("TOU") that is presented to first-time users of Battle.net after they have purchased and installed the game, and which requires the user to agree not to reverse engineer any part of the Battle.net software. *Id*.

None of these "agreements" were the result of any actual negotiation between Plaintiffs and their customers. DER195-97, 201-02, 207-08. Instead, the terms were offered on a "take it or leave it" basis, without any recognition of the impact of this absolute ban on reverse engineering on customers' fair use rights.

SUMMARY OF THE ARGUMENT

The District Court ruled that despite the clear conflict with federal statutory protections for all fair use of copyrighted materials, including fair use by reverse engineering, Plaintiffs could use state law to enforce contractual prohibitions on reverse engineering to prevent consumers from developing their own software that

could interoperate with their lawfully purchased videogames. Under the Supremacy Clause of the United States Constitution, this conflict is not permitted. As both the Supreme Court and this Court have held, state law is preempted where it "stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress." Plaintiffs' absolute ban on fair use completely undermines the explicit protections for fair use set forth in 17 U.S.C. §§107 and 1201(f). Because it relies upon state law to enforce this ban, Plaintiffs' ban is preempted by federal law.

The District Court also misapplied the standards applicable to both the reverse-engineering exemption and *prima facie* liability for circumvention and trafficking under the DMCA. Enacted in 1998, the DMCA created a new form of liability related to copyright infringement. Specifically, in section 1201, it created liability for those who circumvent technological tools that prevent digital piracy or traffic in devices that are designed for such circumvention. *See* 17 U.S.C. §1201(a), (b). It also included a host of specific exemptions that immunize circumventions under specific circumstances. *See* 17 U.S.C. §1201(d)-(j).

Regarding the reverse engineering exemption set forth in section 1201(f), the District Court incorporated a host of new requirements that are not found anywhere in the statute. For example, it held that the sole purpose behind a program

developed by reverse engineering could not be "interoperability" with authorized copies of videogames unless the program refused to interoperate with unauthorized copies of those games. The District Court also held that any program developed by reverse engineering for interoperability could not be intended as a functional alternative to a competing interoperable program offered by the copyright owner. Nor could the program be distributed for free. Nothing in section 1201(f) suggests these limitations and, in fact, these limitations contradict earlier case law on fair use by reverse engineering that Congress specifically intended to preserve. Compounding its error in its section 1201(f) analysis, the District Court also found that Defendants' actions comprised copyright infringement even though there was no evidence or analysis of infringement presented in the District Court's Order.

Regarding the *prima facie* case for circumvention and trafficking set forth in section 1201(a)(1) and (2), the District Court similarly ignored the plain language of the statute. Plaintiffs' Battle.net mode, the alleged work protected by Plaintiffs' CD Key checking mechanism, is a procedure, process, system or method. It is not creative expression entitled to copyright protection. Nor does Plaintiffs' CD Key checking mechanism "effectively control" access to Battle.net mode, when consumers can simply read the code for Battle.net off of the CD-ROM of the videogame that they have purchased.

ARGUMENT

I. STANDARD OF REVIEW

Orders denying and granting summary judgment are reviewed *de novo*. *See Walters v. Weiss*, No. 03-3674, 2004 WL 2913558, at *2 (8th Cir. Dec. 17, 2004). "The question before the district court, and this court on appeal, is whether the record, when viewed in the light most favorable to the non-moving party, shows that there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law." *Id.*

II. PLAINTIFFS' STATE CLAIM FOR BREACH OF CONTRACT IMPERMISSIBLY CONFLICTS WITH FEDERAL PROTECTIONS OF FAIR USE ACTIVITIES

The law of federal preemption is based on the Supremacy Clause of Article VI of the Constitution, which provides that "the Laws of the United States . . . shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding." *See Lorillard Tobacco Co. v. Reilly,* 553 U.S. 525, 540-41 (2001). Because state law may act "contrary" to the "Laws of United States" in a variety of ways, the Supreme Court has explained that federal law may preempt state law as follows: (1) Congress may expressly preempt state law in a federal statute; (2) even though not expressly stated by Congress, a state law may be subject to field preemption where "the scheme of federal regulation is sufficiently

comprehensive to make reasonable the inference that Congress 'left no room' for supplementary state regulation;" and (3) "in those areas where Congress has not completely displaced state regulation, federal law may nonetheless pre-empt state law to the extent it actually conflicts with federal law." *California Fed. Sav. and Loan Assoc. v. Guerra*, 479 U.S. 272, 280-81 (1987). This third form of preemption — conflict preemption — is the basis for Defendants' challenge to Plaintiffs' state law claims for breach of contract.

This Court has articulated and applied the Supreme Court's standard for finding conflict preemption of state law, holding that it may find implied conflict preemption "where state law 'stands as an obstacle to the accomplishment and execution of the full purposes and objectives of Congress.'" *Nordgren v. Burlington N. R.R. Co.,* 101 F.3d 1246, 1248 (8th Cir. 1996) (quoting *Freightliner,* 514 U.S. 280). This Court has further held that state law is conflict preempted by federal law where "state procedures interfere with the framework created by Congress." *Forest Park II v. Hadley*, 336 F.3d 724, 734 (8th Cir. 2003).

A. Congress's "full purposes and objectives" in passing the Copyright Act and Digital Millennium Copyright Act included protecting the right to fair use by reverse engineering.

The fair use doctrine has long been recognized as an important doctrine in copyright law that permits individuals to engage in certain unauthorized uses of

copyrighted material. *See* 4 *Nimmer on Copyright*, §13.05 (2004); *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569, 575-76 (1994) (tracing history of fair use doctrine back to English common law). As early as 1841, for example, Justice Story noted in *Folsom v. Marsh*, 9 F.Cas. 342, 344-45 (No. 4,901) (CCD Mass. 1841), that the unauthorized use of a copyrighted work "for the purposes of fair and reasonable criticism" would constitute a fair use of the work. More recently, the Supreme Court has explained that "[f]rom the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purpose, '[t]o promote the Progress of Science and useful Arts.'" *Campbell,* 510 U.S. at 575 (citing U.S. Const., Art. I, §8, cl. 8). *See also Eldred v. Ashcroft*, 537 U.S. 186, 219 (2003) ("the 'fair use' defense allows the public to use not only facts and ideas contained in a copyrighted work, but also expression itself in certain circumstances."); *Harper & Row Publishers, Inc. v. Nation Enterprises*, 471 U.S. 539, 549 (1985) (characterizing fair use as "a necessary incident of the constitutional policy of promoting the progress of science and the useful arts"); *Quality King Distribs., Inc. v. L'anza Research Int'l, Inc.*, 523 U.S. 135, 151 (1998) (noting "the importance of the fair use defense to publishers of scholarly works, as well as to publishers of periodicals").

The doctrine of fair use is grounded in the principle that "in truth, in

literature in science, and in art, there are, and can be, few, if any, things, which in an abstract sense, are strictly new and original throughout. Every book in literature, science and art, borrows, and must necessarily borrow, and use much which was well known and used before." *Campbell,* 510 U.S. at 575 (quoting J. Story in *Emerson v. Davies*, 8 F.Cas. 615, 619 (No. 4,436) (CCD Mass.1845)). Thus, to ensure that individuals retain the freedom to borrow from copyrighted materials so that new works may be created, the fair use doctrine "permits [and requires] courts to avoid rigid application of the copyright statute when, on occasion, it would stifle the very creativity which that law is designed to foster." *Campbell,* 510 U.S. at 577 (internal quotations omitted).

Indeed, many legal scholars have noted the importance of the fair use doctrine in promoting economic efficiency in situations where the restrictions of copyright would stifle beneficial uses of copyrighted material. Professor Landes and Judge Posner, for example, identify three types of situations in which fair use rights serve to promote economic efficiency. First, fair use promotes efficiency where the transaction costs of obtaining a license to the copyrighted work are prohibitively high relative to the benefit of the use, such as where all that the user wants to do is quote a brief passage of the work. William Landes and Richard Posner, *The Economic Structure of Intellectual Property Law*, at 115 (2003).

Second, fair use promotes efficiency where the unauthorized use provides a net benefit to the copyright holder, such as a book review that quotes portions of the book but at the same time provides free advertising of the work. *Id* at 117-18. Third, fair use promotes efficiency where any harm that the unauthorized use causes to the copyright holder is outweighed by the benefits to others, such as in the transformative use of the work to create a parody. *Id.* at 122.

While fair use began as a judicial doctrine, Congress later expressly recognized the fair use doctrine and put into place statutory protections for fair use by enacting 17 U.S.C. §107. Specifically, section 107 states:

> Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright ….

17 U.S.C. §107 (2004).

In addition, section 107 also includes a statement of four factors that are to be used by courts to determine whether an unauthorized use of a copyrighted work is protected as a fair use or not: (1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the

effect of the use upon the potential market for or value of the copyrighted work. *Id.* Congress therefore set forth in section 107 the guidelines that courts are to use to determine what activities constitute fair use in the individual instance. *See Campbell*, 510 U.S. at 577-78.

The legislative history of the Copyright Act highlights Congress's desire to ensure adequate protection of fair use rights through section 107. In the House Report regarding the enactment of section 107, the House Judiciary Committee characterized fair use as "one of the most important and well established limitations on the exclusive right of copyright owners." H.R. Rep. No. 94-1476, at 65 (1976). The legislative history further shows that Congress intended to preserve fair use law as it has been shaped by the courts: "the courts must be free to adapt the [fair use] doctrine to particular situations on a case-by-case basis. Section 107 is intended to restate the present judicial doctrine of fair use, not to change, narrow, or enlarge it in any way." *Id.* at 66; *see also Harper,* 471 U.S. at 549 ("The statutory formulation of the defense of fair use in the Copyright Act reflects the intent of Congress to codify the common-law doctrine."); *Campbell*, 510 U.S. at 577.

Recognizing this and applying the fair use principles set forth by Congress in section 107, numerous appellate courts have held that reverse engineering of

computer software for the purpose of making one computer program compatible with another, as Defendants did, is a form of fair use that is explicitly protected from copyright infringement liability. For example, in *Sega*, 977 F.2d at 1527-28, the Ninth Circuit addressed reverse engineering by disassembly, or code copying, and held that "where disassembly is the only way to gain access to the ideas and functional elements embodied in a copyrighted computer program and where there is a legitimate reason for seeking such access, disassembly is a fair use of the copyrighted work, as a matter of law." *See also Sony*, 203 F.3d at 602; *Micro Data Base Sys., Inc. v. Dharma Sys., Inc.*, 148 F.3d 649, 652 (7th Cir. 1998); *Bateman v. Mnemonics, Inc.*, 79 F.3d 1532, 1539 n. 18 (11th Cir. 1996); *Atari Games Corp. v. Nintendo of Am. Inc.*, 975 F.2d 832, 843 (Fed. Cir. 1992); *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255, 268-270 (5th Cir. 1988); *see also Lotus Dev. Corp. v. Borland Int'l, Inc.*, 49 F.3d 807, 821-22 (1st Cir. 1995) (Boudin, J., concurring), *aff'd by equally divided Court* 516 U.S. 233 (1996).

Indeed, the District Court did not dispute that reverse engineering as a fair use had been "firmly established," 334 F.Supp.2d at 1180, and numerous commentators have argued that fair use by reverse engineering is essential to competition in the software industry.[3] These cases and commentators all recognize

[3] *See, e.g.* J. Band and M. Katoh, *Interfaces on Trial: Intellectual Property and*

reverse engineering as "an essential part of innovation" that deserves protection because such activities can lead to "significant advances in technology." *Bonito Boats, Inc. v. Thunder Craft Boats, Inc.,* 489 U.S. 141, 160 (1989); *see also Brooktree Corp. v. Advanced Micro Devices, Inc*., 977 F.2d 1555, 1570 (Fed. Cir. 1992) (noting that, in the context of copyright protection for semiconductor chip layouts, Congress "described reverse engineering as activity that 'spurs innovation and technological progress'").

Reverse engineering is also so important as a method of research and investigation that some courts have required parties to undertake reverse engineering prior to filing suit in order to satisfy Fed. R. Civ. P. 11. *See, e.g., Refac Int'l, Ltd. v. Hitachi Ltd.*, 141 F.R.D. 281, 286-87 (C.D. Cal. 1991) (imposing Rule 11 sanctions on plaintiff for failing to reverse engineer products it accused of patent infringement as part of its pre-filing investigation); *Network*

Interoperability in the Global Software Industry, at 167-225 (1995); Julie E. Cohen, *Reverse Engineering and the Rise of Electronic Vigilantism: Intellectual Property Implications of 'Lock-out' Programs*, 68 S. Cal. L. Rev. 1091 (1995); Dennis S. Karjala, *Copyright Protection of Computer Software, Reverse Engineering and Professor Miller*, 19 U. Dayton L. Rev. 975 (1994); Mark A. Lemley & David McGowan, *The Law and Economics of Network Effects*, 86 Calif. L. Rev. 479 (1998); Charles R. McManis, *Intellectual Property Protection and Reverse Engineering of Computer Programs in the United States and the European Community*, 8 High Tech. L. J. 25 (1993).

Caching Tech., LLC v. Novell, Inc., 67 U.S.P.Q.2d 1034, 1039 (N.D. Cal. 2002) (holding that Rule 11 requires plaintiff to engage in "reverse engineering or its equivalent" as part of its investigation prior to filing patent infringement claim).

Not only has the principle of reverse engineering as fair use been embraced by the courts, but Congress has also explicitly recognized reverse engineering as a fair use in the DMCA and sought to ensure that reverse engineering activities would not be restricted in any way as a result of the enactment of anti-circumvention laws in the DMCA. To make clear that nothing in the DMCA affected defenses to copyright infringement including fair use, Congress enacted section 1201(c), which states that "[n]othing in this section shall affect rights, remedies, limitations, or other defenses to copyright infringement, *including fair use*, under this title." 17 U.S.C. §1201(c)(1) (emphasis added). To protect reverse engineering rights against claims of circumvention and trafficking, Congress enacted section 1201(f) in the DMCA, which shields from liability any reverse engineering of software for purposes of enabling interoperability. Specifically, section 1201(f) reads in relevant part:

> *Reverse engineering*.—(1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program

> with other programs…. (2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability….

17 U.S.C. §1201(f) (2004).

The legislative history behind Congress's action here is particularly illuminating. It reveals that Congress's intent in enacting section 1201(f) was to ensure that despite the anti-circumvention laws in the DCMA, the public would remain free to engage in reverse engineering activities defined by the courts as fair use. In the Senate Report on the DMCA, the Judiciary Committee characterized the purpose of (now) section 1201(f) as:

> to allow legitimate software developers to continue to engage in certain activities for the purpose of achieving interoperability to the extent permitted by law prior to enactment of this chapter. The objective is to ensure that the effect of current case law interpreting the Copyright Act is not changed by enactment of this legislation for certain acts of identification and analysis done in respect of computer programs. *See Sega Enterprises Ltd. v Accolade, Inc.,* 977 F.2d 1510, 24 U.S.P.Q.2d 1561 (9th Cir. 1992). The purpose of this section is to foster competition and innovation in the computer and software industry.

S. Rep. No. 105-190, at 13 (1998).

In sum, Congress's clear purpose in enacting section 107 of the Copyright Act and section 1201(f) of the DMCA as part of the "framework" of copyright

protection was to ensure that fair use rights, including fair use by reverse engineering that has been universally recognized as essential to promoting innovation, would not be restricted in any way. *See Lexmark*, 387 F.3d at 537 ("Congress has established a fair use defense to infringement claims to ensure that copyright protection advances rather than thwarts the essential purpose of copyright: '[t]o promote the Progress of Science and useful Arts.'").

B. Plaintiffs' state law enforcement of contract prohibitions on reverse engineering "stands as an obstacle" to Congress's fair use "purposes and objectives."

State law impermissibly "stands as an obstacle" to Congress's "full purposes and objectives" when it "undermines" those purposes and objectives. *Freightliner*, 514 U.S. at 289-90. Here, the record reveals that Plaintiffs' state law claims undermine, and therefore "stand as an obstacle" to, Congress's purpose and objectives in protecting fair use of copyrighted material.

Plaintiffs' video game products are distributed with an End User License Agreement ("EULA") that customers are forced to accept before they may install and use the Blizzard product they have purchased. These EULAs uniformly include a provision that prohibits the purchaser from engaging in any form of fair use of the purchased product, including fair use by reverse engineering. The provision states:

> [**Y]ou may not, in whole or in part copy, photocopy, reproduce, translate, reverse engineer**, derive source code, modify, disassemble, decompile … the Program … without the prior consent, in writing, of [Plaintiffs].

DER 258, 261-62, 266, 270 (emphasis added) In addition, before a customer can use Plaintiffs' Battle.net service, the customer must agree that he or she "shall not be entitled to … reverse engineer, modify, disassemble, or de-compile in whole or in part any Battle.net software." DER274. Thus, in order to use any of Plaintiffs' products or services, the customer must surrender all rights to engage in the fair use of those products and services, including specifically fair use by reverse engineering.[4]

The fact that Plaintiffs' complete ban on reverse engineering is included in shrinkwrap and clickwrap licenses, which the purchaser has no power or opportunity to negotiate, renders Plaintiffs' claims an even bigger obstacle to Congress's purposes and objectives in protecting fair use of copyrighted material. The purchaser has no choice other than to either accept all the contractual terms that have been dictated by Plaintiffs or return the product. In order to engage in

[4] By contrast, other software firms, including those in the videogame industry, employ End User License Agreements that restrict users from reverse engineering only to the extent that the restrictions do not impinge upon the users' fair use rights. DER317, 320.

any productive reverse engineering activities, however, the user must first have the ability to access to the work that is to be reverse engineered. Consequently, Plaintiffs' contractual restrictions create an impossible Catch-22 situation: in order to engage in legitimate reverse engineering of a Blizzard software product, an individual must first accede to Plaintiffs' contract; but by doing so, the individual surrenders all of his reverse engineering rights.

The Fifth Circuit's decision in *Vault Corp. v. Quaid Software Ltd.,* 847 F.2d 255 (5th Cir. 1988) is directly on point. As in the present case, in *Vault* a software producer attempted to enforce a software license that prohibited purchasers from engaging in any fair use of the software, including fair use both by reverse engineering the software and by making backup copies of the software. The license was drafted in accordance with a Louisiana statute, which permitted software producers to impose licenses that prohibit any adaptation of the software "by reverse engineering, decompilation or disassembly." *Id*. at 268-69. The Fifth Circuit held that the Louisiana statute impermissibly conflicted with the fair use purposes and objective set forth in §117 of the Copyright Act, which specifically authorizes software purchasers to make fair use of the software by creating backup copies, and was therefore preempted. *Id.* at 268-70. The *Vault* court thus squarely addressed the question of whether software companies could eliminate the fair use

rights of their customers through terms in contracts, and concluded that when state law contract terms conflict with provisions in the Copyright Act, the Copyright Act trumps.[5]

The District Court summarily dismissed the Fifth Circuit's decision in *Vault*, and relied instead upon the Federal Circuit decision in *Bowers v. Baystate Techs., Inc*., 320 F.3d 1317 (Fed. Cir. 2003), for the proposition that state contract law may usurp federal protections for fair use rights. *See* 334 F.Supp.2d at 1181.[6] The District Court's reliance on *Bowers*, a case involving express preemption and not conflict preemption, was misplaced.

In *Bowers*, the Federal Circuit considered whether the statutory preemption provision in the Copyright Act, embodied in 17 U.S.C. §301, would preempt a prohibition against reverse engineering in a software shrink-wrap license. The *Bowers* court focused on the limited language in section 301 that "all legal or

[5] It is of no consequence to the doctrine of conflict preemption that Plaintiffs rely on contract claims under state common law rather than a state statute. Just as statutes passed by state legislatures may be preempted by federal law, state law claims to enforce private rights may also be preempted where they impermissibly conflict with federal law. For example, in *Molasky v. Principal Mutual Life Ins. Co*., 149 F.3d 881, 883-84 (8th Cir. 1998), this Court held that a plaintiff's state law breach of contract claim was preempted by federal ERISA law. *See also Metropolitan Life Ins. Co. v. Taylor*, 481 U.S. 58, 62 (1987); *Oberkramer v. IBEW-NECA Service Center, Inc*., 151 F.3d 752, 756 (8th Cir. 1998).

[6] Notably, in *Bowers* the court agreed that "at times, federal regulation may preempt private contract." *Bowers*, 320 F.3d at 1323-24.

equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright … are governed exclusively by this title," and considered whether the plaintiff's contract claim was equivalent to any claim under federal copyright law. *Bowers*, 320 F.3d at 1323-25. Applying the First Circuit's "extra element" test, the Federal Circuit concluded that §301 did not expressly preempt the plaintiff's breach of contract claim because it was qualitatively different from a copyright infringement claim. *Id.*

But as noted by Judge Dyk in dissent, the *Bowers* court never addressed the issue of whether such a prohibition against reverse engineering might be preempted under principles of conflict preemption, rather than express preemption. *Id.* at 1336 (Dyk, J., dissenting). The District Court in this case made a similar error, despite Defendants' explicit statements in its briefs that its argument was based on the doctrine of conflict preemption, rather than statutory preemption. *Compare* 334 F.Supp.2d at 1174-75 *with* DER341, 148-49. Moreover, section 301 only addresses *claims* that may be equivalent to the rights protected under sections 106 and 106A of the Copyright Act. It does not address whether *defenses* such as fair use preempt state law claims because they conflict. The *Bowers* majority failed to recognize this distinction in its opinion.[7]

[7] Even the "extra element" test for section 301 preemption relied on by both the

The case law is clear that conflict preemption, a form of implied preemption, may exist even when there is an express statutory preemption provision. *See Freightliner*, 514 U.S. at 288-89 ("The fact that an express definition of the pre-emptive reach of a statute 'implies' — *i.e.,* supports a reasonable inference — that Congress did not intend to pre-empt other matters does not mean that the express clause entirely forecloses any possibility of implied pre-emption."); *cf. Gaier v. American Honda Motor Co., Inc.*, 529 U.S. 861, 870-72 (2000) (holding that presence of express preemption and savings clauses did not preclude conflict preemption analysis); *Union Center Redevelopment Corp. v. National Railroad Passenger Corp.*, 103 F.3d 62, 64-65 (8th Cir. 1997) (rejecting appellant's argument that there could be no implied preemption where a federal statute contains an express preemption clause).

In fact, other circuit courts have acknowledged that, in order to assess claims of preemption under the Copyright Act, one must take into consideration not only express preemption under section 301, but conflict preemption as well. For

---

Bowers majority and the District Court has been roundly criticized, including by courts that continue to apply it. *See, e.g. Ritchie v. Williams*, No. 03-1279, 2005 WL 41553, at *3 n.3 (6th Cir. Jan. 11, 2005). ("Thus, the 'extra element' test has proved circular in practice, and the cases are ad hoc, inconsistent, or wrong." (quoting Schuyler Moore, *Straightening Out Copyright Preemption*, 9 UCLA Ent. L. Rev. 201, 204 (2002)). *See also* David A. Rice, *Copyright and Contract: Preemption After Bowers v. Baystale,* 9 Roger Williams L. Rev. 595 (2004).

example, in *Brown v. Ames*, 201 F.3d 654 (5th Cir. 2000), the Fifth Circuit, after concluding that a state law misappropriation claim was not expressly preempted by section 301 of the Copyright Act, went further to examine whether the claim was conflict preempted. The court reasoned that "[t]he fact that section 301 does not apply does not end the inquiry, however. Although section 301 preemption is not appropriate, conflict preemption might be." *Id.* at 659; *see also Orson, Inc. v. Miramax Film Corp*., 189 F.3d 377, 383 (3rd Cir. 1999). Thus, it was error for the District Court to base its preemption decision solely on a conclusion that there was no express statutory preemption, and to completely ignore the additional issue of whether Blizzard's reverse engineering prohibition was conflict preempted by the Copyright Act and the DMCA.

Nor is the District Court's reasoning that all statutory rights can be waived persuasive. *See* 334 F.Supp.2d at 1181. Contrary to the District Court's view, not all statutory rights can be waived through contract. Where a statutory restriction on intellectual property rights serves public, as well as private, interests, parties cannot use state law to enforce a private contract extending those rights. For example, in the area of patent law, parties cannot contractually agree to extend the term of a patent. In *Brulotte v. Thys Co*., 379 U.S. 29 (1965), a patentee attempted to enforce licenses to its patents relating to hop-picking machines that required the

licensees to continue paying royalties one the patents even after the patents had expired. The Supreme Court held that such licenses were unenforceable because they constituted an impermissible attempt to use contracts to prolong the term of the patent monopolies past their expiration date. *Id.* at 32-33. The Court noted the danger that if the patentee's contract "device were available to patentees, the free market visualized for the post-expiration period would be subject to monopoly influences that have no proper place there." *Id*.

Similarly, in *Scott Paper Co. v. Marcalus Mfg. Co.*, 326 U.S. 249, 255-56 (1945), the Supreme Court explained the danger of allowing patent owners to limit through contracts uses of patented products that are expressly permitted under statute:

> If a manufacturer or user could restrict himself, by express contract … from using the invention of an expired patent, he would deprive himself and the consuming public of the advantage to be derived from his free use of the disclosures. The public has invested in such free use by the grant of a monopoly to the patentee for a limited time. Hence any attempted reservation or continuation in the patentee or those claiming under him of the patent monopoly, after the patent expires, whatever the legal device employed, runs counter to the policy and purpose of the patent laws.

Thus, courts have held that state law may not enforce private contracts that alter certain statutory limitations on patent rights, for such alterations would deprive the public of the rights the patent law has reserved to them. *See also Pope Mfg. Co. v. Gormully*, 144 U.S. 224, 234 (1892) (refusing to enforce provision in patent

licensing agreement whereby licensee agreed never to challenge the validity of the licensed patents, finding it "a serious question whether public policy permits a man to barter away beforehand his right to defend against unjust actions or classes of actions.").

The situation is no different in the area of copyright. In enacting the Copyright Act and the DMCA, Congress specifically limited the rights of the copyright owner under sections 106 and 106A of the Act and section 1201 of the DMCA by specifying the fair use rights of the copyright user in section 107 of the Act and section 1201(f) of the DMCA. It did so to strike a balance between providing incentives to copyright owners and protecting the public benefits of fair use. Plaintiffs seek, however, to disrupt this balance by taking away from the public certain fair use rights that Congress has determined must be preserved in order to benefit the public interest.[8] This is exactly what conflict preemption aims to prevent.[9]

---

[8] *Cf. Thomas James Assocs., Inc. v. Jameson*, 102 F.3d 60, 66-67 (2nd Cir. 1996) (waiver in employment agreement of right to arbitration held unenforceable in light of strong federal policy favoring arbitration of employment-related disputes).

[9] In support of its holding, the District Court cited to the Older Workers Benefit Protection Act, 29 U.S.C. §626(f) (2004) for the proposition that "[p]arties may waive their statutory rights under law in a contract." 334 F.Supp.2d at 1181. But in fact, that statute only undercut the District Court's holding, because in it Congress specifically endorsed and outlined a procedure that permits a party to

This Court's decision in *United Steelworkers of America AFL-CIO-CLC v. Johnson*, 799 F.2d 402 (8th Cir. 1986), is instructive. In *United Steelworkers*, a South Dakota statute prevented union members from receiving the same unemployment benefits during a labor strike as non-union members. While it was not expressly preempted by federal law, the statute did create a strong disincentive to union membership. As a result, this Court held that the statute was nonetheless conflict preempted because it stood as an obstacle to Congress's purposes and objectives in enacting the National Labor Relations Act ("NLRA"). As the Court reasoned, the NLRA reflected Congress's desire to create "a fine and even balance of the dynamic and conflicting interests of labor and management," *id*. at 408, and "[b]y altering the balance of power between labor and management, South Dakota has transgressed against Congress's concern to maintain the fine balance between labor and management." *Id.* at 409.[10] Similarly, Plaintiffs cannot use state law to

---

waive his statutory right to sue under the ADEA. Here, Congress has provided no such procedure for waiver, precisely because fair use rights are essential to fulfilling its constitutional mandate of promoting the progress of "science and the useful arts."

[10] *See also South Dakota Mining Assoc. v. Lawrence County*, 155 F.3d 1005, 1011 (8th Cir. 1998) (county ordinance conflict preempted by federal Mining Act because despite lack of express conflict, "[t]he ordinance's de facto ban on mining on federal land acts as a clear obstacle to the accomplishment of" federally encouraged mining activities); *Union Center*, 103 F.3d at 65 (condemnation of Amtrak property under state law was conflict preempted because such action

transgress against the delicate balance that Congress has created between the rights of copyright holders and the fair use rights of the public. If Plaintiffs' state law contractual scheme is permissible, then all software producers could employ similar restrictive provisions in their license agreements to their customers as well. The end result would be that no consumer would have any right to engage in the reverse engineering of any software product. Nor could a company reverse engineer a competitor's software for the purpose of developing a product that could interoperate with that software, resulting in much less competition in the market for such interoperable products.

Indeed, under the District Court's reasoning, all fair use rights protected by Congress, including fair use for the purposes of scholarship, criticism, or parody, could be prohibited through private contracts of adhesion or even outright bans by state legislatures. Movie studios could add language to the back of ticket stubs prohibiting newspaper or television critics from including any examples of dialogue in a critical review of the firm. Publishers could shrinkwrap their novels with a license banning any high school English teacher or college professor from quoting the novel during a lecture. Clearly, Congress did not intend that the fair

---

would "frustrat[e] Amtrak's ability to accomplish its federal mandate of creating a nationwide rail system").

use rights that it worked so hard to protect in the Copyright Act and the DMCA could be so easily and completely vitiated through state law. Because Plaintiffs' prohibition on all fair use, including fair use by reverse engineering, is a clear obstacle to the accomplishment of Congress's objective of protecting and encouraging fair use activities, Plaintiffs' state law claim must be conflict preempted.

III. PLAINTIFFS' CLAIMS NEITHER OVERCOME THE EXEMPTION FROM LIABILITY FOR REVERSE ENGINEERING NOR PRESENT A *PRIMA FACIE* CASE UNDER THE DIGITAL MILLENNIUM COPYRIGHT ACT

Congress and the courts have shielded fair use of computer programs by reverse engineering for interoperability to assure that the public may access those aspects of programs that are not entitled to copyright protection. "With respect to computer programs, fair use doctrine preserves public access to the ideas and functional elements embedded in copyrighted computer software programs." *Lexmark,* 387 F.3d at 537 (quoting *Sony,* 203 F.3d at 603). This shield extends beyond liability for copyright infringement under section 106 of the Copyright Act to include immunization from liability for circumvention and trafficking under section 1201(a) of the DMCA. *See Chamberlain*, 381 F.3d at 1200 (noting "the explicit immunization of interoperability from anticircumvention liability under §1201(f)").

A defendant "who has lawfully obtained the right to use a copy of a computer program" is not liable if he circumvented the technological measure "for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs." 17 U.S.C. §1201(f). Nor can a defendant be held liable for trafficking software programs or tools that circumvent for the purposes of reverse engineering or interoperability. *Id.*

A. The District Court failed as a matter of law to correctly apply the statutory "reverse engineering for interoperability" defense of 17 U.S.C. §1201(f)

1. Congress explicitly exempted reverse engineering for interoperability from liability under the DMCA

As noted above, courts have long recognized that the public has a right under the fair use doctrine to access the inner workings and ideas behind software and other copyrighted works. *See Eldred,* 537 U.S. at 219 (copyright law contains built-in First Amendment accommodations, such as "fair use", to allow the public to use not only facts and ideas, but also the expression itself in certain circumstances); *Mazer v. Stein*, 347 U.S. 201, 219 (1954); *Baker v. Selden*, 101 U.S. 99, 101-102 (1879). This includes the right to reverse engineer copyrighted software and from that process create compatible software that can interact with the original product. *See Sony*, 203 F.3d at 602; *Sega*, 977 F.2d at 1527-28; *Atari,*

975 F.2d at 843; *see also Lexmark,* 387 F.3d at 537 ("With respect to computer programs, 'fair use doctrine preserves public access to ideas and functional elements embedded in copyrighted computer software programs.'") (citing *Sony*, 203 F.3d at 603).

In enacting the DMCA, Congress recognized this balance between copyright protection and access to ideas and interoperability. To preserve this access, Congress incorporated 17 U.S.C. §1201(f), explicitly immunizing interoperable programs from anti-circumvention liability under the DMCA. Under section 1201(f), a person may circumvent an access control measure "for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to [that person]." 17 U.S.C. §1201(f)(1). A person may also "develop and employ technological means" that are "necessary" to enable interoperability. 17 U.S.C. §1201(f)(2). And these means may be made available to others "solely for the purpose of enabling interoperability of an independently created computer program with other programs." 17 U.S.C. §1201(f)(3). All three defenses apply only when such actions do not otherwise constitute copyright infringement. *Id.*

The legislative history of section 1201(f) makes it crystal clear that these

immunities exist to protect legitimate attempts to make one program work with another, even if that means the first program must circumvent an access control to the other program in order to do so. *See* S. Rep. No. 105-190, at 13; *see also Chamberlain,* 381 F.3d at 1202 ("The statutory structure and the legislative history [of section 1201] both make it clear that the DMCA granted copyright holders additional legal protections, but neither rescinded the basic bargain granting the public non-infringing and fair uses of copyrighted materials, §1201(c), nor prohibited various beneficial uses of circumvention technology, such as those exempted under §§1201(d),(f),(g),(j)."). Thus, actions and devices that qualify for fair use reverse engineering under section 1201(f) cannot violate the DMCA.

2. Defendants Qualify Under Every Prong of the Test for Section 1201(f)

Under the requirements set forth in section 1201(f), Defendants must establish that:

1) Defendants lawfully obtained the right to use a copy of the computer program they circumvented;

2) The information needed for interoperability must have been previously unavailable;

3) The sole purpose of any circumvention or distribution of a circumvention tool must have been to achieve interoperability of an independently created computer program with other programs; and

4) No alleged act of circumvention or distribution of a circumvention tool constituted copyright infringement.

17 U.S.C. §1201(f).

Regarding the first two prongs, the District Court found both that Defendants had "lawfully obtained the right to use a copy of the [Plaintiffs'] computer programs," 334 F.Supp.2d at 1185, and that Plaintiffs had not previously disclosed to the public the methods used in Battle.net mode's secret handshake. *Id.* at 1173.

The District Court then considered the third "sole purpose" prong. Without reference to any language in the statute, any legislative history, or any applicable case law, it held that an accused program satisfying this prong may neither interoperate with unauthorized copies of Plaintiffs' games (*i.e.*, games that do not have a valid or unique CD key) nor be distributed by Defendants for free so that others could copy and use the program. *Id.* at 1185. The District Court further held that a program could not meet the "sole purpose" prong if it was intended as a "functional alternative" to a program offered by Plaintiffs because it would no longer be "independently created." *Id.* None of these limitations, however, are part of the "sole purpose" prong under section 1201(f).

Regarding the fourth prong, the District Court held, without explanation or citation, that "defendants' actions extended into the realm of copyright

infringement." *Id.* But there is no evidence in the record below that any of the allegedly circumventing code infringes any of Plaintiffs' copyrights. The only *allegations* of copyright infringement in the record concern a few small, unrelated icon files that were distributed with the bnetd server in order to help player recognize others when they "chatted" on the system.[11] Those separate claims were dismissed with prejudice pursuant to a consent judgment that is not at issue in this appeal. DER349. In any event, as explained further below, they have nothing to do with accessing Battle.net mode or any alleged circumvention under the DMCA.

(a) The District Court Ignored Its Own Factual Findings and Imported Improper Limitations into the "Sole Purpose" Requirement

Regarding the third prong of the *prima facie* case for liability under section 1201(a)(1) or (a)(2), the District Court ignored its own factual findings and imported limitations not found anywhere in the plain language of the statute.

(i) The District Court failed to recognize that bnetd's access to Battle.net Mode was for the sole purpose of interoperability

The District Court held that the sole purpose of Defendants' bnetd server was not interoperability because bnetd "always allows the Blizzard game to access

[11] Before Plaintiffs' copyright claims were dismissed with prejudice, Defendants raised substantial fair use and *de minimis* use defenses to these claims. DER137-43.

Battle.net mode features even if the user does not have a valid or unique CD key" and that as a result "[u]nauthorized copies of the Blizzard games were played on bnetd servers." 334 F.Supp.2d at 1185. [12]

This conclusion, however, does not address the purpose of the access — as the statute requires — but rather the result. It also ignores the District Court's own factual findings. First, the District Court found that because Plaintiffs had not previously disclosed its CD Key checking method, "there is no way that defendants could have implemented a check for CD Key validity in the bnetd program." *Id.* at 1173. Second, the District Court specifically found that in order for the bnetd server to interoperate with Plaintiffs' games, it always *had* to access Battle.net mode. *Id.* ("The bnetd server computer code always sends the game an "okay" reply regardless of whether the CD key is valid or currently in use by another player, as the *game will otherwise not allow access to Battle.net mode*.") (emphasis added); DER183. Thus, according to the District Court's own factual findings, there was no way for the bnetd server to check CD Keys and no way for the bnetd server to interoperate with the Plaintiffs' videogames in Battle.net mode other than

[12] The District Court divided its section 1201(f) analysis between its discussions of "access" under section 1201(a)(1) and "trafficking" under section 1201(a)(2); however, because its reasons for denying application of the defense were identical for both sections, Defendants will discuss them together.

to allow the game to access Battle.net mode by issuing an "okay" reply every time the game sent a CD Key to the server. Because Plaintiffs chose not to disclose their CD Key checking mechanism, the bnetd server's failure to check CD keys was a necessary side effect of achieving interoperability, not an alternative purpose for circumvention. There was no other way to do it.

There is also no evidence in the record to suggest any connection between any allegedly illegal third-party conduct and Defendants' purpose. As the District Court itself found, "Defendants never advised people to play pirated copies of Plaintiffs' games using the bnetd server." *Id.* at 1173. Under the express terms of section 1201(f), the fact that unknown, unidentified third parties may have played pirated games using bnetd servers at some point in time has no bearing on Defendants' sole purpose, and cannot prejudice the case against them without evidence that Defendants themselves had the purpose to create such a result.[13]

---

[13] Again, the substantial case law on interoperability is instructive. In *Sega, Sony, Lexmark, and Chamberlain*, the potential for "unauthorized" use of games, consoles, cartridges, and garage door opener remotes was well known to the parties and the courts; yet this did not prevent the Ninth, Sixth, and Federal Circuits from finding in favor of the defendants in those cases because there was no evidence that such unauthorized use was encouraged or intended by defendants.

Absent any evidence in the record that Defendants' purposes included encouraging the piracy of Plaintiffs' games, the District Court's ruling effectively mandates that Defendants include a mechanism for preventing the bnetd server from interoperating with unauthorized copies of Plaintiffs' games. Congress, however,

(ii) No connection exists between Defendants' sole purpose for circumvention and the fact that they later distributed the bnetd server for free over the internet

The District Court also concluded that Defendants did not have a sole purpose of achieving interoperability because, after designing the bnetd server to interoperate with Plaintiffs' games, they distributed bnetd for free over the Internet and therefore had "limited commercial purpose." Again, there is no rational connection between the "sole purpose" test under section 1201(f) and the District Court's conclusions. First, sections 1201(f)(2) and (3) explicitly permit the distribution of circumvention tools for the purpose of enabling interoperability. This is exactly what distribution of the bnetd server enabled. Second, every defendant in each of the seminal interoperability cases – including the *Sega* case explicitly noted by the Senate when it passed section 1201(f) – released their product to the public in order to allow consumer interoperability with the plaintiff's product. *See Sega,* 977 F.2d at 1514; *Sony,*203 F.3d at 599; *Atari,* 975 F.2d at 836-37; *Chamberlain,* 381 F.3d at 1183; *Lexmark*, 387 F.3d at 530; *accord* S. Rep. No. 105-190, at 13 (section 1201(f) meant to preserve settle law). Indeed, there would be little purpose in learning how to make a compatible product if one were unable to subsequently create and distribute it.

---

has specifically rejected any such mandate. *See* 17 U.S.C. §1201(c)(3).

(iii) There is no evidence that the bnetd server is anything but an independently created computer program

The District Court further concluded that Defendants did not create an independently created computer program because the bnetd program "was intended as a functional alternative to the Battle.net service." 334 F.Supp.2d at 1185. This conclusion also has no basis in either section 1201(f) or any relevant case law. As noted above, the legislative history of section 1201(f) specifically meant to preserve settled case law regarding interoperable software. In *Sony*, the seminal Ninth Circuit case, the defendant had produced a Virtual Game Machine (VGM) emulator that, similar to the bnetd server, was intended to be a functional alternative to Sony's Playstation game console. *Sony*, 203 F.3d at 599. The Ninth Circuit found that the VGM emulator qualified as an interoperable computer program under the *Sega* fair use doctrine because there was no evidence that it was made with any infringing code and was therefore an independently created computer program. *Id.* at 606-07. The same is true in the other interoperability cases. *See Lexmark,* 387 F.3d at 530 (SCC ink cartridges were a functional alternative to Lexmark's cartridges); *Chamberlain*, 381 F.3d at 1184-85 (noting that Skylink's remote was a functional alternative to Chamberlain's remote). There is simply no basis for the District Court's conclusion that Congress excluded

such functional alternatives from the exemption under this section when the statute and case law provide exactly the opposite.

(b) The District Court Concluded That Copyright Infringement Existed with Any Analysis or Evidence in Support

Finally, inexplicably, the District Court addressed the fourth prong of the section 1201(f) exemption and concluded that "[b]ased on these facts, defendants' actions extended into the realm of copyright infringement and they cannot assert the defenses under §1201(f)(1)." 334 F. Supp.2d at 1185. Once again this conclusion does not have any basis in fact or law. There are no findings in the record to show that any part of the bnetd server code for accessing Battle.net infringes any copyright assigned to Plaintiffs. Nor is there even an explanation from the District Court as to what alleged works were copied, how they are copied, whether they are substantially similar,[14] or whether a fair use or *de minimis* use defense would apply.[15] There is only the naked assertion that somewhere, somehow, infringement exists.

The only allegations of copyright infringement in the record concern a few

---

[14] This Court has repeated required a finding of substantial similarity as a predicate to finding copyright infringement. *See, e.g., Taylor Corp. v. Four Seasons Greetings, LLC,* 315 F.3d 1039, 1043 (8th Cir.2003); *See also* 4 *Nimmer on Copyright*, §13.03[A].

[15] *See* 4 *Nimmer on Copyright*, §13.03[F][5] at 13-145.

small, unrelated icon files that were distributed with the bnetd server in order to help player recognize others when they "chatted" on the system. DER331-38. They have nothing to do with accessing Battle.net mode or any alleged circumvention under the DMCA. And in any event, these claims were dismissed with prejudice. DER349. Furthermore, Defendants had raised substantial fair use and *de minimis* use defenses to these claims. DER137-43.

B. Plaintiffs failed to prove a prima facie case under the DMCA

Even if Defendants were not entitled to the statutory exemption for reverse engineering under section 1201(f), Plaintiffs failed to establish a *prima facie* case of either circumvention under section 1201(a)(1) or trafficking under section 1201(a)(2).

To prove either circumvention under section 1201(a)(1) of the DMCA or trafficking in circumvention technologies under section 1201(a)(2), a plaintiff must establish *prima facie* that the defendant's actions or devices circumvent a "technological measure that effectively controls access to a [copyrighted] work." 17 U.S.C. §1201(a)(1) and (a)(2). The District Court recognized this. 334 F.Supp.2d at 1183. But it then held that Defendants circumvented Plaintiffs' technological measure without addressing at all the Plaintiffs' failure to demonstrate that the technology alleged circumvented either (1) protects something

copyrightable and (2) effectively controls access to something that is otherwise unavailable to the user. *Id.* at 1183-85. The plain language of both section 1201(a)(1) and (a)(2) clearly requires a plaintiff to establish these facts.

In its complaint, Plaintiffs' sole DMCA allegation is that when game users activate the functionality of the Battle.net mode within their videogames by using a bnetd server instead of Blizzard's Battle.net service, they are "accessing" their game's Battle.net mode without DMCA authorization and therefore circumventing Blizzard's anti-piracy protections. DER64-65. Moreover, the District Court specifically found that the only work protected by the Battle.net service was Battle.net mode. 334 F.Supp.2d at 1169. But Battle.net mode cannot be protected under this theory for two reasons: (1) Battle.net mode is a process and therefore not copyrightable and (2) access to Battle.net mode is not "effectively controlled."

1. Battle.net mode is not a work protected by copyright law

Copyright law only protects copyrightable expression, such as images on a screen or words on a page. It does not protect how things work or the way they work. This limitation is strictly built into the Copyright Act in section 102(b):

> In no case does copyright protection for an original work of authorship extend to any idea, *procedure*, *process*, *system*, *method of operation*, concept, principle, or discovery, regardless of the form in which it is described, explained, illustrated, or embodied in such a work.

17 U.S.C. §102(b) (emphasis added). This provision embodies longstanding common-law principles that distinguish the spheres of copyright and patent law, often called the idea-expression dichotomy,[16] the merger doctrine,[17] and the doctrine of scene a faire.[18] As part of the Copyright Act, the DMCA's section 1201 likewise only protects *copyrighted* works. *See* 17 U.S.C. §§1201(a)(1)(A) (protecting only access controls for copyrighted work), 1201(a)(2)(A) (same).[19]

By its very definition, "Battle.net *mode*" is a procedure, process, system, and/or method of operation.[20] The evidence is undisputed on this point, and one need only consult the District Court's order for such evidence. *See* 334 F.Supp.2d at 1168 (noting that Battle.net mode allows users to create and join multi-player games, to chat with other potential players, to record wins and loses and save advancements in a password protected account, to participate with others in

---

[16] *Mazer v. Stein*, 347 U.S. 201, 217 (1954); *See also* 4 *Nimmer on Copyright*,§13.03[B[2][a].

[17] *Schoolhouse, Inc. v. Anderson***,** 275 F.3d 726, 730 (8th Cir. 2002); 4 *Nimmer on Copyright*, §13.03[B][3].

[18] *Taylor*, 315 F.3d at 1042; *Ets-Hokin v. Skyy Spirits, Inc.*, 225 F.3d 1068, 1081 (9th Cir. 2000). *See also* 4 *Nimmer on Copyright*, §13.03[B][4].

[19] *See also Chamberlain*, 381 F.3d at 1194 ("What the DMCA did was introduce new grounds for liability in the context of the unauthorized access of *copyrighted material*.").

[20] The American Heritage Dictionary of the English Language, Fourth Edition (2000), defines a "mode" as a manner, way or *method* of doing or acting." (emphasis added).

tournament play featuring elimination rounds, and to set up private chat "channels" and private games); *id.* ("These Battle.net mode features are accessed from within the games themselves."); *id.* at 1168-69 ("The features and functions of Battle.net mode, however, cannot be accessed when players are connected through [local area networks or direct computer connections].").

Battle.net mode is not creative expression that you can see or hear or touch like a book, a song, or a movie. Rather, it merely functions mechanically as a process within the computer to allow Blizzard gamers to play each other over the Internet via a server. As such, it cannot be protected under federal copyright law. *See Lotus Dev.*, 49 F.3d at 816 ("If specific [works] are essential to operating something, then they are part of a "method of operation' and, as such, are unprotectable.").

The Sixth Circuit's recent decision in *Lexmark Int'l. v. Static Control Components* is particularly instructive on this issue. In that case, Lexmark had attempted to protect use of its computer printers by building a "secret handshake" into its ink cartridges so that only official Lexmark cartridges would work on Lexmark printers. The handshake method was almost identical to the one in this case. Every time a user wanted to run a Lexmark printer, the printer would check the ink cartridge to make sure it was a cartridge made by Lexmark. If not, the

printer's engine program would not run and the user could not print. *See Lexmark,* 387 F.3d at 530.

Defendant Static Control Corp. ("SCC") decided to make a competing ink cartridge so that consumers of Lexmark printers would have more options in the marketplace for ink. But in order to do this, it needed to make its cartridges compatible with Lexmark printers. Because SCC knew the Lexmark printer would check the SCC cartridge for a "handshake," SCC designed its cartridges to respond to Lexmark printers with handshake identical to that of the Lexmark cartridge. *Id.* at 530-31. Lexmark, much like Plaintiffs, objected to anyone offering an alternative to its own product and sued SCC under the DMCA. *See id.* at 531. The District Court, much like the court below here, ruled in favor of the plaintiff, finding that any use of plaintiff's products without its permission was unlawful. *See id.*

On appeal, however, the Sixth Circuit reversed. It found that the "secret handshake" between printers and cartridges, however cleverly designed to protect Lexmark's business model, was not protected expression under the DMCA because it was an uncopyrightable "lock-out code" that was purely functional in nature and to which a competitor would need access in order to offer competing ink cartridges:

> Generally speaking, "lock-out" codes fall on the functional-idea rather than the original-expression side of the copyright line. Manufacturers of interoperable devices such as computers and software, game consoles and videogames, printers and toner cartridges, or automobiles and replacement parts may employ a security system to bar the use of unauthorized components. To "unlock" and permit operation of the primary device (i.e. the computer, the game console, the printer, the car), the component must contain therein a certain code sequence or be able to respond appropriately to an authentication process. To the extent compatibility requires that a particular code sequence be included in the component device to permit its use, the merger and scene a faire doctrines generally preclude the code sequence from obtaining copyright protection.

Id. at 536.[21]

In his *Lexmark* concurrence, Judge Merritt explained why allowing access to lock-out codes was not only proper for copyright law but also for fair competition in the marketplace:

> If we were to adopt [Plaintiff]'s reading of the [DMCA], manufacturers could potentially create monopolies for replacement parts simply by using similar, but more creative, lock-out codes. Automobile manufacturers, for example, could control the entire market of replacement parts for their vehicles by including lock-out chips. Congress did not intent to allow the DMCA to be used offensively in this manner, but rather solely to reach those who circumvented protection measures "for the purpose" of pirating works protected by the copyright statute.

Id. at 552 (Merritt, J., concurring).

Here, there is no dispute that the bnetd server only accesses Battle.net mode

[21] *See also Sega*, 977 F.2d at 1524 ("To the extent that a work is functional or factual, it may be copied.").

in order to "unlock" Plaintiffs' videogame for compatibility reasons. 334 F.Supp.2d at 1173. There is no evidence in the record that bnetd was designed for the purpose of pirating works. In fact, the District Court held that "Defendants never advised people to play pirated copies of Blizzard games using the bnetd server." *Id*. Thus, just like the lock-out code in *Lexmark*, any code accessed in "Battle.net mode" by the bnetd server cannot be protected under either traditional copyright law or the DMCA. *See also Sega*, 977 F.2d at 1524 n.7; S. Rep. No. 105-190, at 13 (DMCA intended to preserve *Sega*).

2. Plaintiffs do not "effectively control" access to Battle.net mode

In addition to Battle.net mode being functional and thus unprotectable, the fact that Battle.net mode is freely accessible to users without circumvention also makes it unprotectable under the DMCA. Again, in *Lexmark*, the Sixth Circuit found that while the ink cartridges' "secret handshake" was, in fact, one way to "block" access to the printer engine program, it did not block another relevant form of "access" — the ability to obtain a copy of the literal elements of the printer program (its code) by directly copying it from the printer's memory. *Lexmark*, 387 F.3d at 546-47. Because the DMCA ubiquitously refers to technological measures "control[ling] access to a work protected under this title," the Sixth Circuit held that it did not naturally apply when the "work protected under this title" is

otherwise accessible. *Id.* at 547.

The *Lexmark* court found that anyone who buys a Lexmark printer may read the literal code of the Printer Engine Program (the allegedly protected work) directly from the printer memory, with or without the benefit of the "handshake," and that the data from the program may be translated into readable source code after which copies may be freely distributed: "No security device, in other words, protects access to the [Printer Engine Program] Code and no security device accordingly must be circumvented to obtain access to that program code." *Id.* The Court went on to discuss how such an approach comported with common sense:

> Just as one would not say that a lock on the back door of a house "controls access" to a house whose front door does not contain a lock and just as one would not say that a lock on a door of a house "controls access" to the house after its purchaser receives the key to the lock, it does not make sense to say that this provision of the DMCA applies to otherwise-readily accessible copyrighted works.

Id.

This reading of the DMCA is also supported by its legislative history. For example, the Senate Report states:

> Paragraph (a)(3) defines certain terms used throughout paragraph (a). Subparagraph (1) defines the term "circumvent a technological protection measure" as meaning "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner. This definition applied to paragraph (a) only, which covers protections against unauthorized *initial* access to a copyrighted work.

S. Rep. No. 105-190, at 29 (emphasis added). Likewise, the House Judiciary Committee Report states:

> Paragraph (a)(1) does not apply to the *subsequent actions* of a person once he or she has obtained authorized access to a copy of a work protected under Title 17, even if such actions involve circumvention of additional forms of technological protection measures. In a fact situation where access is authorized, the traditional defenses to copyright infringement, including fair use, would be fully applicable. So, an individual would not be able to circumvent in order to gain unauthorized access to a work, but would be able to do so in order to make fair use of a work which he or she has acquired lawfully.

H.R. Rep. No. 105-551, pt. 1 at 18. Even *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 (2nd Cir. 2001), the primary case relied upon below by Plaintiffs, DER230, supports this reading: "the DMCA targets *the circumvention of digital walls* guarding copyrighted material (and trafficking in circumvention tools), but does not concern itself with the *use* of those materials." (emphasis in original). In other words, the DMCA only protects content that is otherwise unavailable to a consumer. Content to which consumers otherwise have access is not "effectively controlled" by a technological protection measure and therefore cannot be the basis for circumvention or trafficking liability.

Here, every consumer who purchases a Blizzard game has full access to the literal code of Battle.net mode and all of its associated programs because they come available on the CD-ROM the consumer has purchased. She can, among

other methods, simply read the literal code off of the CD-ROM on which it came or off her computer once the game is installed without having to employ any "secret handshake." Just as in *Lexmark*, no security device protects access to the Battle.net mode code in these ways and no security device accordingly must be circumvented to obtain access to that program code. Thus, as the *Lexmark* court found, accessing such code is not a DMCA violation.

CONCLUSION

Recently, in *In re Charter Communications*, this Court affirmed that "it is the province of Congress, not the courts, to decide whether to rewrite the DMCA 'in order to make it fit a new and unforeseen internet architecture' and 'accommodate fully the varied permutations of competing interests that are inevitably implicated by such new technology." No. 03-3802, 2005 WL 15416, at *5 (8th Cir. Jan. 5, 2005) (quoting *Recording Indus. Ass'n of Am. v. Verizon Internet Servs.*, 351 F.3d 1229, 1238 (D.C. Cir. 2003)). Here, the District Court's order granting Plaintiffs' motion for partial summary judgment and denying Defendants' summary judgment motion not only rewrites the DMCA to fit the unforeseen architecture of the bnetd server, but also rewrites the Supremacy Clause of the Constitution by undermining the explicit decisions that Congress has already

///

///

made in this field to preserve fair use of copyrighted material. The order should be reversed, and summary judgment should be entered in favor of Defendants.

Dated: January 13, 2005

Respectfully submitted,

By: _____

Robert M. Galvin, *pro hac vice*
Paul S. Grewal, *pro hac vice*
Richard C. Lin, *pro hac vice*
DAY CASEBEER MADRID & BATCHELDER LLP
20300 Stevens Creek Boulevard, Suite 400
Cupertino, CA 95014
(408) 873-0110

Jason M. Schultz, *pro hac vice*
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
(415) 436-9333

Mark Sableman (4244)
Matthew Braunel (109915)
THOMPSON COBURN LLP
One US Bank Plaza
St. Louis, MO 63101-1611
(314) 552-6000

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of OPENING BRIEF OF DEFENDANTS-APPELLANTS INTERNET GATEWAY, INC., TIM JUNG, ROSS COMBS and ROB CRITTENDEN and DEFENDANT-APPELLANTS' APPENDIX AND EXCERPTS OF RECORD, was duly served upon counsel for Plaintiffs-Appellees Davidson & Associates, Inc., D.B.A. Blizzard Entertainment, and Vivendi Universal Games, Inc. by forwarding two copies of the Brief, one copy of the Appendix, and a 3.5" floppy diskette containing a .pdf version of the Brief via overnight courier addressed to:

Stephen H. Rovak / Kirill Y. Abramov
Sonnenschein Nath & Rosenthal LLP
One Metropolitan Square, Suite 3000
St. Louis , Missouri 63102

Additionally, the original and ten copies also have been sent via overnight courier for next business day delivery to:

Clerk of the Court
U.S. Court of Appeals Clerk's Office
For the Eighth Circuit
Thomas F. Eagleton Courthouse
Room 24.329
111 South 10th Street
St. Louis, MO 63102

this 12th day of January 2005.

By:_____
Paul S. Grewal

CERTIFICATE OF COMPLIANCE

The undersigned hereby certifies that this brief complies with Fed. R. App. P. 32(a)(7)(B). It contains 13,980 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); has been prepared in proportionally spaced typeface using Microsoft Word 2002 in 14 pt. Times New Roman font; and includes a virus free 3.5" floppy disk in .pdf format.

Dated: January 12, 2005

_____
Paul S. Grewal