Super Mario, Esq. to the Rescue: The Growing Legal Fight Over Cheating and Hacking in Online Video Game Play

Jonathan H. Blavin

Jonathan H. Blavin is a partner in the San Francisco office of Munger, Tolles & Olson. His practice focuses on high-tech intellectual property disputes, including those involving online and social games, and Internet and privacy-related litigation. He is on the board of the San Francisco Intellectual Property Law Association and is a member of the executive committee of the Intellectual Property Section of the Bar Association of San Francisco. He has served as Chair of the Intellectual Property and Internet Law Section of the Barristers Club of the Bar Association of San Francisco. He is a graduate of the University of Michigan and Harvard Law School.

INTRODUCTION

The video game industry is one of the fastest growing sectors of the U.S. economy. See http://www.theesa.com/facts/econdata.asp. From 2005 to 2009, the entertainment software industry's annual growth rate exceeded 10 percent, while the entire U.S. economy grew at a rate of less than 2 percent. Consumers spent $20.77 billion on video games, hardware, and accessories in 2012. http://www.theesa.com/facts/. And it is estimated that 58 percent of Americans play video games. http://www.theesa.com/facts/econdata.asp.

One of the newest and most lucrative forms of video game play is online gaming. Online purchases of digital content, including mobile apps, subscriptions, and social networking games, accounted for 40 percent of video game sales in 2012. See http://www.theesa.com/facts/. Unlike earlier generations of disconnected video game users, players today widely log onto online interconnected gaming platforms. Indeed, approximately 48 million players are now on Microsoft's Xbox LIVE online gaming network. http://www.xbox.com/en-US/live.

A pervasive threat to the online gaming economy, however, is cheating and hacking in video game play. This conduct includes users gaining unfair advantages in online game play against other players, *e.g.*, seeing through walls, having more powerful weapons, flying, or using automated "bots" (short for robots) to advance to higher levels of a game without human involvement. It also includes users obtaining stolen contents or points in game play, *e.g.*, unearned game assets and other virtual content. A common form of cheating involves the use of automated bots to gather valuable materials in an online game, which are then resold on sites like eBay. Players who feel that others have obtained unearned advantages in game play will no longer play certain online games, will cancel their existing subscription service to online games (*e.g.*, Xbox LIVE), or will stop earning or purchasing virtual assets in games when others have obtained them for free or through other unauthorized means. Indeed, following the widespread security breach of the Sony PlayStation Network in 2010 and 2011, cheating and hacking became rampant in online PlayStation games. One disgruntled user noted, "When I pay $60 for a game I expect it to work for more than a year and a half. I popped in MW2 [Modern Warfare 2] just now and it is rampant with cheating. Hackers aren't even trying to hide it. . . . The game is effectively unplayable." http://community.us.playstation.com/t5/Shooter-General/COD-MW2-Hacking-Cheating/td-p/30870984?start=0&tstart=0.

As video game expert Scott Steinberg has observed, through cheating and hacking "[i]t's entirely possible to break not only the in-game economy, but the actual economics around the game." See http://techland.time.com/2013/05/24/cheating-in-online-video-games/. It is estimated that this kind of conduct has cost the video game industry millions of dollars, not to mention vast amounts of time and money that game developers spend to police their game servers and to identify and ban cheaters. Polic-

ing efforts often present a whack-a-mole problem as gamers regularly change their online identities.

Some game developers have resorted to legal action to stem the tide of cheating and hacking on their networks. Although legal actions against individual cheaters or hackers are rarely economically sensible given the whack-a-mole problem, in some circumstances, it may make sense to initiate legal action against third parties who sell devices that broadly enable cheating and hacking in game play.

A common form of cheating involves the use of automated bots to gather valuable materials in an online game, which are then resold on sites like eBay.

This article provides an overview of the various legal claims a game developer may have against such third parties, including claims under the Copyright Act (17 USC §§101–1332), the anti-circumvention provisions (17 USC §1201) of the Digital Millennium Copyright Act (DMCA) (Pub L 105–304, 112 Stat 2860) (including the evolving interplay between the DMCA and antitrust law), contract law, and the Computer Fraud and Abuse Act (CFAA) (18 USC §1030). This article also notes the risks of bringing such claims without sufficient factual or legal support at the outset of an action, including the potential denial of an early motion for preliminary injunctive relief.

POTENTIAL LEGAL CLAIMS AGAINST THIRD PARTIES DISTRIBUTING CHEATING AND HACKING DEVICES

Copyright

Game developers have had mixed results in using copyright law to protect against the hacking or cheating of video games. One of the first legal challenges to an early video game hacking device was in *Lewis Galoob Toys, Inc. v Nintendo of Am., Inc.* (9th Cir 1992) 964 F2d 965. In this instance, Nintendo's attempt to use copyright law to halt the sale of the device was unsuccessful.

Galoob, the declaratory relief plaintiff, manufactured the Game Genie, a device that allowed players of the original Nintendo Entertainment System (NES) to alter several features in a game, including increasing the number of lives of the player's character, increasing the speed at which the character moves, and allowing the character to float above obstacles. 964 F2d at 967. The Game Genie was inserted between the game cartridge and the NES; it did not alter the data stored on the cartridge and its effects were temporary. Below is an image of the Game Genie:

Because this was the pre-Internet era of online gaming, the cheating that players engaged in with the Game Genie did not harm other players or an interconnected universe of online play; in effect, the players were only cheating the machine.

The Ninth Circuit held that Galoob was not secondarily liable for allowing consumers to create derivative works infringing Nintendo's copyrights in its games because "[a] derivative work must incorporate a protected work in some concrete or permanent form." 964 F2d at 967 (internal quotation marks omitted). The audiovisual displays generated by combining the NES with the Game Genie were not incorporated in any permanent form; when the game was over, they were gone. Thus, the Game Genie did not infringe any of Nintendo's copyrights.

The game developer had more success in *Micro Star v FormGen Inc*. (9th Cir 1998) 154 F3d 1107. There, in another declaratory relief action, the game developer defendant sold a game called Duke Nukem 3d, in which players explored a futuristic city infested with evil aliens and other hazards, while searching for the hidden passage to the next level. 154 F3d at 1109. Although the basic game came with 29 levels, the game also included a "Build Editor" that enabled players to create their own levels. Micro Star, a computer software distributor, downloaded 300 user-created levels from the Internet, stamped them onto a CD, and sold them commercially. FormGen claimed that these distributed user levels directly infringed its copyrights in the Duke Nukem game.

The Ninth Circuit found the user levels to be infringing derivative works. The court noted that, unlike the audiovisual displays created by the Game

Genie, which were never recorded in any permanent form, the level files described in exact detail the audio-visual displays in the Duke Nukem game. 154 F3d at 1111. Thus, "[b]ecause the audiovisual displays assume a concrete or permanent form in the [level] files," *Galoob* was "no bar to finding that they are derivative works." 154 F3d at 1112. The Ninth Circuit further held that the works were not protectable as fair use. 154 F3d at 1113. Finally, the court rejected Micro Star's argument that FormGen abandoned its rights by encouraging players to create new levels, noting that "FormGen never overtly abandoned its rights to profit commercially from new levels" and that it "warned players not to distribute the levels commercially and has actively enforced that limitation by bringing suits such as this one." 154 F3d at 1114.

[C]heating and hacking . . . has cost the video game industry millions of dollars, not to mention vast amounts of time and money that game developers spend to police their game servers and to identify and ban cheaters.

A more modern case, involving true online game play, is *MDY Indus., LLC v Blizzard Entertainment, Inc.* (9th Cir 2010) 629 F3d 928, which concerned Blizzard's World of Warcraft game, a "massively multiplayer online role-playing game" (629 F3d at 935) in which players interact in a virtual world. The game has tens of millions of subscribers. Players install game software on the machines and access the game server software on a subscription basis by connecting to the game's servers; there are no offline or single-player options. MDY, the declaratory relief plaintiff, developed "Glider," a software bot that automates play of WoW's early levels. To quote Glider's marketing materials, Glider "kills for you, automatically. You can do something else, like eat dinner or go to a movie, and when you return, you'll have a lot more experience and loot." 629 F3d at 935. Blizzard argued that Glider disrupted the game's environment for non-Glider players by enabling Glider users to advance quickly and unfairly through the game and to amass additional game assets. 629 F3d at 935. Following the release of Glider, Blizzard launched Warden, a technology that it developed to prevent its players who use unauthorized third party software, including bots, from connecting to the game's servers. Warden was able to detect Glider, and Blizzard immediately used Warden to ban most Glider users. 629 F3d at 936. MDY responded by modifying Glider to avoid detection, and added a subscription service, Glider Elite, which offered "additional protection from game detection software" for $5 a month. 629 F3d at 936.

Blizzard argued that MDY was liable for secondary copyright infringement, because end users had created copies of the game in random access memory (RAM) on their computers, and did so in violation of the Blizzard's End User License Agreement, which prohibited the use of bots such as Glider. The Ninth Circuit reversed the grant of summary judgment to Blizzard on the copyright infringement claim, holding that Blizzard had not established secondary infringement because there was not a sufficient nexus between the contractual condition not to use bots and Blizzard's exclusive rights of copyright. 629 F3d at 941. Thus, the court concluded, World of Warcraft "players do not commit copyright infringement by using Glider in violation of the ToU [terms of use]. MDY is thus not liable for secondary copyright infringement, which requires the existence of direct copyright infringement." 629 F3d at 941.

DMCA

The DMCA may be a sturdier foundation for legal challenges against distributors of cheating and hacking devices. In the *MDY* case, for example, although Blizzard's copyright claim was rejected by the Ninth Circuit, Blizzard fared better with its DMCA claim. The DMCA bars trafficking in "any technology, product, service, device, component, or part thereof that is primarily designed or produced for the purpose of circumventing" technological protection measures that protect against unauthorized access to copyrighted content. 17 USC §1201(a)(2). Blizzard claimed that MDY violated the DMCA's prohibition on trafficking in technology that circumvents a technological measure, *i.e.*, "Warden," that "effectively controls access" to a copyrighted work. 17 USC §1201(a)(2). The Ninth Circuit affirmed judgment in Blizzard's favor on the claim.

The Ninth Circuit noted that although Warden did not effectively control against unauthorized access to the "literal" elements of the game (*i.e.*, the actual software code) or the individual "non-literal" ele-

ments of the game (*e.g.*, the roars of a particular monster or a virtual image of that monster, which could be called up by a user at any given time), it did control against unauthorized access to the "dynamic nonliteral" game elements, *i.e.*, the "real-time experience of traveling through different worlds, hearing their sounds, viewing their structures, encountering their inhabitants and monsters, and encountering other players," which are subject to copyright protection 629 F3d at 943, 952. Because Glider circumvented Warden, which protected against unauthorized access to copyrighted content, MDY's trafficking in Glider therefore violated §1201(a)(2). In so holding, the Ninth Circuit also expressly disagreed with the Federal Circuit's holding in *Chamberlain Group, Inc. v Skylink Technol., Inc*. (Fed Cir 2004) 381 F3d 1178, 1203, that §1201(a) requires plaintiffs to demonstrate that the circumventing technology infringes or facilitates infringement of the plaintiff's copyright (an "infringement nexus requirement"), as "contrary to the plain language of the statute," which simply requires unauthorized access to copyrighted content, but not any underlying infringement itself. 629 F3d at 950.

Another case involving DMCA claims and allegations of video game hacking and cheating was *Datel Holdings, Ltd. v Microsoft Corp.* (ND Cal, Oct. 4, 2010, No. CV 09–5535 EDL) 2010 US Dist Lexis 110304 (the author of this article represented Microsoft in the action). The British company Datel filed an action against Microsoft for violations of §§1 and 2 of the Sherman Act (15 USC §§1, 2) and §3 of the Clayton Act (15 USC §14), alleging that Microsoft unlawfully monopolized the relevant markets for the Xbox 360 online video game system and Xbox 360 accessories by issuing a software update that disabled Datel's memory card devices and controllers after Datel circumvented the Xbox 360's accessory authentication system. Microsoft counterclaimed for violation of the DMCA, among other things, alleging that Datel trafficked in circumvention devices (including its memory card and other accessories) that bypassed security features of the Xbox 360 that protected against unauthorized access to copyrighted video game content. See 2010 US Dist Lexis 110304, *2.

As Microsoft alleged, the Xbox 360 was designed, among other things, to prevent ordinary consumers from copying copyrighted video game data to and from a personal computer to prevent, not only the unauthorized modification and distribution of video game content, but also any arbitrary, unauthenticated data from being transferred to the Xbox 360. The Xbox 360 console has layers of protection, including encryption, cryptographic algorithms, and unique, unpublished file formats to prevent copying. Microsoft alleged that Datel circumvented several of these protection layers by selling memory cards with a transferable secure digital (SD) card reader, which allowed users to transfer data to and from editable environments such as a PC and to transfer and alter video game content. The action ultimately settled before the court reached a ruling on the DMCA claims.

Below is an image of Datel's memory card with the removable SD card:

Interplay Between DMCA and Antitrust Law

The *Datel* case raised an interesting question relating to the intersection of antitrust law and the DMCA's anti-circumvention provisions. Datel, together with amici from the Electronic Frontier Foundation and Public Knowledge, argued that Microsoft was using the DMCA to enforce technological protection measures that had been designed to limit consumer choice and prevent outside competition. Microsoft responded that it was challenging Datel's memory cards under the DMCA not to hinder competition, but because the features that distinguished Datel's memory cards from Microsoft's memory card gave unauthorized access to game content, threatening rampant cheating in online play, piracy of virtual goods and games, and security breaches to the Xbox 360 console and LIVE network. Microsoft only challenged Datel's memory cards and related devices that allowed users to copy copyrighted game content to a PC and to access that content at the individual file level so that the content could be modified and shared over the Internet; Microsoft was not challenging any other competing Datel devices.

In an earlier case, *Sony Computer Entertainment Am., Inc. v Gamemasters* (ND Cal 1999) 87 F Supp 2d 976, the defendant sold a product called the "Game Enhancer" for the Sony PlayStation, which had "similar" functionality to the Game Shark made

by Sony, but "unlike" the Game Shark product "enable[d] users to play imported, i.e., non-territory games." 87 F Supp 2d at 982. The court held that the defendant's distribution of the product likely violated the DMCA and granted Sony a preliminary injunction. 87 F Supp 2d at 989. Without reaching the question of whether there could be a misuse defense to a §1201(a) claim, the court rejected the defendant's "misuse" theory that the "plaintiff is actually seeking to enjoin sales of the Game Enhancer because it competes with a similar product manufactured by [Sony], the Game Shark." As the court held, the "GameShark and the Game Enhancer *are not the same product* as only the Game Enhancer allows users to play non-authorized, non-territory video games by circumventing the PlayStation's built in controls," which is its "*distinguishing feature*." 87 F Supp 2d at 989 (emphases added).

By selling devices that facilitate cheating and hacking in game play, parties may be inducing end users to breach the games' terms of use, which prohibit cheating, hacking, and similar conduct.

The Ninth Circuit also recently addressed the interplay between antitrust law and the DMCA in *MDY Indus., LLC v Blizzard Entertainment*, *Inc.* (9th Cir 2010) 629 F3d 928. There, the Ninth Circuit considered and rejected the defense of copyright misuse to a 17 USC §1201(a) claim. The Ninth Circuit noted that in *Chamberlain Group, Inc. v Skylink Technol., Inc*. (Fed Cir 2004) 381 F3d 1178, the Federal Circuit "feared that § 1201(a) would allow companies to leverage their sales into aftermarket monopolies, in potential violation of antitrust law and the doctrine of copyright misuse." *MDY Indus., LLC,* 629 F3d at 949. In rejecting *Chamberlain*'s interpretation of §1201(a), the Ninth Circuit emphasized that such "policy concerns" are "best directed to Congress in the first instance," and "*cannot trump the statute's plain text and structure*." 629 F3d at 950 (emphasis added). As Judge Patel similarly held in *RealNetworks, Inc. v DVD Copy Control Ass'n* (ND Cal 2009) 641 F Supp 2d 913, "the reach of the DMCA is vast and it does not allow courts the discretion" to "render a value judgment untethered from the language of the statute." 641 F Supp 2d at 944.

In considering the defendant's copyright misuse defense, the Ninth Circuit held (*MDY Indus., LLC,* 629 F3d at 951 n13 (emphasis added)):

> Copyright misuse is an equitable defense to *copyright infringement* that denies the copyright holder the right to enforce its copyright during the period of misuse. . . . Since we have held that § 1201(a) *creates a right distinct from copyright infringement*, we conclude that we need not address copyright misuse in this case.

Although the Ninth Circuit declined to determine the precise "interplay between this new anti-circumvention right and antitrust law," noting that Blizzard did "not seek to put a direct competitor who offers a competing role-playing game out of business," the court made clear that policy considerations cannot displace the plain language of the statute. 629 F3d at 951.

Tortious Interference With Contractual Relations

Other possible legal avenues to pursue distributors of cheating and hacking devices are claims for the inducement of breach of contract or tortious interference with contractual relations. By selling devices that facilitate cheating and hacking in game play, parties may be inducing end users to breach the games' terms of use, which prohibit cheating, hacking, and similar conduct.

In *MDY Indus., LLC v Blizzard Entertainment*, Inc. (9th Cir 2010) 629 F3d 928, Blizzard asserted a claim against MDY for tortious interference with contractual relations under Arizona law. The Ninth Circuit held that Blizzard satisfied four of the five elements under Arizona law for the claim: first, a valid contractual relationship existed between Blizzard and its customers based on the operative end user license agreement and terms of use; second, MDY was aware of this relationship: third, MDY intentionally interfered with Blizzard's contracts, *e.g*., MDY programmed Glider to be undetectable by Warden; and finally, Blizzard proffered evidence that it was damaged by MDY's conduct. 629 F3d at 955. The Ninth Circuit nonetheless held that there were disputed issues of fact with respect to the last element, whether MDY's actions were "improper," which involves a seven-factor test under Arizona law. 629 F3d at 955. The court noted, *e.g*., that "if the fact-finder decides that Blizzard did not ban bots at the time that MDY created Glider, the fact-finder might conclude that MDY had a legitimate interest in continuing to sell Glider." 629 F3d at 956.

Notably, California does *not* require that a plaintiff prove that an act was independently wrongful or improper in a tortious interference claim. Therefore, the Ninth Circuit's analysis on this last element would not apply to claims brought under California law. See

Quelimane Co. v Stewart Title Guar. Co. (1998) 19 C4th 26, 56.

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (CFAA) (18 USC §1030) makes it unlawful to: "knowingly and with the intent to defraud . . . exceed . . . authorized access [of a protected computer], and by means of such conduct further . . . the intended fraud and obtain . . . anything of value." 18 USC §1030(a)(4). Although the CFAA likely would apply to individual hackers or cheaters of video games who gain unauthorized access to computer systems, *i.e*., primary violators, it may be difficult to assert CFAA claims against those who distribute video game cheating and hacking devices under a secondary liability theory, although there is a split of authority on that point. See, *e.g., Doe v Dartmouth-Hitchcock Med. Ctr.* (D NH, July 19, 2001, No. 00–100-M) 2001 US Dist Lexis 10704, *12 (rejecting plaintiff's theory of vicarious liability under CFAA and noting that statute creates "only a limited private right of action against *the violator*") (emphasis in original)). But see *Charles Schwab & Co. v Carter* (ND Ill, Sept. 27, 2005, No. 04 C 7071) 2005 US Dist Lexis 5611, *22 (holding that "imposing vicarious liability would further the CFAA's purpose"); *Ipreo Holdings LLC v Thomson Reuters Corp*. (SD NY, Mar. 8, 2011, No. 09 Cv. 8099 (BSJ)) 2011 US Dist Lexis 25356 (same).

A Cautionary Tale, but with a Happy Ending?

Filing a motion for a preliminary injunction against a distributor of cheating or hacking devices should not be a knee-jerk reaction, but should be sufficiently supported by the law and the facts, because the denial of such a motion can potentially be the death knell of a case. Although a plaintiff ultimately may prevail on the merits despite losing a preliminary injunction motion, the outcome can be several months if not years down the road, during which time the economic damage to a game might be irreversible as players flock to the next hot game.

In *Jagex Ltd. v Impulse Software* (D Mass 2010) 750 F Supp 2d 228, the owner of Runescape, a massive multi-player interactive online game, brought suit against the defendants, who operated several websites that offered tools allowing players to cheat at several interactive games, including Runescape. The defendants developed and sold a software program called "iBot" or "Bot" that enabled Runescape users to advance their characters through the game with little or no human participation, similar to MDY's Glider tool. The Bot software functioned by downloading a free copy of Runescape from the plaintiff's website and using a process called "reflection" to examine the game's internal operation, which is normally hidden from users. 750 F Supp at 231. The Bot software used this information to identify objects in the Runescape game with which it wished to interact and then completed a desired task according to instructions from a script. In essence, the Bot played the game for its owner while he or she was away from the computer.

To preserve the competitive level playing field that attracts the majority of users to online play—and to preserve internal game economics—game developers have no choice but to police online cheating and hacking activities.

The plaintiff Jagex moved for a preliminary injunction under several claims, including copyright infringement and violation of the DMCA and the CFAA. The court found that the plaintiff was unlikely to prevail on its copyright claim because the plaintiff had not alleged infringement of its game client software or website. The plaintiff did not have any copyright registrations covering its game client software or website; rather, it only had registrations applicable to various two-dimensional icons that appeared in the Runescape game (*e.g*., an "anvil icon," an "archery icon," and a "chisel icon"), none of which the defendants had used in their Bots or websites. 750 F Supp at 236. The court further rejected the plaintiff's DMCA claim because, unlike the plaintiff in *MDY Indux., LLC v Blizzard Entertainment, Inc., supra,* the plaintiff Jagex had not indicated a specific "technological measure" that the defendants' Bots were circumventing. 750 F Supp at 237.

Finally, the court rejected the plaintiff's claim under the CFAA. The plaintiff had alleged that the defendants, by offering the Bots for sale, exceeded their authorized access to the plaintiff's server by violating the terms and conditions stated on the Runescape website. 750 F Supp at 238. Although the court rejected the defendants' argument that the Runescape server did not qualify as a "protected computer" under the statute, the plaintiff "fail[ed] to explain how the defendants (as opposed to the Bots users) exceed[ed] authorized access to the Runescape server." 750 F Supp at 238. At best, the plaintiffs had proffered a theory of contributory liability under the CFAA, which the court concluded was not sufficiently supported by the case law.

Notwithstanding the plaintiff's early loss at the preliminary injunction stage, it ultimately did reach a settlement with the defendant nearly 2 years later. In January 2012, the defendant agreed to a permanent injunction to cease distribution of the products at issue. Although the settlement undoubtedly was an important victory for the plaintiff, there could have been a significant economic impact on the plaintiff in the interim. Two years can be a lifetime in the development and release of new online multi-player games, and any new games could take the spotlight (and users) away from Runescape.

CONCLUSION

As online game play becomes increasingly widespread, inevitably there will be more and more people who seek to bend or break the rules of online play—and more and more third parties who profit off of such players by distributing cheating and hacking tools to facilitate such conduct. To preserve the competitive level playing field that attracts the majority of users to online play—and to preserve internal game economics—game developers have no choice but to police online cheating and hacking activities. While internal enforcement measures may stem cheating and hacking in the short term, gaming developers are beginning to understand that a more broad-based and effective means of halting such behavior is to seek legal action against third parties that distribute the tools that enable cheating and hacking. And as the action shifts from the iPad or computer screen to the courtroom, lawyers may become the new gaming heroes (or, depending on your perspective, villains).