
THE GOD PARADOX

JOSHUA A.T. FAIRFIELD*

INTRODUCTION	1018
I. BACKGROUND	1019
A. <i>Technological and Legal Control</i>	1021
B. <i>A Taxonomy of Control</i>	1022
C. <i>Normative Implications of Game God Control</i>	1024
II. THE LAW OF CONTROL AND LIABILITY	1025
A. <i>Control of Intellectual Property</i>	1025
1. Control and Copyright Infringement	1025
a. <i>Direct Infringement</i>	1026
b. <i>Vicarious Liability</i>	1029
c. <i>Contributory Liability</i>	1030
d. <i>Control Under the Digital Millennium Copyright Act</i> ..	1031
2. Control and Trademark Infringement	1035
a. <i>Secondary Trademark Liability in Electronic Markets</i> .	1036
b. <i>Secondary Trademark Liability in Virtual Worlds:</i> <i>Marvel</i>	1037
3. Control and Net Neutrality	1038
B. <i>Control in the Common Law</i>	1040
1. The Communications Decency Act and Control	1040
2. Contract Law	1045
3. Tort Liability	1048
a. <i>Negligence</i>	1048
b. <i>Third Party Hacks</i>	1049
4. Property Law	1051
a. <i>Real Property</i>	1052
b. <i>Personal Property</i>	1054
5. Agency and Employment	1055
C. <i>Democracy Versus Theocracy: Control and the Constitution</i> ...	1058
1. Public Liability for Private Actors	1058
2. The Panopticon	1059
3. The Company Town	1061

* Associate Professor of Law, Washington & Lee University School of Law. Many thanks to the Frances Lewis Law Center for research funding. Thanks to Sandy Askland, Gary Marchant, the participants at the ASU Virtual Worlds Roundtable, the Hans-Bredow-Institut, the Friedrich Ebert Foundation, and the participants of the Virtual Worlds and Law Berlin 2008 conference for the opportunity to present these ideas. Thanks to Ted Castronova, Greg Lastowka, Dan Hunter, Benjamin Duranske, Richard Bartle, Viktor Mayer-Schoenberger, Ren Reynolds, Eric Goldman and Robert Bloomfield for suggestions and conversations, and to Steve Mammarella for invaluable research assistance. All errors must be blamed on the inscrutable workings of the game gods.

III. RESOLVING THE GOD PARADOX.....	1062
A. <i>A Model for Minimalism: Common Carriage</i>	1063
B. <i>Recognition of Virtual Property for Ownership Disputes</i>	1066
C. <i>Stronger User Tools</i>	1067
CONCLUSION.....	1067

The companies that run virtual worlds – self-proclaimed “game gods” – exercise significant power over the environments they create and the people who use them. Game gods believe that they must retain ownership of and control over their creations and over the creations of their users. In some cases, control is necessary to ensure the artistic integrity of the world. However, in other cases, game gods assert control because they fear legal liability. This latter approach will backfire. This is the “God Paradox”: the more control a game god keeps in order to avoid legal liability, the more responsibility it will ultimately bear. This Article details the types of control currently exercised by game gods, how that control can and will increase the risk of liability, and several practical solutions to the problem.

“With great power comes great responsibility.”¹
 – Peter Parker (Spider-Man)

INTRODUCTION

This Article asks whether the companies that create and control virtual worlds should exercise the power of “game gods” over their customers or should instead permit the free flow of information over their networks. I argue the latter: companies wishing to limit their exposure to legal liability should view themselves less as gods and more like telephone companies.

The companies that create virtual worlds style themselves “gods.” The term is descriptive: game gods exercise complete technological control over the worlds that they create. Game gods also claim legal authority to regulate the economic, public, and intimate lives of the millions of people who work, play, and live in those worlds. Virtual world creators must exercise some control over virtual worlds to ensure the success of their artistic vision. But they claim much more control than is necessary. Game gods do this because they believe that total control over virtual environments is necessary to avoid legal liability.² For example, game gods claim ownership of all virtual land within a

¹ SPIDER-MAN (Columbia Pictures 2002).

² See Richard Bartle, *Pitfalls of Virtual Property*, 2004 THEMIS GROUP 9, available at <http://www.themis-group.com/uploads/Pitfalls%20of%20Virtual%20Property.pdf> (father of modern virtual worlds noting that game gods must retain ownership and control over all virtual land and property or else risk liability for damage to players’ property); BENJAMIN TYSON DURANSKE, VIRTUAL LAW 102 (2008) [hereinafter DURANSKE, VIRTUAL LAW] (“If a provider failed to set up appropriate contractual protections and shut down the servers while ‘owing’ users their virtual property, everyone who had an account would presumably be able to get in line with the electric company and the provider’s real-world landlords to try to

world because they are concerned that they might be liable to virtual world residents for loss of the land if the virtual world is shut down.³ Or they claim ownership of all user-generated content out of fear that users might sue them for copyright infringement.

This Article argues that the strategy of increasing control to reduce liability is fundamentally flawed. A theme runs through U.S. statutory and common law: the more control a corporation asserts over people, places, and things, the more responsibility the company bears when things go wrong. This is the God Paradox: game gods assert control in order to avoid legal liability, but such efforts instead increase risk. Conversely, if game gods cede control to their players, they will be less open to liability.

The Article demonstrates this basic idea in three Parts. Part I discusses how game gods control virtual worlds through technology and law. Part II details the many different places in our legal framework where an increase in control results in an increase in legal liability, and demonstrates the increased risk through case examples. Part III proposes some solutions. My conclusion is a simple one: game gods must relinquish a little control or suffer a lot of liability.

I. BACKGROUND

Virtual worlds are three-dimensional social software, the marriage of social networking technologies and three-dimensional game graphics.⁴ Although there are varied uses for virtual worlds, the largest commercial applications for the technology to date have been in games. For purposes of simplicity, I will therefore refer to users of virtual worlds – even of worlds that are not games – as “players,” and creators of virtual worlds as “game gods.”

In a virtual world, a player logs in to a simulated three-dimensional environment. The player is represented by an avatar, which is a virtual representation of the person, character, or concept she wishes to express. The player often uses a client program on her computer to access a central server, which coordinates all of the different users’ experiences. Thus, the player is

collect on the debt of virtual swords . . .”). The same problems exist with Web 2.0 providers. See Posting of Mark Zuckerberg to Facebook Blog, <http://blog.facebook.com/blog.php?post=54434097130> (Feb. 16, 2009, 14:09) (attempting to calm public reaction against Facebook’s attempt to change its Terms of Use to grant itself a perpetual license in the personal information of its users, and characterizing the attempt as a formality intended to protect Facebook from liability).

³ *Id.*; see also DURANSKE, VIRTUAL LAW, *supra* note 2, at 102.

⁴ See Bragg v. Linden Research, Inc., 487 F. Supp. 2d 593, 595 n.1 (E.D. Pa. 2007) (citing Woodrow Barfield, *Intellectual Property Rights in Virtual Environments: Considering the Rights of Owners, Programmers and Virtual Avatars*, 39 AKRON L. REV. 649, 649 (2006)) (“The virtual world at issue is an interactive computer simulation which lets its participants see, hear, use, and even modify the simulated objects in the computer-generated environment.”).

not alone in this three-dimensional world. She shares it with thousands of other users.

A fundamental characteristic of a virtual world is that it is social. Imagine a small city, with perhaps five to ten thousand residents. Citizens buy and sell goods, build friendships and romantic relationships, go on trips, explore, sightsee, build houses, earn money, work together, learn, and fight. If that city were a digital landscape, inhabited by virtual characters controlled by real people, it would be a virtual world.

Although the worlds are virtual, the users experience them as real. Virtual worlds are important to players, because they offer opportunities for real social interaction. For example, roughly fifty percent of users in Linden Lab's Second Life⁵ claim that their online friends are as good as or better than their "real-life" friends.⁶ Players import real-world concerns, conflicts and relationships online, and they export relationships, ideas, and social connections made in the virtual world. People pay real dollars for virtual land and objects, and use virtual currencies to buy real-world items.⁷ Players make a real-world living designing virtual objects and spaces. For example, Anshe Chung, the first virtual-world millionaire, made her fortune speculating on virtual land in the virtual world Second Life.⁸ For many players, virtual worlds are not merely a game to pass time, or a replacement for the real world, but an augmented way to live life.⁹

Some worlds are quite small and are limited to text. Others are enormous: Blizzard's World of Warcraft game claims ten million subscribers.¹⁰ Some virtual worlds are games.¹¹ Others, like Second Life, There,¹² or IMVU¹³ are

⁵ Second Life, <http://secondlife.com/> (last visited Mar. 16, 2009).

⁶ See *Online Virtual Worlds: Applications and Avatars in a User-Generated Medium: Hearing Before the H. Subcomm. on Telecomms. and the Internet*, 110th Cong. (2008) (statement of Rep. Cliff Stearns, Ranking Member, H. Subcomm. on Telecomms. and the Internet), available at http://energycommerce.house.gov/cmte_mtgs/110-ti-hrg.040108.VirtualWorlds.shtml.

⁷ See, e.g., *Bragg*, 487 F. Supp. 2d at 595 n.5.

⁸ See Posting of Rob Hof to The Tech Beat, http://www.businessweek.com/the_thread/techbeat/archives/2006/11/second_lifes_fi.html (Nov. 26, 2006).

⁹ Indeed, when Second Life modified one of its policies about sexual and violent content, many residents joined in protest, claiming that they, as a community, determined what was acceptable, not Linden Lab. See Posting of Tateru Nino to Second Life Insider, <http://www.secondlifeinsider.com/2007/06/09/painted-into-a-corner> (June 9, 2007, 1:00).

¹⁰ Press Release, Blizzard Entertainment, Inc., World of Warcraft Reaches New Milestone: 10 Million Subscribers (Jan. 22, 2008), available at <http://eu.blizzard.com/en/press/080122.html>.

¹¹ Blizzard's World of Warcraft, Eidos Interactive's Age of Conan: Hyborian Adventures, Webkins, Neopets, Club Penguin, and Coke Studios, to name a few.

¹² There, <http://www.there.com/> (last visited Mar. 16, 2009).

¹³ IMVU, <http://www.imvu.com/> (last visited Mar. 16, 2009).

predominantly social tools – chat interfaces combined with networking and software development tools. Some virtual worlds exist solely for entertainment purposes and look like networked video games. Other worlds look like games, but are open to whatever the residents in the virtual worlds wish to create. Virtual worlds have been used for medical, military, commercial, and educational purposes.¹⁴

Virtual world technology is rapidly increasing in importance.¹⁵ Just as businesses rushed to develop websites in the 1990s, many businesses are developing their own virtual worlds in which consumers can try products, build brand identity, and network.¹⁶ Virtual worlds thus may become the next iteration of Internet technology. From a two-dimensional interface, virtual worlds provide a three-dimensional context. Humans instinctively think in three dimensions, and this new context has proven extremely attractive to millions of players worldwide. Yet despite the widespread adoption of virtual world technology, legal analysis of the issues arising in virtual worlds is still in its early stages. Questions of liability are a particularly hot topic. Because of fear of liability, cases settle or are dropped, and few cases have reached conclusion in a way that yields clear rules.¹⁷ This Article seeks to fill that gap.

A. *Technological and Legal Control*

Game gods seek to control virtual worlds by technological means and regulate the actions of players by law. Technologically, game gods build

¹⁴ For example, many college and universities have established “virtual classrooms” where professors can interact with students and even teach classes. Harvard Law School established one such class in the fall of 2006. For a description of this course, see CyberOne: Law in the Court of Public Opinion, <http://web.archive.org/web/20071218105316/http://blogs.law.harvard.edu/cyberone/administration/course-description> (last visited Mar. 16, 2009).

¹⁵ See Jessica Bennett & Malcolm Beith, *Alternate Universe*, NEWSWEEK, July 30, 2007, <http://www.newsweek.com/id/32824>.

¹⁶ See Adam Reuters, *IBM Accelerates Push into 3D Virtual Worlds*, REUTERS, Nov. 9, 2006, <http://secondlife.reuters.com/stories/2006/11/09/ibm-accelerates-push-into-3d-virtual-worlds> [hereinafter Reuters, *IBM Accelerates Push*].

¹⁷ For example, Blizzard Entertainment’s lawsuit against Peons4Hire settled. See Benjamin Duranske, *Blizzard v. In Game Dollar Update: Injunction Entered, Peons Not 4Hire in World of Warcraft Anymore*, VIRTUALLY BLIND, Feb. 1, 2008, <http://virtuallyblind.com/2008/02/01/peons4hire-blizzard-injunction> [hereinafter Duranske, *Peons Not 4Hire*]. Bragg’s suit against Linden settled as well. See Benjamin Duranske, *Bragg v. Linden Lab – Confidential Settlement Reached*, VIRTUALLY BLIND, Oct. 4, 2007, <http://virtuallyblind.com/2007/10/04/bragg-linden-lab-settlement/> (explaining that Bragg had brought suit after Linden Lab revoked his account for allegedly obtaining virtual land through non-public portions of the Second Life website).

virtual worlds and reserve to themselves powers that players do not have.¹⁸ A game god can change the terrain of a virtual world merely by altering the code. Gods can create or destroy virtual property or land at the click of a button. They can ban or destroy players' goods, land, and avatars.¹⁹ They can change the physics of the world. If the god permits, players can fly; if not, players must walk. The god can invisibly observe any place or person and can listen in on and record all conversations. Thus, game gods have truly godlike control over a virtual world.

Gods exercise legal control through contracts such as End User License Agreements (EULAs) and Terms of Service that permit access to virtual worlds.²⁰ These EULAs read in part like standard intellectual property licenses.²¹ But they also contain provisions alien to IP licensing. In a virtual-world EULA, users agree to a set of social constraints.²² Players agree not to say provocative things and to play nicely.²³ Sometimes players agree to not access or use the virtual world with products developed by other software companies.²⁴ In short, EULAs require players to agree to many things that would seem odd in relation to a license of intellectual property. Suppose the license to view a rented DVD required the viewer to publish a positive review of the movie on the Web, or only to eat Orville Redenbacher's popcorn while watching it.²⁵ That would seem strange, yet these sorts of social constraints are routine in virtual world EULAs. The question remains: why do game gods feel that they need this level of technological and social control over their worlds and the players that inhabit them?

B. *A Taxonomy of Control*

Game gods exercise control to achieve two distinct ends. First, gods need to continue development and ensure the artistic integrity of the worlds. For example, if a game needs new content, the game god can add a continent, a city, new areas to explore and new challenges to overcome. This is a

¹⁸ A player, for example, cannot add six fingers to their avatar unless the program code allows them to do so. A game god, in contrast, can simply change the code to add six fingers.

¹⁹ See, e.g., Second Life, Terms of Service § 5.3, <http://secondlife.com/corporate/tos.php> (last visited Mar. 16, 2009).

²⁰ See *id.* (stating that if a user declines the terms, he is prohibited from accessing or using Second Life).

²¹ See *id.* § 3.2.

²² See, e.g., Second Life, Community Standards, <http://secondlife.com/corporate/cs.php> (last visited Mar. 16, 2009) (describing six behaviors that lead to suspension or expulsion from the Second Life community: intolerance, harassment, assault, invasion of privacy, indecency, and disturbing the peace).

²³ See *id.*

²⁴ See Second Life, Terms of Service, *supra* note 19, § 4.2.

²⁵ Relax, they don't; eat whatever popcorn you like.

necessary power for the betterment of the game. It is not directed at controlling the players of the virtual world except to entice the players to pay for new content. An appropriate analogy would be Microsoft's ability to release patches to its software, security updates, and so on. This ability does not directly constrain users of Microsoft's operating system, but instead maintains the structural integrity of the overall product.

Gods also exercise their technological power in order to control players. If a player harasses other players or cheats, for example, the player may find herself suspended or permanently banned, or have her account deleted.²⁶ If the player protests unfair actions by the company, or speaks on an issue that the company considers politically or religiously inappropriate, the user may again find herself removed.²⁷ Under the received wisdom, there are no limitations on the gods' right to suspend or delete accounts that players may have spent years building.²⁸ Suppose Microsoft had the ability to delete all copies of any content drafted on Microsoft Word that was critical of its business practices. Game gods routinely exercise that sort of power over players.

There is a connection between the two kinds of control. If the social behavior of players spirals out of control, game gods will not be able to deliver a useful product, or the artistic integrity of the world might be compromised. But this Article is not concerned with close questions – I am happy to cede to game gods the ability to exercise control when the integrity of the game is at stake. Nevertheless, game gods claim too much. Game gods claim that the exercise of free speech disrupts their world.²⁹ They claim that ownership of private property disrupts their world.³⁰ They claim that truthful criticism of their product disrupts their world.³¹ They claim that the basic capitalist exchange of money for time disrupts their world.³² They claim that user creativity and ownership of user-created intellectual property disrupts their world.³³ These claims are certainly somewhat true, if often overstated. But

²⁶ See Second Life, Terms of Service, *supra* note 19, § 4.1.

²⁷ See *id.*

²⁸ See *id.* § 2.6.

²⁹ See Nick Wadhams, *Online Games Increasingly a Place for Protest, Social Activism*, LONG BEACH PRESS-TELEGRAM, Feb. 8, 2003.

³⁰ See Tom Loftus, *Virtual Worlds Wind Up in Real World's Courts*, MSNBC.COM, Feb. 7, 2005, <http://www.msnbc.msn.com/id/6870901>.

³¹ See PETER LUDLOW & MARK WALLACE, *THE SECOND LIFE HERALD: THE VIRTUAL TABLOID THAT WITNESSED THE DAWN OF THE METAVERSE* 5-17 (2007) (describing how Ludlow's account in The Sims Online was terminated after publishing an online newspaper critical of security measures in place by the game operator, Electronic Arts).

³² Blizzard has recently begun targeting spammers who sell gold and offer to level up your World of Warcraft character for you. A recent victory, resulting in a permanent injunction against peons4hire.com, has both players and commentators happy. See Duranske, *Peons Not 4Hire*, *supra* note 17.

³³ In 2006, Billy Bragg, a British musician, removed his songs from the social networking website MySpace.com claiming that the site's Terms of Use granted a

game gods who act on these claims and exercise absolute control over virtual worlds place themselves at a significant risk of increased legal liability.

C. *Normative Implications of Game God Control*

Given that virtual worlds are having a serious impact on society, and that millions of U.S. citizens are importing their creative, emotional, political, and economic lives into these worlds, it is worth asking what the impact of these expressions of legal and technological control will be on the populations of virtual worlds.

This Article takes a decidedly pro-consumer libertarian normative position. If virtual-world technology is to become a ubiquitous and powerful communications technology in a free and democratic society, then the companies who run virtual worlds ought to be more like telephone companies and less like “gods.” The telephone company does not filter messages, engage in mass surveillance of telephone calls for customer-service purposes, arbitrate disputes between callers, or determine which calls are appropriate or inappropriate. Game gods currently do all these things and they should not. Game gods control what people can say via their networks, own all content posted to their networks, and can record and parse all conversations that occur through their networks. But imagine if early telephone companies had tried to exercise this level of control over telephone conversations. The telephone would not have become the engine of discourse and communication it currently is.

Further, this Article takes what I will term an “augmentationist” technological position. Virtualization technology is at its least interesting when confined to fantasy worlds, and its most interesting when it mixes elements of play with real-world profit and communication. If virtual worlds remain just games, then it will not matter much that they cannot be used as spaces for conversation, commerce, and democracy. But if this technology is to become mainstream, game gods will need to do a little less dictating and a little more customer service in order to succeed.

Thus, this Article argues that basic principles of U.S. law increase the liability of companies that exercise excessive control over the ideas, property, personhood, and communications of the multi-million citizen populations of such worlds. Conversely, U.S. law should do more to protect companies that adopt a hands-off policy. The following Parts analyze the interplay between control and liability in U.S. statutory and common law and offer suggestions for improvement.

“nonexclusive, fully paid and royalty-free worldwide license” in his music. *See* Robert Levine, *Billy Bragg’s MySpace Protest Movement*, N.Y. TIMES, July 31, 2006, at C5. Since then, however, MySpace has modified the Terms of Use to severely limit their rights in user-posted content. *See* MySpace.com, Terms & Conditions § 6.1 (Feb. 28, 2008), <http://www.myspace.com/index.cfm?fuseaction=misc.terms>.

II. THE LAW OF CONTROL AND LIABILITY

The law is no stranger to the conversation between corporations and citizens. Corporations have long claimed that they must have control over how customers use products, but must have no liability for any harm that occurs from such use.³⁴ That argument has not worked before, and will not protect game gods now. Everywhere one looks in the U.S. legal system, the more control a corporation asserts over the uses of its products and the actions of its customers, the more liability that corporation will bear in the event of harm.

There are three major sources of potential liability for game gods. First, questions of control of intellectual property spawn the most disputes between players, game gods, and third-party owners of intellectual property. Second, common law legal theories, including claims sounding in contract, tort, or even property law, may provide a basis for proceedings against game gods that retain too much control. Finally, constitutional law and other public-policy-oriented legal theories may impose the responsibilities of government on companies that claim the regulatory powers of governments. The following Sections act as a legal archaeological expedition, unearthing the control/liability principle in intellectual property, in several basic areas of the common law, and finally in constitutional law and public policy.

A. *Control of Intellectual Property*

The fiercest disputes in virtual worlds are those that involve the intellectual property created by the game god, by the community itself, or by third parties but ostensibly misused by either the god or the community. This Section examines these intellectual property claims in detail, and demonstrates that game gods' attempts to claim control or ownership over these three categories of intellectual property exposes them to increased liability.

1. Control and Copyright Infringement

Most game gods claim a copyright interest in all content that appears in their virtual worlds.³⁵ Sometimes the game gods generate the copyrighted material; there, the interest is legitimate.³⁶ Some copyrighted material, however, is generated by the user base.³⁷ This proliferation of user-generated content is called Web 2.0 in somewhat passé developer slang. Web 2.0 models (which

³⁴ For instance, if a toaster manufacturer disclaims all uses of its product, it does so to try to limit liability and control user actions. However, from a sale point of view, it will want consumers to use the toaster in any way conceivable (so they will sell more), but without exposing itself to additional liability.

³⁵ See, e.g., World of Warcraft, End User License Agreement § 4(A), <http://www.worldofwarcraft.com/legal/eula.html> (last visited Apr. 9, 2009) (stating that, among others, all "characters, character names, . . . character inventories, . . . [and] character likenesses . . . are owned or licensed by Blizzard").

³⁶ See, e.g., *id.* § 1.3.

³⁷ See *id.* § 4(A).

include non-game websites such as YouTube or Facebook, as well as virtual worlds) rely on the consumers to develop content. Several virtual worlds follow some form of the Web 2.0 model. For example, Second Life permits near-total user freedom to create. The company creates the infrastructure and tools used to create the content. Other social sites, like The Lord of the Rings Online,³⁸ limit user creativity to the assembly of pre-generated components. A user might create a unique room or avatar by combining pre-set components provided by the game god.

Game gods claim this control because they fear liability to the user. The problem is this: if a user leaves a game, the company wants to be able to continue to display the content in its own right.³⁹ But this approach will backfire. First, as a matter of general fairness, one wonders whether mass expropriations of intellectual property from consumers to corporations can withstand court scrutiny under doctrines of unconscionability. But more importantly, game gods' claims of control over user-generated copyrighted material may expose the god to liability, especially when users create, distribute, and use infringing content.

a. *Direct Infringement*

The gods' claim of control over user-generated copyrighted material creates the first problem. Early in the development of the Internet, intellectual property owners sued internet service providers ("ISPs") (much like game gods in many respects) because users posted infringing content to the ISPs' bulletin boards. These first claims of direct infringement were successful, based on plaintiffs' claims that the ISP directly violated the plaintiffs' copyrights by

³⁸ The Lord of the Rings Online, <http://www.lotro.com/> (last visited Mar. 16, 2009).

³⁹ This is apparent through the game god either claiming ownership over all virtual content, World of Warcraft, End User License Agreement, *supra* note 35, § 4, or, in Second Life's case, reserving an irrevocable license. See Second Life, Terms of Service, *supra* note 19, § 3.2. For example, in February 2009, the *Consumerist* broke news that Facebook amended its Terms of Use to grant itself a perpetual, universal, irrevocable license, with right to sublicense, in its users' content. See Chris Walters, *Facebook's New Terms of Service: "We Can Do Anything We Want With Your Content. Forever."*, CONSUMERIST, Feb. 15, 2009, <http://consumerist.com/5150175/facebooks-new-terms-of-service-we-can-do-anything-we-want-with-your-content-forever>. Facebook CEO Mark Zuckerberg attempted to calm fears by asserting the liability-reduction rationale for control: "When a person shares information on Facebook, they first need to grant Facebook a license to use that information so that we can show it to the other people they've asked us to share it with. Without this license, we couldn't help people share that information." See Posting of Mark Zuckerberg to Facebook Blog, <http://blog.facebook.com/blog.php?post=54434097130> (Feb. 9, 2009, 14:09). The resulting uproar caused Facebook to retract its TOU changes.

making infringing material publicly available.⁴⁰ These cases established the control principle within the law of direct copyright infringement.

Courts soon began to develop a safe harbor for ISPs that did not claim any interest in the infringing material and had stored or posted material solely at a user's request. In *Religious Technology Center v. Netcom*,⁴¹ the Northern District of California instituted a new legal standard covering claims of direct infringement against bulletin-board operators by reading a knowledge requirement into copyright law.⁴² The court found that it would be inequitable to burden the ISP with strict liability for copyright infringement when the content was posted at the behest of the user, and the ISP had no legal interest beyond following the user's instructions.⁴³

Game gods do not leave the control over content to their users, have legal interests well beyond following the user's instructions, and often have knowledge of actual infringement because of the extensive monitoring apparatus that enables that control. Thus, many may not qualify for the *Netcom* safe harbor. The *Netcom* ISP did not claim the ability to display or make copies of the intellectual property itself; it merely claimed that it was following the user's instructions.⁴⁴ Thus, even the most basic ISP protection may be denied to game gods that claim a direct ownership interest in infringing intellectual property, or exercise their contractual right to display or copy material that turns out to be infringing.⁴⁵

An example applying these issues to virtual worlds may help. In *Marvel Enterprises, Inc. v. NCsoft Corp.*, comic-book titan Marvel sued game god NCsoft, the creator of the virtual world City of Heroes, for copyright infringement.⁴⁶ City of Heroes had a flexible and powerful character creator.

⁴⁰ See, e.g., *Playboy Enters. v. Frena*, 839 F. Supp. 1552, 1559 (M.D. Fla. 1993) (finding a bulletin board operator directly infringed Playboy's copyrights, stating that "knowledge is not an element of infringement").

⁴¹ 907 F. Supp. 1361 (N.D. Cal. 1995).

⁴² See *id.* at 1372.

⁴³ See *id.* at 1372-73. The court explained:

The court does not find workable a theory of infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred. Billions of bits of data flow through the Internet and are necessarily stored on servers throughout the network and it is thus practically impossible to screen out infringing bits from noninfringing bits.

Id.

⁴⁴ *Id.* at 1372.

⁴⁵ 17 U.S.C. § 501(a) (2006) establishes direct infringement when any of the rights of a copyright holder are infringed. Those rights, established in 17 U.S.C. § 106, include the right to reproduce, modify, distribute and transfer ownership, perform and display. Claiming ownership affects some, if not all, of these rights.

⁴⁶ *Marvel Enters., Inc. v. NCsoft Corp.*, 74 U.S.P.Q.2d 1303, 1305 (C.D. Cal. 2005) (contending that NCsoft's game "create[s] characters that are virtually identical in name, appearance, and characteristics to characters owned by Plaintiffs").

Using the character creation process, players could create nearly any superhero avatar they desired. Some players used the character generator to create superhero characters that were clearly imitations of, or derivative of, some of the comic book heroes that appear in Marvel comics.⁴⁷ For example, a City of Heroes character with bad hair and claws that sprout from the backs of his hands, called “The Badger,” would infringe Marvel’s copyright in the superhero Wolverine.

NCsoft had claimed control over user-generated content, including avatars, in its EULA. At trial, NCsoft reversed course, repudiated those claims, and asserted that it in fact did not control its players or the content they created.⁴⁸ After the Central District of California dismissed Marvel’s trademark claims,⁴⁹ and denied cross motions for summary judgment,⁵⁰ NCsoft and Marvel settled the copyright claims.⁵¹ The language of the settlement agreement was viewed in the industry as a clear win for NCsoft.⁵² NCsoft’s litigation posture – that it did not control its players and was not a co-owner of their intellectual property – appears to have been successful.

Although NCsoft repudiated at trial its EULA-based claims of control, other game gods have not followed suit. Not only do those gods reserve and exercise control over the players’ actions, but the gods also routinely claim either sole or co-ownership of the intellectual property that such players generate. It is likely that these claims of ownership and control will cause problems for game gods not only as a matter of direct copyright infringement, but also as a matter of customer relations. Players value their intellectual property contributions, and will resist enforcement of contract clauses designed to divest them of the ownership of their creative output.

Game gods could perhaps have foreseen these difficulties. The clauses in which game gods make these IP ownership claims were inherited from social networking sites, which suffered significant public relations setbacks once customers noticed and understood the import of the clauses. For example, MySpace’s EULA contained a clause granting MySpace a non-exclusive, unlimited, and universal license to display and distribute music posted to MySpace.⁵³ British rocker Billy Bragg noticed the clause, and complained that he did not want to give a potential competitor the license to distribute and

⁴⁷ *Id.* at 1306-07.

⁴⁸ See Memorandum of Points and Authorities in Support of Motion of Defendants NCsoft Corp. & NC Interactive, Inc. to Dismiss Plaintiffs’ First Amended Complaint at 17, *Marvel*, 74 U.S.P.Q.2d 1303 (No. 04CV9253RGK), 2005 WL 4748152.

⁴⁹ *Marvel*, 74 U.S.P.Q.2d at 1307-09 (dismissing claims of direct, contributory and vicarious infringement of both registered and common-law trademarks).

⁵⁰ See *id.* at 1306-07.

⁵¹ See Daniel Terdiman, *NCsoft Happy with Marvel Settlement*, CNET NEWS, Jan. 7, 2006, http://news.cnet.com/8301-10784_3-6023179-7.html.

⁵² See *id.*

⁵³ See Levine, *supra* note 33.

perform his music.⁵⁴ The resulting furor caused MySpace to reconsider its position,⁵⁵ but the clause remains standard throughout other social networking sites and virtual worlds.

Although game gods often claim total control and sole or shared ownership of copyright material created in virtual worlds, their desired litigation posture will differ dramatically from these pre-litigation claims. It is not surprising that Web 2.0 entrepreneurs, including game gods, desire control over the material created by their customers. The creativity of online communities drives the success of multi-billion-dollar companies like Facebook, YouTube, and MySpace. Yet game gods' claims of control over player-generated intellectual property exposes them to greater liability from claims of direct copyright infringement.

b. *Vicarious Liability*

Game gods may also be secondarily liable for what players do. The control-liability principle is directly expressed in the legal standard for vicarious liability.⁵⁶ A court may hold an ISP vicariously liable for infringing content if the ISP has the right and ability to exercise control over the actual user (the true infringing party) and derives profit from the posting.⁵⁷ Thus, “[i]n the context of copyright law, vicarious liability extends . . . to cases in which a defendant ‘has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities.’”⁵⁸ Therefore, “[o]ne infringes . . . vicariously by profiting from direct infringement while declining to exercise the right to stop or limit it.”⁵⁹ Reservations of control entangle ISPs with the infringing acts of their users. The risk of liability is directly linked to the extent of the power to police reserved by the company over its users.

Once a company has established control, failure to exercise it can also result in liability. This is not immediately intuitive. It is plausible that a company could claim control over a place or person, but need not act on its ability to control. However, case law has indicated that once a company asserts control,

⁵⁴ *See id.*

⁵⁵ *See* MySpace.com, Terms & Conditions, *supra* note 33, § 6.1.

⁵⁶ *See* Mark Bartholomew and John Tehranian, *The Secret Life of Legal Doctrine: The Divergent Evolution of Secondary Liability in Trademark and Copyright Law*, 21 BERKELEY TECH L.J. 1363, 1367 (2006) (“The most common test used to determine vicarious liability is control or the right to control the direct tortfeasor.”).

⁵⁷ *See* A&M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1022-24 (9th Cir. 2001) (stating that plaintiffs demonstrated a likelihood of success on vicarious copyright infringement claim based on Napster’s failure to police its system as well as the financial benefits to Napster from the continued availability of infringing files).

⁵⁸ *Id.* at 1022 (quoting *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259, 262 (9th Cir. 1996)).

⁵⁹ *See* *Metro-Goldwyn-Mayer Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913, 930 (2005). While the Supreme Court noted the widespread use of the vicarious/contributory liability framework, it did not itself endorse or reject that framework. *Id.* at 931.

it must exercise that control or be liable. For example, the Ninth Circuit noted: “To escape imposition of vicarious liability, the reserved right to police must be exercised to its fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability.”⁶⁰ This presents a serious problem for ISPs. If an ISP acts, it has exercised control and is liable for any harm. If it does not act, but has claimed control, the ISP is still liable for failing to prevent the harm. The sole solution for ISPs is to reduce the scope of claimed control, and to refrain from exercising control over the content.⁶¹

c. *Contributory Liability*

The direct relationship between control and liability is also present in the commonly used contributory liability standard. The general test for contributory liability is that the ISP, to be free from liability, must not materially contribute to, or actively induce, the infringement.⁶² The inducement portion is straightforward: the seller of a technology must not advertise the technology as being useful for infringement. But the other portion is harder. All Internet technologies materially contribute to the ability of users to directly infringe.

In order to avoid tarring all makers of communications technologies with the brush of secondary infringement, courts have focused on the concept of knowledge.⁶³ If a technology is susceptible of substantial non-infringing use, and the seller of the technology has no actual knowledge that the technology is being used to infringe, then the seller is not liable for contributing to the direct infringement of its customers.⁶⁴ There are two kinds of knowledge for purposes of a manufacturer’s potential contributory liability. Knowledge may be imputed if the technology is not susceptible to non-infringing uses.⁶⁵ Or, direct knowledge of specific infringing acts can be proven by evidence tending to show that the ISP was aware of acts of infringement by its customers and

⁶⁰ *Napster*, 239 F.3d at 1023 (citing *Fonovisa*, 76 F.3d at 261).

⁶¹ As discussed *infra* Part II.A.1.d, an ISP may exercise control on behalf of the copyright holder and be shielded from liability through the notice-and-takedown system described in the Digital Millennium Copyright Act (DMCA), 17 U.S.C. § 512 (2006) (providing that to be immune from copyright infringement, service providers must, upon receiving notice of claimed infringement, “respond[] expeditiously to remove, or disable access to, the material that is claimed to be infringing”).

⁶² See *Grokster*, 545 U.S. at 935.

⁶³ See *Napster*, 239 F.3d at 1021.

⁶⁴ See *id.* (stating that, without more, “a computer system operator cannot be liable for contributory infringement merely because the structure of the system allows for the exchange of copyrighted material”).

⁶⁵ The *Sony* Court established that a technology must “merely be capable of substantial noninfringing uses” to avoid constructive knowledge. See *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 442 (1984).

did nothing to stop it.⁶⁶ Absent this specific knowledge, generalized and background knowledge of infringement is insufficient to support liability.

Actual knowledge of specific infringement is therefore a serious threat to the developer of technology. Service providers can derive this actual knowledge from the apparatus that they use to manage and control their sites. For example, Napster and Grokster gathered information about what their customers were downloading in order to manage their networks, and were held liable as a result.⁶⁷ If an ISP is aware of specific acts of copyright infringement, then courts have determined that the ISP can be held liable for users' copyright violations.⁶⁸ Knowledge is indeed power for an ISP; but knowledge of infringing acts can also yield contributory liability for bad acts by users.

Game gods use many of the same informational tools to manage virtual worlds that Web 2.0 ISPs use. Game gods track economic transactions, parse chat logs, and log IP addresses. They wish to know what, where, when, how, and how often their players are doing the things they are doing. This knowledge is one of the primary sources of a god's ability to govern; however, that very knowledge can be an Achilles heel. If game gods come to have actual, direct knowledge of specific infringing acts, courts may deem them contributorily liable for those infringing activities.

d. *Control Under the Digital Millennium Copyright Act*

Under the legal regime set out above, ISPs were liable if they attempted to exercise control to stop infringement, and were liable if they did not. Congress intervened to carve out a narrow exception: ISPs would be protected from claims of vicarious and contributory infringement if they exercised their ability

⁶⁶ See *Napster*, 239 F.3d at 1021.

⁶⁷ Napster allowed users to upload a list of song titles to a centralized server. Grokster, in contrast, was decentralized, with no master list of copyrighted material. However, the court found:

[I]t is uncontested that [Grokster and Streamcast] are aware that users employ their software primarily to download copyrighted files, even if the decentralized . . . networks fail to reveal which files are being copied, and when. From time to time, moreover, the companies have learned about their users' infringement directly, as from users who have sent e-mail to each company with questions about playing copyrighted movies they had downloaded, to whom the companies have responded with guidance.

Grokster, 545 U.S. at 923.

⁶⁸ Indeed, in *Napster*, the district court found actual knowledge in the form of business memos emphasizing "the need to remain ignorant of users' real names and IP addresses since they are exchanging pirated music." *Napster*, 239 F.3d at 1020 n.5 (internal quotation marks omitted). In *Grokster*, the court found that Grokster and StreamCast specifically targeted their advertisements at Napster users, while the file-sharing pioneer was embroiled in legal troubles. See *Grokster*, 545 U.S. at 939.

to control on behalf of third-party owners of intellectual property.⁶⁹ Digital Millennium Copyright Act (“DMCA”) subsections 512(a) and (c) attempt this balance.⁷⁰ These safe harbors permit ISPs to take action to limit infringers, while avoiding liability for acting to control the content, if certain standards are met.⁷¹

Section 512(a) protects ISPs that act merely as neutral conduits for information. To qualify for the safe harbor, ISPs must not themselves be the source of, or exercise control over, the transmitted information. The statute expresses this requirement in five conditions. First, a third party must initiate the transfer.⁷² Next, the transmission must be automatic, without the service provider selecting the material to be sent.⁷³ The service provider also may not select the recipient.⁷⁴ No copy of the material may be kept by the ISP longer than is necessary,⁷⁵ and no modification of the content may be made.⁷⁶ If an ISP meets these standards, it is protected from claims of direct or secondary copyright infringement based on the infringing acts of its users.

Interference with the transmission of content strips the ISP of passive conduit protection. A conduit is protected because it does not exercise any control. Telephone companies do not, for example, screen telephone calls for potentially infringing, defamatory, or even criminal conversations. They are protected precisely because they do not control what their users say or do over the telephone lines. Similarly, if an ISP were to begin choosing what content is transmitted from game client to server or from one user to another – as a game god might – they would then lose the DMCA conduit shield, exposing them to the secondary liability regime described above.

Whereas § 512(a) governs liability for transmitting infringing content, § 512(c) provides a shield for conforming ISPs that store infringing content.⁷⁷ Section 512(c) first incorporates the control standard of vicarious liability, limiting liability only if the ISP “does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.”⁷⁸ Further, § 512(c) incorporates the knowledge component of the contributory liability standard,

⁶⁹ See 17 U.S.C. § 512(a), (c) (2006) (limiting the liability for copyright infringement by service providers engaged in transitory network communications and information storage at the direction of users, respectively).

⁷⁰ See *id.*

⁷¹ See *id.*

⁷² *Id.* § 512(a)(1).

⁷³ *Id.* § 512(a)(2).

⁷⁴ *Id.* § 512(a)(3).

⁷⁵ *Id.* § 512(a)(4).

⁷⁶ *Id.* § 512(a)(5).

⁷⁷ See § 512(c)(1)(B).

⁷⁸ See *id.*

following the *Netcom* and *Sony* precedents.⁷⁹ Section 512(c) draws a line between an ISP that knows in the abstract that some violations will necessarily occur, and an ISP that has or should have actual knowledge of specific copyright violations.⁸⁰

The more control an ISP exercises over data posted by users, the more likely it is to meet the threshold of control plus financial benefit, or actual knowledge of infringement. Conversely, should an ISP exercise less dominion over the data posted by its users, it can only be less likely to be found liable. If an ISP has no knowledge of infringement, the burden falls on the owner of the intellectual property to send notice that the data is infringing and should be removed.⁸¹ Only once this notice is received is the ISP required to take the content down.⁸² This simple standard exists not to constrain ISPs but to protect them.⁸³ Abandoning this safe harbor is a very risky move.

The pending lawsuit against YouTube by content-provider Viacom demonstrates the risk companies take in asserting control over their customers' actions. In early 2007, Viacom sued YouTube, alleging that YouTube had failed to prevent YouTube users from posting infringing videos.⁸⁴ The videos allegedly consisted of entire television shows or movies owned by Viacom.⁸⁵ Viacom sent YouTube 160,000 DMCA takedown notices, with which YouTube complied.⁸⁶ However, most clips were reposted promptly by YouTube users.⁸⁷ Viacom then brought suit against YouTube for one billion

⁷⁹ See *supra* notes 41-43, 65 and accompanying text.

⁸⁰ See § 512(c)(1)(A)(ii) (limiting liability for a service provider who "in the absence of such actual knowledge [of infringing activity], is not aware of facts or circumstances from which infringing activity is apparent").

⁸¹ Indeed, the DMCA expressly outlines appropriate and legally recognized methods of informing the operator of the infringing activity and requesting the content be removed or blocked. See *id.* § 512(c)(3).

⁸² *Id.* § 512(c)(1)(C) (providing safe-harbor protection only if the service provider, upon notification, "responds expeditiously to remove, or disable access to, the material that is claimed to be infringing").

⁸³ ISPs do not need to spend enormous resources poring through data to search for protected content. They need only have systems in place for removal when a copyright holder notifies them of the infringing activity.

⁸⁴ *Viacom Sues Google over YouTube Video Clips*, N.Y. TIMES, Mar. 13, 2007, <http://www.nytimes.com/2007/03/13/business/13wire.viacom.html>.

⁸⁵ See *YouTube Law Fight 'Threatens Net,'* BBC NEWS, May 27, 2008, <http://news.bbc.co.uk/2/hi/technology/7420955.stm> (last visited Mar. 7, 2009) ("[Viacom] said it had identified more than 150,000 such abuses which included clips from shows such as South Park, SpongeBob SquarePants and MTV Unplugged.").

⁸⁶ See OUT-LAW.com, *Viacom's YouTube Lawsuit Could Test Limits of DMCA*, REGISTER (London), Mar. 14, 2007, http://www.theregister.co.uk/2007/03/14/viacom_youtube_lawsuit_dmca.

⁸⁷ See *id.*

dollars, alleging direct, contributory, and vicarious copyright infringement.⁸⁸ YouTube answered, *inter alia*, that the copyright infringement claims were barred by § 512 of the DMCA.⁸⁹

Viacom's complaint repeatedly linked YouTube's control over its site, customers, and content directly to claims that YouTube was liable.⁹⁰ Viacom asserted that "YouTube has the right and ability to control the massive infringement on its site";⁹¹ that "the infringement is being committed on YouTube's own website, which Defendants control, not on other websites controlled by others";⁹² that "YouTube has reserved to itself the unilateral right to impose Terms of Use";⁹³ that "YouTube has the power and authority to police what occurs on its premises";⁹⁴ and that YouTube "reserves and exercises the unfettered right to block or remove any video."⁹⁵ Viacom also raised the ownership issue, noting that "YouTube also demands that users grant YouTube a 'worldwide . . . license to use, reproduce, distribute, prepare derivative works of, display, and perform' the videos they add to YouTube's library."⁹⁶

The examples that Viacom selected depend on the control/liability principle. For example, Viacom's amended complaint targeted the level of control that YouTube exerted via filtering.⁹⁷ Viacom asserted that YouTube took an active role in selecting YouTube content, via YouTube's filters.⁹⁸ Viacom pointed out that YouTube successfully filters out pornographic material, and alleged that by doing so, YouTube had exercised sufficient control over content to abandon the DMCA safe harbor.⁹⁹ Viacom also claimed that YouTube has filtered other material, on behalf of companies that have granted licenses to YouTube.¹⁰⁰

⁸⁸ First Amended Complaint for Declaratory and Injunctive Relief and Damages and Demand for Jury Trial at 5, 19-28, *Viacom Int'l Inc. v. YouTube, Inc.*, 540 F. Supp. 2d 461 (S.D.N.Y. 2008) (No. 1:07-cv-02103), 2008 WL 2062868.

⁸⁹ Defendants' Answer to First Amended Complaint and Demand for Jury Trial at 10, *Viacom*, 540 F. Supp. 2d 461 (No. 1:07-cv-02103), 2008 WL 2260018.

⁹⁰ First Amended Complaint, *supra* note 88, at 27.

⁹¹ *Id.* at 15.

⁹² *Id.*

⁹³ *Id.*

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ *Id.* (quoting YouTube's Terms of Use).

⁹⁷ *Id.* at 18-19 (alleging that YouTube's content-filtering policy preferentially protected its business partners from copyright infringement).

⁹⁸ *Id.* ("Until recently, it was YouTube's policy . . . to use filtering technology to identify and remove copyrighted works for companies that grant licenses with YouTube, but not for companies that declined to grant licenses on YouTube's terms.")

⁹⁹ *See id.* at 15, 27.

¹⁰⁰ *See id.* at 18-19.

Viacom's complaint further attempted to use concepts of control to preempt YouTube's argument that it is shielded by § 512. For example, Viacom claimed that YouTube copies the videos onto its own servers and then publicly performs the videos by streaming them to users' computers.¹⁰¹ Viacom alleged, therefore, that the copyright infringement happened "on YouTube's own website, which is operated and controlled by Defendants, not users."¹⁰²

Although these arguments have varying degrees of legal viability, their thrust is clear: to succeed, Viacom must mine the record for instances in which YouTube exercised control over the infringing content such that YouTube abandoned § 512 protections. The pending question is whether YouTube indeed possessed – and failed to exercise – control over the actions of its users such that it will be denied DMCA safe harbor protection. YouTube's business model hangs by the thread of whether it has properly gauged the balance of control and liability.

2. Control and Trademark Infringement

Gods risk secondary liability beyond copyright. A similar system of contributory and vicarious liability governs those companies who have the right and ability to control the trademark-infringing actions of their customers.¹⁰³ Virtual worlds often contain markets in which players may buy or sell virtual objects.¹⁰⁴ Sometimes those objects use real-world trademarks. For example, the virtual world Second Life has thriving markets in which one

¹⁰¹ See *id.* at 11.

¹⁰² *Id.* (contrasting YouTube's alleged misconduct with "simply providing storage space, conduits, or other facilities to users who create their own websites with infringing materials," activities that might qualify for a DMCA safe harbor).

¹⁰³ See *Vulcan Golf, LLC v. Google Inc.*, 552 F. Supp. 2d 752, 780 (N.D. Ill. 2008) ("Liability for vicarious trademark infringement 'requires a finding that the defendant and the infringer have an apparent or actual partnership, have authority to bind one another in transactions with third parties or exercise joint ownership or control over the infringing product.'" (quoting *Hard Rock Cafe Licensing Corp. v. Concession Servs.*, 955 F.2d 1143, 1150 (7th Cir. 1992))); *Tiffany Inc. v. eBay, Inc.*, 576 F. Supp. 2d 463, 506 (S.D.N.Y. 2008) (holding that eBay exercised sufficient control over the listing of Tiffany jewelry on its website to be liable for contributory infringement of the Tiffany trademark).

¹⁰⁴ The dollar value of the total supply of Second Life currency exceeded \$21 million in February 2009. Second Life, Economic Statistics (Feb. 26, 2009), http://s3.amazonaws.com/static-secondlife-com/reports/marketplace_stats/2009-02-26/LD_total_supply.xml; Second Life, L\$ Marketplace, [http://wiki.secondlife.com/wiki/L\\$Marketplace](http://wiki.secondlife.com/wiki/L$Marketplace) (last visited Mar. 9, 2009) ("Buyers will usually be able to buy approximately L\$ 260 [Linden dollars, the Second Life currency] for each \$1 plus a \$0.30 fee."). There is approximately \$10 million U.S. dollars in Second Life currency. More than a thousand players earned in excess of \$1,000 in February 2009, half of whom generated over \$2,000 a month. Second Life, Economic Statistics (Mar. 7, 2009), http://s3.amazonaws.com/static-secondlife-com/reports/marketplace_stats/2009-03-07/in_world_business_profits.xml.

may buy a virtual Gucci handbag, a virtual Rolex watch, virtual Ray-Ban sunglasses, or even a virtual Ferrari.¹⁰⁵ Rarely if ever are such sales made by licensed vendors of the trademarked goods.¹⁰⁶ The following Subsections discuss the control/liability principle in trademark law.

a. *Secondary Trademark Liability in Electronic Markets*

Game gods might look to recent cases on e-market liability for trademark infringement to predict how such issues will unfold for virtual worlds. E-marketing companies have come under considerable threat of liability based on the trademark-infringing acts of buyers and sellers. For example, auction giant eBay was recently found liable for nearly €40 million to plaintiffs LVMH and subsidiaries Christian Dior, Kenzo, Givenchy, and Guerlain by a Paris court for failing to stop sales of counterfeit products.¹⁰⁷ eBay users had used the site to sell fake LVMH-branded merchandise.¹⁰⁸ Further, eBay users sold legitimate luxury items, but were not licensed by the manufacturers of such items to do so.¹⁰⁹ Although not a traditional U.S. trademark cause of action, the French claim of culpable negligence for failure to stop the counterfeit and extracontractual sales would sound in trademark if brought in a U.S. court.¹¹⁰ The threat such a decision poses to Internet commerce is clear. The idea that ISPs ought to monitor and police the contractual licenses of their users is difficult to defend. But the relationship between control and liability is clear. The French court held that eBay both possessed and failed to exercise the ability to shut the counterfeit trades down.¹¹¹ eBay's control was sufficient to impose liability.

E-marketers may take some comfort in comparing the U.S. approach with the French approach. Under the U.S. approach, a defendant may be liable for contributory infringement of trademark if she induces another to infringe a trademark, or continues to supply a product or service to one whom she knows

¹⁰⁵ See Benjamin Duranske, *Rampant Trademark Infringement in Second Life Costs Millions, Undermines Future Enforcement*, VIRTUALLY BLIND, May 4, 2007, <http://virtuallyblind.com/2007/05/04/trademark-infringement-vws> [hereinafter Duranske, *Rampant Trademark Infringement*].

¹⁰⁶ *Id.* (estimating that between one and five percent of goods for sale in Second Life bear unlicensed trademarks).

¹⁰⁷ Michael Herman, *eBay Ordered to Pay €40m for Selling Luxury Fakes*, TIMES ONLINE (London), June 30, 2008, <http://business.timesonline.co.uk/tol/business/law/article4241267.ece>.

¹⁰⁸ *Id.*

¹⁰⁹ Ladka Bauerova, *eBay Is Ordered to Pay \$63 Million in LVMH Lawsuit (Update3)*, BLOOMBERG.COM, June 30, 2008, <http://www.bloomberg.com/apps/news?pid=newsarchive&sid=a1hiQyXAcPbk> (“The court ruled that EBay isn’t qualified to sell LVMH perfumes, which should be distributed only through selected retailers with trained staff.”).

¹¹⁰ See, e.g., *Tiffany Inc. v. eBay, Inc.*, 576 F. Supp. 2d 463, 469 (S.D.N.Y. 2008).

¹¹¹ See Bauerova, *supra* note 109.

or has reason to know is engaging in trademark infringement.¹¹² In the e-marketing context, the court in *Tiffany v. eBay* determined that where online retailer eBay had created a system for trademark holders to inform eBay of infringing sales, and under which eBay promptly de-listed such sales, eBay was not contributorily liable for trademark infringement.¹¹³ Under such a regime, it is the responsibility of the intellectual property holder to inform the e-marketer that customers were infringing; only then would the ISP have the duty to remove the proposed auction, or act to block the trade.¹¹⁴

But even in the United States, control has a significant impact on the analysis. The *Tiffany* court referenced the Ninth Circuit's oft-quoted determination in *Lockheed Martin Corp. v. Network Solutions, Inc.* that "[t]he relevant inquiry is . . . 'the extent of control exercised by the defendant over the third party's means of infringement.'"¹¹⁵ Thus, as one court recently noted, contributory trademark infringement depends on whether the defendant had "[d]irect control and monitoring of the instrumentality used by the third party to infringe the plaintiff's mark."¹¹⁶ Of course, the comforting converse is true: in the United States, companies that have ceded control over content are much less likely to be found contributorily liable.¹¹⁷

Which standard will prevail is an open question. Currently, European courts have become a clearinghouse for targeting U.S. e-commerce giants.¹¹⁸ But European courts will eventually be deciding the fate of European companies, and I predict that the current standards of monitoring that such courts impose will thus soften. For the time being, overbroad control remains a threat to companies in the European context and in many U.S. courts as well.

b. *Secondary Trademark Liability in Virtual Worlds: Marvel*

Trademark issues have already begun to impact virtual worlds. A significant portion of *Marvel Enterprises, Inc. v. NCsoft Corp.* dealt with

¹¹² *Inwood Labs., Inc. v. Ives Labs., Inc.*, 456 U.S. 844, 854 (1982).

¹¹³ *Tiffany*, 576 F. Supp. 2d at 518.

¹¹⁴ *Id.*

¹¹⁵ *Id.* at 505 (quoting *Lockheed Martin Corp. v. Network Solutions, Inc.* 194 F.3d 980, 983 (9th Cir. 1999)).

¹¹⁶ See *Louis Vuitton Malletier S.A. v. Akanoc Solutions, Inc.*, 591 F. Supp. 2d 1098, 1111 (N.D. Cal. 2008) (citing *Lockheed Martin Corp.*, 194 F.3d at 983) (applying the "extent of control" theory to find contributory trademark infringement).

¹¹⁷ See, e.g., *Tiffany*, 576 F. Supp. 2d at 505; *SB Designs v. Reebok Int'l, Ltd.*, 338 F. Supp. 2d 904, 913 (N.D. Ill. 2004); *Fare Deals, Ltd. v. World Choice Travel.com, Inc.*, 180 F. Supp. 2d 678, 689 (N.D. Md. 2001).

¹¹⁸ See Herman, *supra* note 107 ("The French Courts have historically taken a very tough line against online infringements, particularly where large overseas companies are said to be at fault." (quoting David Wilkinson, Partner, Intellectual Property and Dispute Resolution, Stevens & Bolton, LLP)).

trademark liability.¹¹⁹ In the case, NCsoft narrowly escaped the application of contributory and vicarious trademark liability. The court held that secondary liability of the game operator could not obtain because primary liability of game users for direct infringement had not been proven.¹²⁰ Players of City of Heroes were not liable for direct trademark infringement because the infringing superhero avatars were not used in commerce.¹²¹ The court's premise seems counterfactual, given the robust trade in City of Heroes game accounts.¹²² Further, it is worth asking whether a game god of a world in which avatars, accounts, items, and land were routinely traded would be immune under such a theory. The *Marvel* decision does not therefore offer gods much protection against a finding that they are contributorily or vicariously responsible for the trademark infringement of their users. If a game god has the right or ability to control the actions of its users, then it may well be liable for their infringing acts, as long as such acts are considered uses in commerce.

3. Control and Net Neutrality

The mechanics of the DMCA § 512(a) safe harbor for passive information conduits underlie a broader debate about net neutrality and virtual worlds. Net neutrality is yet another application of the control/liability principle.¹²³ Companies that carry data without interfering or selecting the content are rewarded and protected under a net neutrality paradigm; companies that interfere with data distribution open themselves to risk.¹²⁴ For example, the FCC has recently begun proceedings against internet service provider

¹¹⁹ *Marvel Enters., Inc. v. NCsoft Corp.*, 74 U.S.P.Q.2d 1303, 1305 (C.D. Cal. 2005).

¹²⁰ *Id.* at 1308.

¹²¹ *Id.* (“Plaintiff has not alleged that the *game users* are using these names in commerce in connection with any sale or advertising of goods and services.”).

¹²² Many websites offer to sell or buy City of Heroes character accounts. *See, e.g.*, Gamepal.com, City of Heroes Store, <http://www.gamepal.com/gamestore/?game=coh> (last visited Mar. 9, 2009).

¹²³ Although the term was coined in 2003, *see* Tim Wu, *Network Neutrality, Broadband Discrimination*, 2 J. TELECOMM. & HIGH TECH. L. 141, 145 (2003), the principle predates it. Net neutrality combats the desire of telecommunications companies to stratify, or tier, network bandwidth, giving priority and higher speeds to some traffic and retarding and slowing other forms of data. *See, e.g.*, 47 U.S.C. § 202(a) (2000) (making it unlawful for a public telecommunications company to “give any undue or unreasonable preference or advantage to any particular person, class of persons, or locality, or to subject any particular person, class of persons, or locality to any undue or unreasonable prejudice or disadvantage”).

¹²⁴ *See* Joe Fay, *FCC Chief Wants to Throttle Comcast*, REGISTER (London), July 11, 2008, http://www.theregister.co.uk/2008/07/11/comcast_fcc_martin.

Comcast, claiming that Comcast has unfairly throttled some traffic and privileged other traffic on its network.¹²⁵

This Article does not take a position on network neutrality directly. Rather, I argue here that the claims of game gods – that they may control transmission of information at their discretion – are shortsighted. Virtual worlds are particularly dependent on maintaining network neutrality. If game gods succeed in arguing that they may control, select, throttle, or deny access to their networks entirely at their discretion, they are likely to find that traditional ISPs will use those rules against them. Virtual worlds are bandwidth-intensive applications. Virtual-world players are residents of the infamous “last mile” of wire, which is more costly for ISPs to reach.¹²⁶ Suppose an ISP moved to hourly metering of Internet usage, or, worse, charging based on bandwidth usage, as several are currently proposing to do.¹²⁷ This would likely be a severe blow to the immersive style of play enjoyed by virtual world players. With metered use, one can easily imagine that virtual-world play would drop off, and a large portion of the value of the virtual-world product would likely disappear.

Network neutrality relies on the many subsidizing the few. Most consumers pay for far more Internet access than they use on a regular basis.¹²⁸ High bandwidth users can pay for the same connection and utilize it fully without significantly affecting the network because they are being subsidized by regular users.¹²⁹ Virtual worlds are subsidized heavily by network neutrality, because they provide large amounts of content to individual consumers who are unlikely to pay the full costs for the bandwidth they use. Game gods ought to be cautious about claiming that they can and should control traffic over their networked virtual worlds. Those arguments work much better when used by ISPs to throttle players of virtual worlds. Game gods may therefore find their current pro-control approach to be deeply counterproductive.

¹²⁵ *Id.* (recounting an FCC investigation of whether Comcast had discriminated against users of high bandwidth peer-to-peer file transfer services).

¹²⁶ See Antonia M. Apps & Thomas M. Dailey, *Non-Regulation of Advanced Internet Services*, 8 GEO. MASON L. REV. 681, 710 (2000) (“Facilities serving the last mile (those of the telephone companies and cable operators) are expensive on a per customer basis, with high maintenance costs and linear growth in use.”).

¹²⁷ See Brian Stelter, *To Curb Traffic on the Internet, Access Providers Consider Charging by the Gigabyte*, N.Y. TIMES, June 15, 2008, at A1 (reporting that Time Warner Cable added surcharges for customers who exceeded their bandwidth limit and that AT&T was “considering pricing based on data volume”).

¹²⁸ *See id.*

¹²⁹ *Id.* (reporting that “5 percent of [Time Warner’s] customers use more than 50 percent of the network’s overall capacity”).

B. *Control in the Common Law*

Thus far I have examined the God Paradox as a matter of U.S. intellectual property law. However, other cases cover basic common law causes of action, sounding in contract, tort, or property law. The following Subsections detail the challenges game gods face in responding to claims based on common law causes of action, and discover that the control/liability principle remains the same. At common law, a game god that attempts to avoid liability by retaining a lot of control will instead risk increased liability.

At the outset, it is worth noting that § 230 of the Communications Decency Act (“CDA”) provides total immunity to ISPs for nearly all state law causes of action that arise out of the actions of users of an ISP’s service.¹³⁰ Intellectual property and federal criminal claims are excluded from this protection.¹³¹ Although CDA immunity originally grew out of the defamation context,¹³² CDA immunity has since been expanded to provide immunity to ISPs for all tort claims and many contract claims that are based on harms caused by third parties.¹³³

This does not mean, however, that game gods can expand control without risking liability. First, the CDA does not protect game gods from consequences of their own wrongdoing.¹³⁴ Moreover, there are gaps in the CDA armor. This Section discusses the changing case law of control and liability while keeping an eye on CDA immunity. It concludes that in the area of the common law, as elsewhere, game gods are needlessly increasing their potential for liability by exerting unnecessary control over the communications media they oversee.

1. The Communications Decency Act and Control

Because the CDA provides such strong immunity to game gods, it is worth discussing first. CDA § 230 grew out of the defamation context. Prior to the CDA, the basic defamation regime held a publisher liable if she exercised any control over the defamatory content, even if that control protected readers or users. “A primary publisher, such as an author or a publishing company, is

¹³⁰ 47 U.S.C. § 230(c) (2000) (“No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”).

¹³¹ *Id.* § 230(e)(1)-(2).

¹³² *See infra* Part II.B.1 (discussing the origins of the CDA).

¹³³ *See Zeran v. Am. Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997) (“[L]awsuits seeking to hold a service provider liable for its exercise of a publisher’s traditional editorial functions – such as deciding whether to publish, withdraw, postpone or alter content – are barred.”); *Doe v. SexSearch.com*, 502 F. Supp. 2d 719, 727 (N.D. Ohio 2007) (concluding that the CDA provided immunity from a contract claim that defendant SexSearch failed to keep minors from becoming registered users).

¹³⁴ *See, e.g., Mazur v. eBay*, No. 07-03967, 2008 U.S. Dist. LEXIS 16561, at *5 (N.D. Cal. Mar. 4, 2008).

presumed to know the content of the published material, has the ability to control the content of the publication, and therefore generally is held liable for a defamatory statement”¹³⁵ In addition, even “one who repeats or otherwise republishes a libel is subject to liability as if he had originally published it.”¹³⁶

In *Stratton Oakmont, Inc. v. Prodigy Services Co.*, this regime was applied to find that Internet host Prodigy was liable for failing to edit out defamatory content that appeared on its bulletin boards.¹³⁷ ISPs were extremely worried that they would be tasked with monitoring all content on the Internet, under pain of liability. Congress responded with § 230 of the CDA. This section provides that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.”¹³⁸ And, as an important corollary, Congress protected attempts to give customers the protection they desire from violence or obscenity by granting immunity for instituting such protections.¹³⁹

But this immunity is not absolute. The CDA only blocks liability for content provided by someone else.¹⁴⁰ A game god or ISP is liable for publishing defamatory content if it exercises such control over the content that it is, itself, functionally the source of the defamatory material.¹⁴¹ There are two broad theories of liability: a game god may so alter content that the content becomes the game god’s product, or it may distribute the content in a forum in which the content was never intended to be released, and thus count as the primary author of the content. If a game god owns the content and intentionally selects, alters, or displays content created by its users, then the information is no longer provided “by another information content provider.”¹⁴² This makes sense: a blogger would not be immune under this provision for repeating another’s statements as her own. Similarly, a game god may become liable for providing the information itself if it publishes the

¹³⁵ *Grace v. eBay Inc.*, 16 Cal. Rptr. 3d 192, 198 (Ct. App. 2004) (citing RESTATEMENT (SECOND) OF TORTS § 581(1) cmt. c (1977)).

¹³⁶ *Stratton Oakmont, Inc. v. Prodigy Servs. Co.*, 63 U.S.L.W. 2765, 2766 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, Communications Decency Act, 47 U.S.C. § 230 (2000).

¹³⁷ *Id.* (holding that while “[c]omputer bulletin boards should generally be regarded in the same context as bookstores” and not subject to liability for defamation, Prodigy was liable because it both claimed to exercise control over its content and in fact exercised such control).

¹³⁸ 47 U.S.C. § 230(c)(1).

¹³⁹ *Id.* § 230(c)(2).

¹⁴⁰ *Id.* § 230(c)(1) (limiting liability only for “information provided by another information content provider”).

¹⁴¹ *See id.* § 230(f)(3) (“The term ‘information content provider’ means any person or entity that is responsible, *in whole or in part*, for the creation *or development* of information” (emphasis added)).

¹⁴² *Id.* § 230(c)(1).

information in a venue in which the author never intended the work to be seen.¹⁴³

The line between providing content and managing content is blurred. For example, in *Batzel v. Smith*, Smith sent an email to Cremers, hypothesizing that Batzel was the descendant of Nazis, and had stolen artwork in her home.¹⁴⁴ Cremers forwarded the email with light edits to a listserv.¹⁴⁵ The question before the court was whether Cremers was himself the provider of the email, or whether he could take shelter under § 230. The court formulated a two-part test: first, the court considered whether the content was so altered by Cremers as to make him the original provider of the content; and second, whether the fact that Smith did not intend the email to be further propagated made Cremers the true provider of the content.¹⁴⁶ The court determined that Cremers's light edits did not make him the original provider of the content, and thus Cremers benefitted from CDA protection.¹⁴⁷

But if Cremers had editorialized in the emails, rather than edited, the outcome might have been quite different. In another email-forwarding case, *Doe v. City of New York*, Bruce Tefft, a counterterrorism advisor, was stripped of CDA protection.¹⁴⁸ Tefft forwarded daily briefings to antiterrorism officers, including the plaintiff.¹⁴⁹ Tefft allegedly did not merely forward the briefings, but also editorialized against Muslims and Arabs in the forwarded emails.¹⁵⁰ The plaintiff, a Muslim and Arab-American, was offended at the commentary, and after first attempting to stop the commentary through channels, eventually sued. The court determined that Tefft was himself a content provider because of his editorialization, and further, that he was not a user of an interactive computing service merely because he used an email system.¹⁵¹

The line between content provider and content transmitter also proves slippery when one considers the power of interactive computing services to

¹⁴³ This result depends on the definition of "provided" in § 230(c)(1). If an information content provider fairly expects his statement to be, for example, kept in confidence, and the interactive computer service breaches that expectation, then the service has "provided" the statement and thereby becomes its publisher. *See Batzel v. Smith*, 333 F.3d 1018, 1032-36 (9th Cir. 2003) (denying CDA immunity to interactive computing services that "intentionally post material they knew was never meant to be put on the Internet" because such material was not "provided" to them within the meaning of § 230(c)(1)).

¹⁴⁴ *Id.* at 1020-21.

¹⁴⁵ *Id.* at 1022.

¹⁴⁶ The court found that (1) Cremers did not exercise sufficient editorial control to be deemed the publisher of the material, and (2) if Cremers reasonably assumed the email was for publication, he received immunity. If, however, he could not have assumed such, the information was not "provided" to him and he was liable. *Id.* at 1031-35.

¹⁴⁷ *Id.* at 1031.

¹⁴⁸ *Doe v. City of New York*, 583 F. Supp. 2d 444, 447 (S.D.N.Y. 2008).

¹⁴⁹ *Id.* at 446.

¹⁵⁰ *See id.*

¹⁵¹ *Id.* at 449.

control what data is contributed by users. For example, users of the online forum craigslist sued the service, claiming that craigslist was the publisher of user-posted advertisements that listed “NO MINORITIES” or “No children” as requirements.¹⁵² If craigslist were the publisher, it would be liable under the Fair Housing Act.¹⁵³ The Seventh Circuit held that craigslist was eligible for CDA safe harbor status shielding it from liability under the FHA for hosting advertisements that indicated a preference for protected classes of race, sex, or family status.¹⁵⁴

In the decision, Judge Easterbrook noted: “Online services are in some respects like the classified pages of newspapers, but in others they operate like common carriers such as telephone services, which are unaffected by [the FHA] because they neither make nor publish any . . . advertisement.”¹⁵⁵ Easterbrook recognized that the practical nature of private carriers – like ISPs, Federal Express, or UPS – did not reasonably permit them to monitor content and censor it for their own purposes.¹⁵⁶ Where these companies had declined to exercise control, Easterbrook understood that their liability ought to be limited.

But a small increase in control over content may result in a different outcome. Internet website Roommates.com operated a website permitting users to list spare rooms or seek out roommates.¹⁵⁷ To create user profiles, users entered their race, sex, and other sensitive data, which was then available as search classifications by potential roommates.¹⁵⁸ Additionally, in their listings users could specify preferences for each of those classifications.¹⁵⁹ This enabled users to discriminate against one another. A critical fact was that subscribers could not refuse to answer questions based on those classifications if they wanted to use the service.¹⁶⁰ The Ninth Circuit held that the classifications and search tools created by Roommates.com were not entitled to CDA protection.¹⁶¹ In effect, the creation of the classification system

¹⁵² Chi. Lawyers’ Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666, 668 (7th Cir. 2008).

¹⁵³ *Id.* (“[The FHA] applies to these ads without constitutional cavil. Courts regularly enforce the statute against newspapers and other publishers.”).

¹⁵⁴ *Id.* at 671 (holding that craigslist “is not the author of the ads and could not be treated as the ‘speaker’ of the posters’ words, given § 230(c)(1)”).

¹⁵⁵ *Id.* at 668.

¹⁵⁶ *Id.*

¹⁵⁷ Fair Hous. Council of San Fernando Valley v. Roommates.com, 521 F.3d 1157, 1161 (9th Cir. 2008).

¹⁵⁸ *Id.* at 1161.

¹⁵⁹ *Id.*

¹⁶⁰ *Id.* at 1165 (“The CDA does not grant immunity for inducing third parties to express illegal preferences. Roommate’s own acts – posting the questionnaire and requiring answers to it – are entirely its doing and thus section 230 of the CDA does not apply to them. Roommate is entitled to no immunity.”).

¹⁶¹ *Id.* at 1167.

constituted direct content creation by Roommates.com. Even though the data that was placed into the search categories was by the users, the actual categories themselves were deemed content created by Roommates.com, and thus CDA protection did not apply.¹⁶²

If game gods are liable as content providers when they exercise control over the format in which data can be entered and searched, gods with worlds that have a significant social networking component will risk significant exposure despite the CDA. Defamation and racial and sexual harassment have been present in virtual worlds for years.¹⁶³ For example, there is significant distrust of Chinese players within virtual worlds because of the gold farming trade.¹⁶⁴ Western players resent Chinese players because Westerners feel the gold trade disrupts the economy of the virtual worlds and destroys the level playing field that players enjoy when they enter a virtual world.¹⁶⁵ Because of this, Western players often target Chinese players for in-world attacks, and make them the subject of rabid message board posts.¹⁶⁶ Direct and indirect harassment of Chinese players is common.¹⁶⁷ If the virtual world requires the input of information that facilitates actionable harassment, the game god risks having the CDA safe harbor revoked.

In short, § 230 does much to absolve game gods of the need to monitor the statements of their users. But even under § 230, there is a direct relationship between control and liability. If game gods merely repost or edit third-party content, then there is no liability. But if the game gods editorialize or recontextualize the content, then liability may result.

¹⁶² *Id.* at 1166 (“By requiring subscribers to provide the information as a condition of accessing its service, and by providing a limited set of pre-populated answers, Roommate becomes much more than a passive transmitter of information provided by others; it becomes the developer, at least in part, of that information.”).

¹⁶³ See Julian Dibbell, *A Rape in Cyberspace, or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society*, VILLAGE VOICE, Dec. 21, 1993, <http://www.villagevoice.com/2005-10-18/specials/a-rape-in-cyberspace/>.

¹⁶⁴ Gold farming is the practice of playing a game to generate virtual items for sale to others, sometimes for real money. The practice is controversial in virtual worlds. See Julian Dibbell, *The Life of the Chinese Gold Farmer*, N.Y. TIMES MAG., June 17, 2007, at 36 (“Real-money trading harms the game, they argue, because the overheated productivity of gold farms and other profit-seeking operations makes it harder for beginning players to get ahead. Either way, the sense of a certain economic injustice at work breeds resentment.”).

¹⁶⁵ See *id.* (describing how American World of Warcraft players filed a class action lawsuit against a virtual gold seller).

¹⁶⁶ See *id.*

¹⁶⁷ *Id.* (“Nick Yee, an M.M.O. scholar based at Stanford, has noted the unsettling parallels (the recurrence of words like ‘vermin,’ ‘rats’ and ‘extermination’) between contemporary anti-gold-farmer rhetoric and 19th-century U.S. literature on immigrant Chinese laundry workers.”).

2. Contract Law

There are two central issues for game gods to consider in their contracts. First, the CDA does not protect them from claims based on the gods' own promises or assertions. Second, the more control that game gods claim in their EULAs, the more likely it is that the EULA will be held unconscionable. This Subsection explores these two issues in turn.

Internet hosts of all stripes, game gods included, exercise control through Terms of Service (TOS) or EULAs that dictate how their customers must use the website, service, or world. The first question raised here is when those "social control" provisions might result in liability for the game god.

The CDA has been extended to bar some contractual claims against interactive computer service providers where the contract claim is based on information provided by a third party. Thus, in *John Doe v. SexSearch.com*, the plaintiff alleged the defendant had failed to stop a minor from registering with the sex service.¹⁶⁸ The plaintiff met the minor through SexSearch, arranged a meeting, had sexual relations with the minor, and went to jail as a result.¹⁶⁹ The plaintiff carefully pled to avoid CDA § 230, by arguing that he was only suing based on SexSearch's broken promise that all members of the site were "18+."¹⁷⁰ The court determined that CDA § 230 immunity extended well beyond the defamation – and even the tort – context.¹⁷¹ The court noted that "the CDA grants immunity from all civil liability, except for the few exceptions expressly laid out in the statute."¹⁷²

But this does not mean that game gods cannot suffer liability for their own affirmative representations that an online environment will be safe. In *Mazur v. eBay*, Michele Mazur sued eBay for its promises that online auctions conducted by third-party auctioneers under eBay's Live Auction program would be "safe."¹⁷³ eBay defended under § 230, claiming that the program was unsafe solely because of the actions of Hot Jewelry Auctions, the Live Auction auctioneer.¹⁷⁴ The court rejected eBay's § 230 defense and noted that "[t]he CDA does not immunize eBay for its own fraudulent misconduct."¹⁷⁵ The court agreed that the CDA blocked liability for eBay's failure to stop

¹⁶⁸ *Doe v. SexSearch.com*, 502 F. Supp. 2d 719, 722 (N.D. Ohio 2007).

¹⁶⁹ *Id.*

¹⁷⁰ *Id.* at 723.

¹⁷¹ *See id.* at 727 (holding that SexSearch had immunity under the CDA against the claim of permitting a minor to use the service).

¹⁷² *Id.*

¹⁷³ *See Mazur v. eBay*, No. 07-03967, 2008 U.S. Dist. LEXIS 16561, at *5 (N.D. Cal Mar. 4, 2008).

¹⁷⁴ *Id.* at *25-26.

¹⁷⁵ *Id.* at *28.

HJA's bad acts, but added that it did not immunize eBay from claims based on eBay's assertions that the live auctions were "safe."¹⁷⁶

Similarly, the Ninth Circuit determined in *Barnes v. Yahoo!, Inc.* that CDA § 230 did not immunize Yahoo for claims based on the contract theory of promissory estoppel.¹⁷⁷ *Barnes* was a core case for CDA immunity: the plaintiff sued because Yahoo failed to take down a false and explicit profile created by plaintiff's vengeful ex-boyfriend.¹⁷⁸ There was a twist, however: a Yahoo employee promised the plaintiff that the material would be taken down. The court found that although CDA § 230 barred plaintiff's negligent undertaking claim, the promissory estoppel claim was not so barred.¹⁷⁹

The second problem for game gods is that if they claim untrammelled control in the form of rights to terminate or ban users, they may find that their contracts are voided by courts as unconscionable. The central legal instrument of game god control is the EULA. These agreements have two basic control functions. First, they set out a very basic set of rules related to the use of intellectual property, whether it belongs to the god, or to the users (e.g., in a "Web 2.0" system) or both.¹⁸⁰ EULAs also set forth a system of social rules that are intended to order relationships between players.¹⁸¹ For infractions of both sorts of rules, EULAs reserve for the gods the most common and important sanction available to game developers: the ban.¹⁸² Thus, the EULA sets forth the legal basis for the exercise of the technological powers that the god may employ. If a player breaches the EULA's terms, the game god claims the authority to terminate the player's account and delete the accumulated virtual assets acquired by the player.¹⁸³

EULAs contain further legal protections for game gods. For example, most EULAs contain arbitration provisions.¹⁸⁴ Arbitration provisions permit a god to: limit the costs of litigation by limiting discovery; specify the location and

¹⁷⁶ *Id.* at *29 (holding that eBay's alleged misrepresentations may be actionable as fraud).

¹⁷⁷ *Barnes v. Yahoo!, Inc.*, No. 05-36189, 2009 WL 1232367, at *11 (9th Cir. May 7, 2009).

¹⁷⁸ *Id.* at *1-*2.

¹⁷⁹ *Id.* at *1, *8, *11.

¹⁸⁰ *See, e.g.*, Second Life, Terms of Service, *supra* note 19, §§ 3.1-4.

¹⁸¹ *See, e.g., id.* §§ 4.1-4.; Second Life, Community Standards, *supra* note 22.

¹⁸² *See, e.g.*, Second Life, Terms of Service, *supra* note 19, § 2.6 ("Linden Lab has the right at any time for any reason or no reason to suspend or terminate your Account, terminate this Agreement, and/or refuse any and all current or future use of the Service without notice or liability to you.").

¹⁸³ *See, e.g., id.*

¹⁸⁴ Second Life's Terms of Service has optional arbitration, likely due to the *Bragg* opinion. *Id.* § 7.3; *see infra* notes 187-196 (discussing the *Bragg* opinion). *But see* World of Warcraft, Terms of Use Agreement § 19(B) (July 29, 2008), <http://www.worldofwarcraft.com/legal/termsofuse.html> (setting forth binding arbitration terms).

forum for resolution of disputes; and most importantly, block class-action treatment of customer complaints. Theoretically, arbitration provisions are liability-neutral provisions that simply order how disputes will be resolved. In practice, they are powerful shields that protect companies against consumer lawsuits.¹⁸⁵

If the game god asserts too much control over players' accounts in its EULA, it may find that a court will strip the liability-shielding elements of the contract away. EULAs are enforceable unless unconscionable. For a contractual provision to be unconscionable, a court must find that the given provision is both procedurally and substantively unconscionable: an unfair bargaining process yielding an unfair result.¹⁸⁶

Courts have already found some such provisions unconscionable. In *Bragg v. Linden Research, Inc.*, player Marc Bragg's Second Life account was frozen by Linden and all his virtual assets were confiscated.¹⁸⁷ Linden claimed Bragg had purchased virtual property through an exploit in the game, and therefore Linden suspended Bragg's account.¹⁸⁸ The property Linden seized included both assets Bragg had gained through the exploit as well as assets Bragg had legitimately purchased.¹⁸⁹ Bragg brought suit and moved to compel arbitration per its Terms of Service.

The court declared that the arbitration provision in the Second Life TOS was unconscionable.¹⁹⁰ The reasoning expressly relied on the powers that the game god had reserved to itself.¹⁹¹ In the TOS, Linden reserved the right to suspend or terminate accounts "at [its] sole discretion."¹⁹² Linden could confiscate funds or property "without notice or liability" to the player.¹⁹³ The court determined that because the god reserved to itself the power to unilaterally seize or destroy players' accounts, the arbitration provision was substantively

¹⁸⁵ See, e.g., Edward Wood Dunham, *The Arbitration Clause as Class Action Shield*, 16 FRANCHISE L.J. 141, 142 (1997) (stating that arbitration clauses are among the "strongest pieces of armor available" against class action litigation).

¹⁸⁶ See, e.g., *Discover Bank v. Superior Court*, 113 P.3d 1100, 1108 (Cal. 2005).

¹⁸⁷ *Bragg v. Linden Research, Inc.*, 487 F. Supp. 2d 593, 595 (E.D. Pa. 2007).

¹⁸⁸ *Id.* at 597.

¹⁸⁹ *Id.*

¹⁹⁰ *Id.* at 611 ("Taken together, the lack of mutuality, the costs of arbitration, the forum selection clause, and the confidentiality provision that Linden unilaterally imposes through the TOS demonstrate that the arbitration clause is not designed to provide Second Life participants an effective means of resolving disputes with Linden. Rather, it is a one-sided means which tilts unfairly, in almost all situations, in Linden's favor.")

¹⁹¹ The court found procedural unconscionability because: (1) "the TOS are a contract of adhesion"; (2) there were "no reasonably available market alternatives"; (3) "Linden buried the TOS's arbitration provision in a lengthy paragraph under the benign heading 'GENERAL PROVISIONS'"; and (4) "Linden . . . failed to make available the costs and rules of arbitration." *Id.* at 606-07.

¹⁹² *Id.* at 611.

¹⁹³ *Id.* at 608.

unconscionable for lack of mutuality.¹⁹⁴ The court struck the arbitration provision, leaving Linden vulnerable to suit in federal court.

As *Bragg* demonstrates, courts may be reluctant to give game gods unbounded and one-sided control over their worlds. The court couched its reasoning in the language of unconscionability of the arbitration agreement, but grounded its real analysis on the self-help power reserved and exercised before arbitration is ever invoked. The arbitration clause could have been unconscionable due to its prohibitive cost¹⁹⁵ or binding confidentiality.¹⁹⁶ However, by basing its analysis on Linden's unilateral power to suspend or revoke player accounts, the court revealed a different motivation: it believed Linden reserved too much control. And because of that control, the court stripped Linden of its contractual litigation shield.

3. Tort Liability

This Subsection examines the God Paradox in tort law. Here, as elsewhere, the more control a corporation exerts over its customers or the customers' content the greater the company's exposure to liability will be. The first Subsection will discuss the relationship between the scope of the control claimed by the company and the scope of the company's duty to prevent harm. The second Subsection will discuss specific cases in which companies have been held liable for negligently protecting their customers' data. Note that under CDA § 230, claims premised on the acts of third-party users of the service will not be actionable against the game god.¹⁹⁷

a. *Negligence*

Negligence is based on principles of duty, breach, and harm.¹⁹⁸ The scope of a game god's duty will depend on the scope of the god's undertaking. As one court succinctly noted, "[t]he extent of the undertaking defines the scope

¹⁹⁴ *Id.* at 611 ("[T]he TOS expressly allow Linden, at its 'sole discretion' and based on mere 'suspicion,' to unilaterally freeze a participant's account, refuse access to the virtual and real currency contained within that account, and then confiscate the participant's virtual property and real estate.").

¹⁹⁵ *Id.* at 609 (estimating the arbitration cost to be at least \$17,000 and possibly "as high as \$27,375").

¹⁹⁶ *Id.* at 610 ("[I]f the company succeeds in imposing a gag order on arbitration proceedings, it places itself in a far superior legal posture by ensuring that none of its potential opponents have access to precedent while, at the same time, the company accumulates a wealth of knowledge on how to negotiate the terms of its own unilaterally crafted contract.").

¹⁹⁷ *See supra* Part II.B.1; *see also* *Barnes v. Yahoo!, Inc.*, No. 05-36189, 2009 WL 1232367, at *8, *11 (9th Cir. May 7, 2009) (holding that Yahoo was immune to suit under CDA § 230 for negligent undertaking, but not immune to suit for failure to perform on its employee's promise to remove the plaintiff's false profile created by her ex-boyfriend).

¹⁹⁸ *See, e.g., Sport Supply Group, Inc. v. Columbia Cas. Co.*, 335 F.3d 453, 466 (5th Cir. 2003).

of duty, and a person is not liable for the negligent performance of a task he or she did not agree to assume.”¹⁹⁹ Thus, the question of whether a defendant has breached a duty will often depend on the scope of control that the defendant exercised over a given situation.

Moreover, when a party undertakes a duty, she may also be negligent for failing to carry out the duty when her undertaking increases the risk of harm, or decreases the chance of someone else (the counterparty included) performing the duty. The Good Samaritan rule is a good example. The rule states that there is no general duty to help passersby, but once a person begins to help, she is liable for any negligent harm she causes.²⁰⁰ The reasoning is that once a Good Samaritan begins helping, she decreases the chance that someone else will help. Thus, “[o]ne who undertakes . . . gratuitously . . . to render services to another . . . is subject to liability to the other for physical harm resulting from his failure to exercise reasonable care to perform his undertaking.”²⁰¹

It is not difficult to see how this basic relationship between the scope of the undertaking and the scope of negligence plays out in virtual worlds. When gods claim control over the entire world, they risk liability for negligently failing to exercise that control. When gods claim control over, and thus responsibility for, the protection of their customers’ data, gods risk liability for negligently failing to protect that data. Gods increase the scope of the duty they owe their customers when they increase the scope of the control they undertake. They doubly do so when their exercise of control prevents the customer from protecting herself, or reduces the chance that she will take necessary precautions. The following cases from the broader electronic context, as well as cases covering virtual worlds, may help to illustrate.

b. *Third Party Hacks*

Consider whether a game god might be liable for user accounts or personal information lost to hackers.²⁰² If those hackers exploit security flaws, game gods may be held liable because of the broad control they assert over their game servers. For example, companies risk liability for negligent failure to properly protect computer information within the company’s control. TJX, the parent corporation of clothing store T.J. Maxx, retained customers’ personal information on its computer systems. Hackers attacked the system through a security loophole over a period of months.²⁰³ The hackers eventually gained access to forty-six million credit card numbers.²⁰⁴ TJX is currently in the

¹⁹⁹ *Brock v. Richmond-Berea Cemetery Dist.*, 957 P.2d 505, 508 (Kan. 1998).

²⁰⁰ *See, e.g.*, RESTATEMENT (SECOND) OF TORTS § 323 (1965).

²⁰¹ *Id.*

²⁰² *Cursor Hackers Target WoW Players*, BBC NEWS, Apr. 5, 2007, <http://news.bbc.co.uk/2/hi/technology/6526851.stm>.

²⁰³ *See T.J. Maxx Data Theft Worse Than First Reported*, MSNBC.COM, Mar. 29, 2007, <http://www.msnbc.msn.com/id/17853440>.

²⁰⁴ *Id.*

process of settling the resulting class action for an estimated \$128 million, to cover reimbursements, attorneys' fees, identity theft insurance and reimbursement, and replacement of compromised drivers' licenses and other documentation.²⁰⁵

The risks are similar for game gods. Because game gods exercise total control over their virtual worlds, they may be liable for damage caused by their negligent failure to close loopholes that permit hacks. For example, in the Chinese case *Li Hongchen v. Beijing Arctic Ice*, a player spent two years and 10,000 RMB – approximately \$1,500 U.S. dollars – gathering virtual property within the Chinese game Red Moon.²⁰⁶ A hacker succeeded in stealing the items through the company's servers.²⁰⁷ At trial, the software company argued that the virtual world items had no real world value.²⁰⁸ The Beijing Intermediate Court nevertheless ruled that a game god was liable for failing to stop the hacking of a player's virtual property by another player.²⁰⁹ The game god was responsible for the loophole in the code.

The situation in *Beijing Arctic Ice* is not unique. Hacking in virtual worlds is an epidemic.²¹⁰ Virtual-world currency is in enormous demand.²¹¹ Because game gods often prohibit the trade of dollars for virtual items or currency rather than meet that demand, players have limited access to legitimate suppliers.²¹² Thus, a hacked virtual-world account is worth more to a hacker than a credit card is.²¹³ Banks have excellent programs that catch misuse of credit cards quickly.²¹⁴ In contrast, virtual-world accounts are often deemed by

²⁰⁵ See *TJX Settles Lawsuits over Huge Data Theft*, MSNBC.COM, Sept. 21, 2007, <http://www.msnbc.msn.com/id/20912876>.

²⁰⁶ Will Knight, *Gamer Wins Back Virtual Booty in Court Battle*, NEW SCIENTIST, Dec. 23, 2003, <http://www.newscientist.com/article.ns?id=dn4510>.

²⁰⁷ *Id.*

²⁰⁸ *Id.* (reporting that the software company claimed that the virtual properties were merely "piles of data").

²⁰⁹ *Id.*

²¹⁰ See, e.g., Min Kim, Dir. of Game Operations, Nexon Am., Inc., *Coming to America: Nexon's Micro-transaction Revolution*, Speech at the Austin Game Developers Conference (Sept. 7, 2007), available at <http://www.virtualworldsnews.com/2007/09/bloggging-the--5.html>.

²¹¹ For example, a Google search for the terms "World of Warcraft gold" generates nearly six million pages, with domain names like www.wowmine.com, www.wowgold-usa.com, and www.world-warcraft-gold.org.

²¹² See World of Warcraft, Terms of Use Agreement, *supra* note 184, § 11 (prohibiting sale of "in-game items or currency" for actual money).

²¹³ See *Cursor Hackers Target WoW Players*, *supra* note 202.

²¹⁴ See J. Howard Beales, III & Timothy J. Muris, *Choice or Consequences: Protecting Privacy in Commercial Information*, 75 U. CHI. L. REV. 109, 124 (2008).

police or policymakers to lack “real value.”²¹⁵ Due to this enforcement gap, hackers have made a robust living from hacking virtual world accounts, looting them, selling off the items for virtual currency, and then selling the currency back to players on the gray market.²¹⁶

A critic might argue that losing credit card data is far more serious than losing magical swords or virtual land. Yet the average value of a hacked credit card is six dollars,²¹⁷ while the value of a hacked World of Warcraft account is roughly ten dollars.²¹⁸ The value of virtual items has been long established; conservative in-world valuations of the virtual-item trade run into the billions of dollars.²¹⁹ Similarly, corporations have made significant and costly investments in virtual assets. For example, if IBM were to lose its \$10 million investment in its Second Life islands due to the negligence of Linden Labs, there would be little argument that IBM had suffered actual harm.²²⁰ And even for the less valuable items prized by players, it is not difficult to establish replacement costs. Players spend countless hours acquiring these items and there are robust (albeit usually extracontractual) markets for these items. The value of items and accounts may run into the thousands of dollars.²²¹

4. Property Law

Property law may at first seem an odd fit with online worlds. But virtual property law and the attendant tort of cyber-trespass are among the most useful and rapidly developing doctrines online.²²² Courts have not hesitated to

²¹⁵ See Edward Castronova, *The Right to Play*, 49 N.Y.L. SCH. L. REV. 185, 191 (2004) (discussing the dichotomy between those who view virtual-worlds as a game and those who view it far more seriously).

²¹⁶ See World of Warcraft, *The Negative Impact of Buying Gold*, <http://www.worldofwarcraft.com/info/basics/antigold.html> (last visited Mar. 14, 2009) (“We regularly track the source of the gold these companies sell, and find that an alarmingly high amount comes from hacked accounts.”).

²¹⁷ See *Cursor Hackers Target WoW Players*, *supra* note 202.

²¹⁸ *Id.*

²¹⁹ In 2007, Tuukka Lehtiniemi estimated the total value of virtual items at \$2.1 billion. See Posting of Tuukka Lehtiniemi to Virtual Economy Research Network, http://virtual-economy.org/blog/how_big_is_the_rmt_market_anyw (Mar. 2, 2007 12:50).

²²⁰ See *IBM Accelerates Push*, *supra* note 16 (reporting that IBM “is already holding meetings and conducting development inside virtual worlds with about 20 major clients, including telecommunications and aerospace firms”).

²²¹ For example, Anshe Chung, the first proclaimed virtual-world millionaire, has assets in Second Life worth at least \$1 million, based on conservative estimates. See Press Release, Anshe Chung, Anshe Chung Becomes First Virtual World Millionaire (Nov. 26, 2006), http://www.anshechung.com/include/press/press_release251106.html.

²²² See DURANSKE, VIRTUAL LAW, *supra* note 2, at 79-115 (describing the implications of adopting virtual property systems in virtual worlds).

recognize property interests in data structures,²²³ in URLs,²²⁴ or in email servers.²²⁵

Property law is not only a method for allocating scarce resources; it is a means for determining legal liability if property is misused or poorly maintained.²²⁶ In the real world, a customer who slips and falls may sue the store for failing to mop the floor. A merchant may argue that the risk of loss or damage to a good falls on the consumer if the consumer buys and takes possession of that good. Given that property law is rapidly developing online, and is a means for determining legal liability, it is worth asking whether the game gods' approach to private property in virtual worlds decreases or increases their exposure.

a. *Real Property*

The basic principle of liability and ownership with respect to property is that the owner of land is liable for harm to invitees on that land.²²⁷ Control of land implies ownership, and ownership generates legal responsibilities. As noted above, if the owner of a store does not clean the floor, and a customer slips and falls, the owner of the store is liable. But if the owner rents the space out to a storefront operator, the operator will bear liability because she controls the space.²²⁸ Similarly, under the doctrine of attractive nuisance, the person in control of the condition of the land may be liable for harm to children, even if the children are trespassing.²²⁹ Control is the touchstone of liability for failure to protect people who are on the land.

Game gods claim ownership of and control over every aspect of a virtual world. If a customer suffers harm, the company in control of the virtual world may be liable. Compare the virtual world Second Life, which sells land to users, to the online game World of Warcraft, which does not. If a Second Life

²²³ Consider the lawsuits involving the theft of credit card data from TJ Maxx, *supra* notes 203-205. Other examples include the multiple settlements between various companies and the FTC regarding inadequate database protection. See Kevin Poulsen, *Tower Records Settles Charges over Hack Attacks*, REGISTER (London), Apr. 22, 2004, http://www.theregister.co.uk/2004/04/22/tower_settles_ftc_hack_charges; Press Release, Fed. Trade Comm'n, *Eli Lilly Settles FTC Charges Concerning Security Breach* (Jan. 18, 2002), <http://www.ftc.gov/opa/2002/01/elililly.shtm>.

²²⁴ See, e.g., *Delor v. Intercosmos Media Group, Inc.*, 232 F.R.D. 562, 563 (E.D. La. 2005) (discussing an interest in the domain name www.1800AsSeenOnTV.com).

²²⁵ See, e.g., *United States v. Gray*, 78 F. Supp. 2d 524, 532 (E.D. Va. 1999) (“[U]nauthorized access into a . . . computer is analogous to breaking and entering in the physical world . . .”).

²²⁶ See, e.g., *Colonial Stores, Inc. v. Pulley*, 125 S.E.2d 188, 190 (Va. 1962).

²²⁷ See, e.g., RESTATEMENT (SECOND) OF TORTS §§ 334-339 (1965).

²²⁸ See, e.g., *McCabe v. Henpil, Inc.*, 889 F. Supp. 983, 993 (E.D. Tex. 1995).

²²⁹ See RESTATEMENT (SECOND) OF TORTS § 339 (asserting that, under certain circumstances, “[a] possessor of land is subject to liability for physical harm to children trespassing thereon caused by an artificial condition upon the land”).

denizen suffers harm on another player's land, Linden Lab is presumptively not responsible – especially if the condition on the land (such as destructive code) is there due to the negligence of the player who owns the land.²³⁰ However, in *World of Warcraft*, Blizzard Entertainment would remain responsible for harm that befalls customers who use that space.

In the real world, the owner and controller of real estate may be liable for harm that befalls customers on the property, even if that harm is caused by a break-in.²³¹ For example, in *Garzilli v. Howard Johnson's Motor Lodges, Inc.*, the victim of a criminal assault successfully sued the Howard Johnson hotel for failing to prevent the intrusion.²³² The plaintiff was raped when an unknown man came through the sliding glass doors of the room.²³³ The doors were locked, but easily could be unlocked from the outside “without much difficulty.”²³⁴ Hotels are generally liable for harm visited upon guests if the harm is reasonably foreseeable and the hotel fails to take adequate precautions.²³⁵

Contrast the situation in *Garzilli* with the sale of a house. If the buyer of the house later complains that someone has broken into his house, he has no one but himself to blame.²³⁶ Since the ownership of the house gives rise to the right to engage in self-help to protect the premises (e.g., installation of locks, security systems, etc.) the buyer of the house has no claim against the seller that the seller should have protected the buyer from third-party acts.²³⁷

Break-ins occur in online worlds just as they do in offline ones. The analogy of break-ins in the real world to hacking in virtual worlds is straightforward. If gods control the world, then they are responsible for protecting it. Failure to do so that results in harm to customers will generate liability. The game gods' claim that they must own all property in virtual

²³⁰ See *Turquitt v. Jefferson County*, 137 F.3d 1285, 1287-89 (11th Cir. 1998) (finding the county not liable for alleged violations of a prisoner's civil rights, since the county had no control over the sheriff who managed the county prisons).

²³¹ See, e.g., *Erickson v. Curtis Inv. Co.*, 432 N.W.2d 199, 201 (Minn. Ct. App. 1988) (“[C]ourts recognize that a landowner may be under a duty to protect others from crime under certain carefully limited ‘special’ circumstances.”).

²³² *Garzilli v. Howard Johnson's Motor Lodges, Inc.*, 419 F. Supp. 1210, 1214 (E.D.N.Y. 1976).

²³³ *Id.* at 1212.

²³⁴ *Id.*

²³⁵ See, e.g., *Schmanski v. Church of St. Casimir*, 67 N.W.2d 644, 645 (Minn. 1954) (asserting that hotels are “bound to exercise ordinary or reasonable care to keep [their premises in] a safe condition for those who come upon them by his express or implied invitation”).

²³⁶ See, e.g., *Gargoni v. Sideris Plumbing & Heating Corp.*, 794 N.Y.S.2d 344, 345 (App. Div. 2005).

²³⁷ *Feinstein v. Beers*, 801 N.E.2d 300, 303 (Mass. App. Ct. 2004) (finding that a condominium association had no duty to warn a resident, who was assaulted in her apartment, that a wooden dowel is not an effective door-locking mechanism).

worlds is therefore likely to increase their risk of liability under property law theories.

b. *Personal Property*

Game gods almost universally prohibit private property ownership in virtual worlds.²³⁸ They do so for familiar reasons. If players own property, then gods fear that they, not the players, will be responsible for harm to that property.²³⁹ Game gods thus routinely insist that all digital objects within their world are governed by the law of intellectual property. Gods hope that by eliminating virtual property interests in virtual worlds and insisting on characterizing disputes as ones about intellectual property, they will maintain control.

But game gods increase their legal risks by converting chattel property causes of action into intellectual property disputes. As noted above, CDA § 230 provides interactive computer service providers absolute immunity for the damage caused by one user to another by using the service.²⁴⁰ But § 230 does not shield interactive computer service providers from intellectual property claims. If one party steals the other's magic sword within the game, and the sword is chattel property, the game god cannot be held liable for the theft. But if one party copies another's magic sword, and the sword is *intellectual* property, the game god is not shielded by CDA § 230. Giving up the strong shield of the CDA is one of the largest liability-increasing moves a game god can make.

Moreover, property is the foundation for shifting risk of loss from producers to consumers. The basic store principle is "you break it, you buy it."²⁴¹ Suppose you purchase a truck and then get into an accident as you drive it off the lot. Because a property interest passed from the dealer to you, you bear the risk of loss for the truck. But if there is an accident before the transfer of the property interest, the merchant bears the loss. The merchant would be foolish to retain the property interest in the truck while you drive it. A merchant who wishes to avoid liability retains property interests for as short a time as possible.

In the virtual world context, this risk of loss regime may matter for game gods that rely on "microtransactions": sales of digital goods to consumers. Once the risk of loss has passed to the buyer, the seller is not liable to repair or

²³⁸ See, e.g., World of Warcraft, Terms of Use Agreement, *supra* note 184, § 11 ("You agree that you have no right or title in or to any such content, including without limitation the virtual goods or currency appearing or originating in the Game . . .").

²³⁹ For instance, if I rent a bicycle and crash it, I am responsible to the owner of the bike. But if I own the bike and damage it, I am indebted to no one for the cost of repair.

²⁴⁰ See *supra* Part II.B.1.

²⁴¹ Indeed, when assessing property ownership, courts have often used the party that bears the risk of loss as a factor to determine the true owner. See, e.g., Keith v. Comm'r, 115 T.C. 605, 611-12 (2000).

replace the good.²⁴² The consumer bears the risk of damage to the good. Property interests therefore provide a strong form of protection against third-party bad acts and unplanned catastrophes.²⁴³ Game gods who choose not to pass the risk of loss to their customers will pass up a powerful tool for limiting their liability.

Finally, game gods eschew property regimes in virtual worlds because they feel they would be better off characterizing their game as a service rather than a sale of goods. Game gods theorize that if players do not own virtual objects and places, they will have no cause of action. But this is based on a false dichotomy. Game gods will be liable for the full extent of harm caused by their bad acts whether they have conveyed a property interest to their players or whether the game is characterized as the provision of a service. Defining the transaction with the client as a provision of a service, rather than a sale of a property interest, does not in itself protect the god from legal liability. Companies are just as liable for failing to provide services as they are for damaging or losing property.²⁴⁴ Game gods who block property rights in virtual worlds give up a valuable tool for limiting loss, and do not gain much additional protection.

5. Agency and Employment

Under principles of agency, corporations risk liability for the negligent or intentional bad acts of employees acting within the scope of their employment.²⁴⁵ Thus, if an employee negligently mishandles information, or if a corporation negligently supervises an employee who commits intentional theft of data, the corporation will be liable.²⁴⁶ Additionally, liability attaches to the employer should the employee act under the employer's apparent authority.²⁴⁷ However, liability will generally not attach if an employee detours from the scope of his employment.²⁴⁸ Moreover, it is not enough that the scope of an employee's authority be limited; that limitation must be effectively communicated to people dealing with that employee.²⁴⁹ In sum,

²⁴² See U.C.C. § 2-401(2) (2007) (stating that title passes to the buyer at time the seller delivers the goods).

²⁴³ This is why the vast majority of insurance policies are taken out by the owners – the people who actually stand to lose should something happen.

²⁴⁴ See, e.g., *Chi. & Nw. Transp. Co. v. Kalo Brick & Tile Co.*, 450 U.S. 311, 313 (1981).

²⁴⁵ RESTATEMENT (THIRD) OF AGENCY § 7.07 (2006).

²⁴⁶ See *Fletcher v. Balt. & Potomac R.R. Co.*, 168 U.S. 135 (1897) (holding that a railroad company had a duty of care to pedestrians when it allowed its employees to throw large pieces of wood from the train, since this action was within the company's control to stop).

²⁴⁷ RESTATEMENT (THIRD) OF AGENCY § 7.08.

²⁴⁸ *Id.* § 7.07.

²⁴⁹ *Id.* § 7.08.

companies are liable for the actions of employees within the scope of their employment and that are performed under the apparent authority of that position.

The doctrine of respondeat superior was designed for employees who are constrained to a limited role, and responsible for a finite set of actions and responsibilities within a firm.²⁵⁰ What is new is the scope of responsibility that game administrators, often called Game Masters (“GMs”), undertake within virtual worlds. While the average bank employee is generally limited to financial transactions, GMs are responsible for monitoring and policing an entire range of social behaviors.²⁵¹ For example, if one player is sexually or racially harassing another, a GM will be responsible for making a decision on whether and how that conduct will be sanctioned.²⁵² GMs are not just traditional employees; they are both judge and police to millions of people. Accordingly, the novel legal questions presented by the negligence or intentional wrongdoing of GMs are not products of new law; they are products of the corporation’s assertion of social control over its players.²⁵³

Since corporations are responsible for bad acts committed by employees within the scope of the employees’ actual or apparent authority, corporations must communicate the scope of the employees’ authority to their customers. Game gods attempt to do this by sharply constraining what GMs can do.²⁵⁴ This is problematic, however, since the EULA reserves broad police powers to the god.²⁵⁵ By retaining police powers for itself, the god has placed itself in a precarious position if or when employees perform their broad mandate incompetently or maliciously.

The more control game gods claim, the more they will be responsible for the bad acts of employees. Narrowing the scope of claimed control is one way to reduce this liability. Under this model, GMs would be legitimately constrained

²⁵⁰ *Id.* § 7.07.

²⁵¹ *See, e.g.,* World of Warcraft, Getting Started, <http://www.worldofwarcraft.com/info/basics/gettingstarted.html> (last visited Mar. 25, 2009). World of Warcraft’s in-game GM paging reveals that GMs are empowered to deal with all forms of verbal and physical harassment, in addition to account issues, and other problems within the world. *See id.*

²⁵² *Id.*

²⁵³ Put differently, since GMs have such broad powers and responsibilities, the line between personal and corporate action is blurred. What actions constitute a deviation from the scope of a GM’s employment?

²⁵⁴ While gods do not impose published limits, there are a variety of issues a GM is not allowed to resolve himself. For example a Google search for “useless WoW GM” reveals numerous rants about the truly limited role of a GM. *See, e.g.,* Posting of Abhorrence to World of Warcraft, Customer Service Forum, <http://forums.worldofwarcraft.com/thread.html?topicId=13275277602&sid=1> (Dec. 3, 2008, 08:27).

²⁵⁵ Recall the standard clause giving the game god sole discretion to suspend or terminate accounts, *supra* note 28 and accompanying text.

to a procedural role. Some companies will have no choice. Entertainment worlds, in particular, must be able to assert control to maintain artistic integrity and prevent bad actors from ruining the entertainment product. Just as the staff of a movie theater must be able to eject drunken patrons, so too must the staff of a virtual world be allowed to remove bad apples who ruin the experience for other players.

But this necessity does not reduce liability. If an employee negligently performs actions within the scope of her employment, the god will be liable. The movie theater employee may remove a drunken patron, but the theater will be liable if, for example, the employee is too rough. Thus, gods must be careful to take only what power they need and to outline the boundaries of this power distinctly with well-established policies.

There are two steps a game god may take to reduce his liability for the acts of his employees. The current practice of *de jure* strict limitations on GMs, but *de facto* GM discretion and power, will not work. Instead, game gods ought to construct player-controlled methods of protection. Every entertainment world has the ability to permit a player to block messages from another player.²⁵⁶ Many worlds have reduced the incentives to harass other players by restricting actions in certain zones.²⁵⁷ A few worlds have multiple instances of the same content – allowing players to choose one of many realms so they may merely hop to another identical world to avoid a harasser.²⁵⁸ Currently, none have implemented a player rating system, similar to eBay, where buyers and sellers establish reputations and leave a trail of negative behavior for all to see.

Once these self-help systems are in place, gods who wish to minimize legal liability may release their policing role and reduce the expectation that GMs will moderate social problems. If they emphasize, through the EULA, for example, that players are responsible for policing their own experiences in the world, few players will expect that policing is within the GMs' role. By making it obvious that the gods expect social situations to be resolved by the players and expressly removing that responsibility from GMs, it becomes far more apparent when a GM exceeds the scope of her authority. No one would believe that resolving social conflict is in the job description of a Microsoft technician. Likewise, a virtual world creator that does not undertake to set or enforce the social rules for use of their software will be in a much stronger position to avoid claims based on employee misconduct.

²⁵⁶ See World of Warcraft's FAQ page, <http://us.blizzard.com/support/article.xml?articleId=20455> (last visited Apr. 10, 2009) (discussing the /ignore command).

²⁵⁷ Many games have also removed the incentive or ability to kill a player over and over.

²⁵⁸ World of Warcraft, for example, has over 200 realms, each with identical content and quests, but each completely independent of the others.

C. *Democracy Versus Theocracy: Control and the Constitution*

Game gods claim the powers of governments, but desire none of the responsibilities that come with such a role.²⁵⁹ This Section looks long-term at the development of online societies, and asks whether constitutional and federal civil rights causes of action will eventually be available to denizens of virtual worlds. The Section concludes that these rights will be available, and that the game gods who exercise the most pervasive and invasive control over their citizens will be the first targets.

If courts decide that game gods exercise so much control that they effectively fill a role traditionally filled by government, then gods may be constrained by the Constitution or federal civil rights laws. However, a caveat is appropriate. The Supreme Court has consistently held that private actors are shielded from such claims if they are acting in their private capacities.²⁶⁰ Courts are admittedly loath to task private actors with the responsibilities of public officials.²⁶¹ Yet when courts do task private actors with these responsibilities, they do so based on the degree and kind of authority asserted by the private actor over her fellow citizen.²⁶² The following Subsections analyze the circumstances that might tempt a court to impose constitutional restraints on game gods.

1. Public Liability for Private Actors

A private actor is liable under § 1983 of the Civil Rights Act for violations of another citizen's constitutional or federal civil rights when she acts under "color of law."²⁶³ Thus, a private actor is considered a state actor when her

²⁵⁹ For example, game gods reserve the right to punish users, block access, exercise eminent domain, and even levy taxes. Yet, they avoid constitutional requirements of due process, freedom of speech, and fair punishment.

²⁶⁰ See *Am. Mfrs. Mut. Ins. Co. v. Sullivan*, 526 U.S. 40, 50 (1999) ("Like the state-action requirement of the Fourteenth Amendment, the under-color-of-state-law element of § 1983 excludes from its reach 'merely private conduct, no matter how discriminatory or wrongful.'" (quoting *Blum v. Yaretsky*, 457 U.S. 991, 1002 (1982))).

²⁶¹ Indeed, the courts have only recognized four circumstances when a private actor may be held to a public level of accountability and liability: (1) when the private entity has a "public function"; (2) when there is joint action between the public and private entities; (3) when the public entity "compels" private action; and (4) when there is a "nexus" between the state and private action. *Kirtley v. Rainey*, 326 F.3d 1088, 1092 (9th Cir. 2003); see also *Lee v. Katz*, 276 F.3d 550, 554 (9th Cir. 2002).

²⁶² See 42 U.S.C. § 1983 (2000) ("Every person who, *under color of* any statute, ordinance, regulation, custom, or usage . . ." (emphasis added)).

²⁶³ *Id.* Federal officers may be held liable for constitutional deprivations under similar conditions. See *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 389 (1971) (holding that "a violation of [the Fourth Amendment] by a federal agent acting under color of his authority gives rise to a cause of action for damages consequent upon his unconstitutional conduct").

conduct is “fairly attributable”²⁶⁴ to the state or when she acts “clothed with the authority of state law.”²⁶⁵ Further, an otherwise private individual is liable for federal civil rights violations when she acts “jointly engaged with state officials”²⁶⁶ or engages in a conspiracy with state actors²⁶⁷ to deny a citizen’s civil or constitutional rights.

This is not surprising. Courts have long held that governments may not circumvent their constitutional obligations by outsourcing public services to private parties. For example, private prisons are bound by the First, Fourth, and Eighth Amendments to the Constitution;²⁶⁸ private contractors working with police are bound by the Fourth Amendment;²⁶⁹ company towns are bound by the First Amendment;²⁷⁰ and so on. Thus, private companies that exercise a governmental level of control over citizens are undoubtedly bound by the U.S. Constitution. The harder question is precisely what level of control over which tasks will cause a court to transform a private actor into public official.

2. The Panopticon

This Subsection argues that the ability of game gods to spy on U.S. citizens may be sufficient to transform them from private to state actors. The Subsection proceeds on the analogy of the Panopticon. The Panopticon metaphor is used by virtual-world theorists to describe one aspect of the virtual world.²⁷¹ In a virtual world, people feel and act as though they have privacy, when they in fact could be observed by the game god at any time. The game god has the ability to act as a fly on the wall, to observe and record some or all

²⁶⁴ *Lindsey v. Bowlin*, 557 F. Supp. 2d 1225, 1231 n.14 (D. Kan. 2008) (quoting *Lugar v. Edmondson Oil Co.*, 457 U.S. 922, 937 (1982)).

²⁶⁵ *West v. Atkins*, 487 U.S. 42, 49 (1988) (quoting *United States v. Classic*, 313 U.S. 299, 326 (1941)).

²⁶⁶ *Dennis v. Sparks*, 449 U.S. 24, 27-28 (1980).

²⁶⁷ *Adickes v. S. H. Kress & Co.*, 398 U.S. 144, 152 (1970).

²⁶⁸ See *Rosborough v. Mgmt. & Training Corp.*, 350 F.3d 459, 461 (5th Cir. 2003) (per curiam) (allowing a prisoner to bring a § 1983 action for cruel and unusual punishment against a private prison); *Skelton v. Pri-Cor, Inc.*, 963 F.2d 100, 102 (6th Cir. 1991).

²⁶⁹ See *Lindsey*, 557 F. Supp. 2d at 1226 (rejecting the defendant’s claim that a “plaintiff cannot bring [a *Bivens* action] against an employee of a privately operated prison”). While these private police are not directly bound by constitutional constraints, liability will be imposed if the private police act under the color of the law. See *supra* notes 263-267 and accompanying text.

²⁷⁰ *Marsh v. Alabama*, 326 U.S. 501, 509-10 (1946) (holding that a company town acts in all respects, save land ownership, as a normal town and that private land ownership alone could not defeat constitutional protection).

²⁷¹ See, e.g., Joshua Fairfield, *Escape from the Panopticon: Virtual Worlds and the Surveillance Society*, 118 YALE L.J. POCKET PART 131, 131 (2009).

of the conversations or interactions between players in a virtual world.²⁷² There is no haven from the game god. Even when conversations are supposedly private, the game god may listen in. Walls are no barrier for a game god who wishes to observe the intimate detail of customers' lives. The god can be everywhere, and listen to everything.

The Panopticon is a theoretical prison designed by Jeremy Bentham. In Bentham's Panopticon, just a few guards can monitor many prisoners without being seen in return.²⁷³ Prisoners would never know whether and when they were being watched, and so would act as though they were being watched at all times. Bentham theorized that eventually, the Panopticon would never need to be guarded.²⁷⁴ Thus, the term Panopticon has become synonymous with the chilling effects of sporadic and unrestrained observation.²⁷⁵

In cases of constitutional claims against private prisons, courts have held the private companies that run these prisons are subject to the same constraints as the government.²⁷⁶ The pervasive, total control that such companies possess over inmates, coupled with the government's traditional role in law enforcement, make the private/public transition a simple one for courts. For example, companies that run private prisons are bound by the First Amendment to permit the free exercise of religion, and to the extent possible, free speech.²⁷⁷ Employees of privately-run prisons are also liable for denying constitutional or federal civil rights under § 1983.²⁷⁸

And, critically, private prison operators may be exposed to § 1983 liability but be denied the sovereign immunity that true government actors would enjoy.²⁷⁹ This creates the precise sort of catch-22 that game gods will wish to avoid, in which a private actor bears governmental responsibilities, but gains no benefit in return.

I am not suggesting that game gods are prison wardens. Among other things, customers may leave game worlds, although not without some cost. However, the pervasiveness and invasiveness of the control game gods exercise might tempt courts to apply constitutional standards to game-god conduct. Consider, for example, the wealth of information that could be gained for intelligence or criminal enforcement purposes if a game god were

²⁷² See Second Life, Terms of Service, *supra* note 19, § 6.2 ("You acknowledge and agree that Linden Lab, in its sole discretion, may track, record, observe or follow any and all of your interactions within the Service.").

²⁷³ MICHEL FOUCAULT, DISCIPLINE & PUNISH: THE BIRTH OF THE PRISON 200 (Alan Sheridan trans., Vintage Books 2d ed. 1995) (1975) (discussing Bentham's work).

²⁷⁴ *Id.* at 201.

²⁷⁵ Indeed, not only do subjects never know when they are being observed, they also do not know the extent and invasiveness of such observation. See *id.*

²⁷⁶ See *Marsh v. Alabama*, 326 U.S. 501, 508 (1946).

²⁷⁷ See *Rosborough v. Mgmt. & Training Corp.*, 350 F.3d 459, 461 (5th Cir. 2003).

²⁷⁸ *Id.*

²⁷⁹ See *Richardson v. McKnight*, 521 U.S. 399, 412 (1997).

free to listen in, record, and pass on all player conversations to law enforcement or the intelligence community without being subject to the warrant requirements of the U.S. Constitution.²⁸⁰

3. The Company Town

The law of prisons is not the only plausible analogy applicable to game gods. Other scholars have examined whether the control exercised by game gods over virtual worlds is so pervasive that gods may be treated as a government under a company-town analysis.²⁸¹ In *Marsh v. Alabama*, a religious proselytizer was arrested for activities in a town owned entirely by a mining concern.²⁸² The company owned the land, the shops, paid the town sheriff and ran the local post office.²⁸³ The Supreme Court held that the company exercised such control over the land, people, and officials of the town that it stood in the shoes of government for purposes of the First Amendment.²⁸⁴ This precedent is an attractive one for purposes of virtual worlds and game gods. Game gods have assumed police duties, just like the company sheriff in *Marsh*. Communications (virtual mail systems, chat systems, etc.) are entirely under the gods' control. Most gods control all spaces, public and private. Virtual worlds are open communities to which the public is invited. These facts dovetail nicely with the *Marsh* analysis.

Yet even more important than slightly stale case law – *Marsh* has not seen much use of late – is the fact that public spaces for speech are functionally shrinking. Traditional First Amendment jurisprudence has unfortunately tied speech to geography.²⁸⁵ Following *Marsh*, the debate shifted from towns to shopping malls, with each step into private property further limiting speech.²⁸⁶ What one may say depends on where one is standing. I may say what I like in

²⁸⁰ For example, Linden Lab keeps rolling chat logs of all instant messages in its virtual worlds for at least three days.

²⁸¹ See, e.g., Peter S. Jenkins, *The Virtual World as a Company Town – Freedom of Speech in Massively Multiple On-line Role Playing Games*, J. INTERNET L., July 2004, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=565181.

²⁸² *Marsh v. Alabama*, 326 U.S. 501, 508 (1946).

²⁸³ *Id.* at 502.

²⁸⁴ *Id.* at 508-09.

²⁸⁵ See, e.g., *Perry Educ. Ass'n v. Perry Local Educ.' Ass'n*, 460 U.S. 37, 45 (1983) (“In places which by long tradition or by government fiat have been devoted to assembly and debate, the rights of the State to limit expressive activity are sharply circumscribed.” (emphasis added)); cf. *U.S. Postal Serv. v. Greenburgh Civic Ass'ns*, 453 U.S. 114, 129 (1981) (“[T]he First Amendment does not guarantee access to property simply because it is owned or controlled by the government.”).

²⁸⁶ See *Hudgens v. NLRB*, 424 U.S. 507, 519 (1976) (finding it permissible to bar protests related to operation of facilities where the private actor does not “[stand] in the shoes” of the government); *Lloyd Corp. v. Tanner*, 407 U.S. 551, 569-70 (1972) (upholding a bar of Vietnam war protest from a private shopping mall because the protest was unrelated to the operation of the mall).

an empty park or on a deserted public street,²⁸⁷ but I may not say what I like on someone else's land or over a publicly funded telecommunications network.²⁸⁸

The marriage of geography and speech was always one of convenience, and I predict it is not one that will last long. No one listens to speeches in parks or on public streets. Democratic debate does not happen there. The important fora for democratic speech have moved online.²⁸⁹ Either courts will maintain protections for free speech by finding ways to protect debate where it is happening, or they will choose to reduce speech and debate by continuing to insist on protections for speech in empty fora. Maintaining the status quo constitutes reducing our commitment to free speech.

One way that game gods can reduce the odds of being tasked with First Amendment constraints is by relinquishing control. If players have their own fora for speech, then courts are far less likely to find that the constraints of public law ought to apply to private companies. Online, the rule has generally been that First Amendment concerns are far less where the speaking party has the ability to buy and build his own website to foster the kind of debate he wants.²⁹⁰ The same rule will likely apply in virtual worlds. If players are free to buy and build their own spaces, courts will find it far less necessary to require game gods to permit people to speak in god-controlled areas.

III. RESOLVING THE GOD PARADOX

In this Part I will offer solutions to the problems posed above. There is a single overarching theme. I recommend that game gods adopt a rule of minimalism when they consider how much control they ought to assert over virtual worlds, the customers who use them, and objects within them. I propose a "virtuous cycle," whereby companies adopt a rule of minimalism, and courts and legislatures reinforce that choice by increasing the protection of companies that do so. I advocate expanding the notice-and-takedown regime that already governs copyright, establishing clear property rules, and developing superior bottom-up player tools for self-governance.

Before moving to my suggestions, I address one caveat. This Article has traced one theme in law – the control/liability principle – as applied to virtual worlds. I do not pretend there are not complementary, competing, or even conflicting themes. For example, Congress has twice expressed an interest in a limited resolution of the control/liability principle by permitting ISPs to

²⁸⁷ See *Perry*, 460 U.S. at 45.

²⁸⁸ See *Greenburgh Civic Ass'ns*, 453 U.S. at 129.

²⁸⁹ For example, during the 2008 presidential primaries, Internet video giant YouTube sponsored debates for both parties through its website and asked the candidates questions posed by website visitors. See, e.g., YouTube, The CNN/YouTube Debates: The Republicans, <http://www.youtube.com/republicandebate> (last visited Mar. 27, 2009).

²⁹⁰ See *Heffron v. Int'l Soc'y for Krishna Consciousness, Inc.*, 452 U.S. 640, 655 (1981) (allowing restrictions on First Amendment rights, with valid reasons, as long as an alternative forum exists).

exercise certain kinds of power on behalf of third parties. The DMCA permits the ISP to take down infringing content on behalf of owners of intellectual property.²⁹¹ CDA § 230(c)(2) privileges ISPs' "Good Samaritan" attempts to block obscene or otherwise objectionable material, like pornography or spam, on behalf of their customers.²⁹² This kind of control – good faith control asserted on behalf of third parties – seems to be popular and necessary.

"Good Samaritanism" and minimalism are not necessarily inconsistent.²⁹³ A rule of minimalism can well complement a rule privileging control on behalf of third parties. For example, in the DMCA context, an ISP may exercise control sufficient to protect third-party intellectual property interests, but no more, or it risks falling outside the safe harbor. But to the extent these themes are inconsistent, I advocate a hands-off rule of minimalism, rather than a command-and-control approach.²⁹⁴ In Web 2.0 technologies, much of the production of value has moved from the ISP to the user, who creates the content. If law seeks to incentivize creation, it ought to protect the end user as the creative engine of Web 2.0 technologies, as well as the infrastructure owner. With this framework in mind, I turn to a discussion of solutions.

A. *A Model for Minimalism: Common Carriage*

It may first be worth examining what the common law and Congress have done in the past when a novel technology, in the control of private corporations, begins to impact the public interest. These are the principles of common carriage, which underlie the statutory requirements of the DMCA as well as numerous other statutes regulating provision of Internet and information services.²⁹⁵ The basic principle of common carriage is an expression of the control/liability principle. The common carrier doctrine creates an obligation not to discriminate among citizens and not to engage in unfair or unreasonable practices or rates.²⁹⁶ If the business is fair and just with its service, it may reap the benefits.²⁹⁷

²⁹¹ See 17 U.S.C. § 512(g) (2006).

²⁹² See 47 U.S.C. § 230(c) (2000) (bearing the title "Protection for 'Good Samaritan' blocking and screening of offensive material"); *e360Insight, LLC v. Comcast Corp.*, 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008) (holding that Comcast's blocking of spam email was privileged under § 230(c)(2)).

²⁹³ See *Doe v. GTE Corp.*, 347 F.3d 655, 660 (7th Cir. 2003) (holding that § 230(c) protects ISPs who choose not to block spam as well as those who do).

²⁹⁴ See *id.* at 661 (explaining that the similarities between ISPs and telecommunications carriers justified protecting providers who adopt a hands-off approach rather than censoring content).

²⁹⁵ Indeed, before the DMCA was enacted, ISPs tried to claim themselves as common carriers to invoke the liability shield it granted. See, e.g., *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 907 F. Supp. 1361, 1369 n.12 (N.D. Cal. 1995).

²⁹⁶ See James B. Speta, *A Common Carrier Approach to Internet Interconnection*, 54 FED. COMM. L.J. 225, 251 (2002) ("The English common law imposed special duties on

At first blush, common carrier rules do not seem to affect game gods. Insofar as game gods are purely information service providers, they benefit from Congress's exclusion of ISPs from the Telecommunications Act's definition of telecommunications service providers, which are subject to a common carrier framework.²⁹⁸ I do not argue that the full range of common carrier obligations ought to be imposed on game gods. Policymakers are likely to have to fit the idea to the application.

But it may be useful to consider a common-carrier-like regime for game gods.²⁹⁹ Game gods create entire worlds in which millions of U.S. citizens work, play, and live. It would be difficult to design a technology that did more to impact the public interest. Thus, I use the common carrier doctrine as one of the most prominent examples of how lawmakers have traditionally balanced the degree of control asserted by a company with the liability the company risks. Common carriage stands as a model that has been adopted in the past when private companies control access to important public technologies.³⁰⁰ Certainly the systemic control that game gods exercise over the lives and livelihoods of those who use such worlds weighs in favor of the sort of considerations addressed by this doctrine.

Several imperfect, but positive, attempts at a common carrier framework for internet service providers exist in U.S. statutory law.³⁰¹ The DMCA, based on the common carriage model, encourages internet service providers to keep a hands-off posture: not to direct traffic to specific recipients or to select content. If an ISP does so, it is shielded from liability for the copyright-infringing acts of users.³⁰² And if a third party believes that content is infringing, the DMCA establishes a notice-and-takedown procedure that both protects the third party's

certain professions to serve all who sought service, on just and reasonable terms, and without discrimination.”).

²⁹⁷ As Lord Chief Justice Hale stated, once “conveniencies are affected with a publick intereft, . . . they ceafe to be *juris privati* only.” Sir Matthew Hale, *De Portibus Maris*, in 1 A COLLECTION OF TRACTS RELATIVE TO THE LAW OF ENGLAND, FROM MANUSCRIPTS 45, 78 (Francis Hargrave ed., photo. reprint 1982) (1787).

²⁹⁸ See generally *Nat'l Cable Telecomms. Assoc. v. Brand X Internet Servs.*, 545 U.S. 967 (2005) (upholding the FCC's statutory interpretation that ISPs are not “telecommunications service providers” but rather “information service providers” and not to be considered common carriers).

²⁹⁹ See, e.g., Speta, *supra* note 296, at 27-28 (arguing that the history of common carriage has useful lessons for internet and electronic interconnection).

³⁰⁰ Common carriage principles are currently applied to shipment and travel via railroad, bus, airplane and boat. Its neutrality requirements are also imposed upon telecommunications providers and public utilities. See, e.g., *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 907 F. Supp. 1361, 1369 n.12 (N.D. Cal. 1995).

³⁰¹ See *supra* Part II.A.1.d (discussing the DMCA).

³⁰² See 17 U.S.C. § 512(a) (2006).

rights, and absolves the ISP of the need to constantly and inefficiently monitor its network.³⁰³

One possibility is to expand this model beyond the domain of copyright. This would be extremely useful for virtual world creators. In a world of superheroes, avatars that infringe the trademarks of a third party (such as the cleverly named “Man-Spider,” “The Sulk,” or “Eyeclops”), even if used in commerce, would not render the game god liable unless the game god had exercised control over player avatars. In Linden Lab’s Second Life, the forty stores that carry “Rolex” and “Chanel watches,” the sixteen stores that carry Ferrari cars, and the fifty-plus stores carrying sunglasses by Gucci, Prada, Ray-Ban and Oakley, would not automatically subject Linden to liability. Rather, purveyors of luxury items could inform Linden that certain stores were unlicensed vendors and ask Linden to de-list the content.³⁰⁴ Linden and the intellectual property owners could then collaborate to stop the trades, rather than sue one another.

Notice-and-takedown systems do have weaknesses. ISPs always have an incentive to remove content when they receive a takedown notice, even when there is no serious claim that content is infringing. For example, virtual-world millionaire and virtual-real-estate mogul Ailin Graef (better known by her virtual identity, Anshe Chung) was targeted by protestors during a CNET interview within Second Life.³⁰⁵ The protestors targeted Chung’s avatar with flying animated genitalia and other offensive content. Movies of the incident were saved by several of the onlookers, and the videos became public.³⁰⁶ Graef’s husband, Guntram, then contacted newspapers, online sites, and other sources for the pictures and video with DMCA takedown notices, claiming that Ailin Graef had a copyright in her avatar, and that videos and pictures of the protest were a violation of this copyright.³⁰⁷ The online sites, including YouTube, promptly took down the videos, without significant inquiry as to whether Graef’s copyright claim had merit.³⁰⁸

However, this takedown abuse was corrected by community norms. Virtual worlds would cease to function if players violated copyright law every time they looked at one another. Every person in a virtual world makes copies of every other denizen’s avatar each time they cross paths, in order to display the

³⁰³ *Id.* § 512(c)(1)(C). It is worth noting that such a notice-and-takedown system seemed to influence the court’s finding of no contributory trademark liability in *Tiffany Inc. v. eBay, Inc.*, 576 F. Supp. 2d 463, 469-70 (S.D.N.Y. 2008).

³⁰⁴ See Duranske, *Rampant Trademark Infringement*, *supra* note 105

³⁰⁵ Jeff Roberts, *Are You Ready for Avatar Rights?*, TORONTO STAR, July 5, 2008, at ID07, available at <http://www.thestar.com/News/article/454742>.

³⁰⁶ *Id.*

³⁰⁷ Adam Reuters, *Anshe Chung Studios Cracks Down on Griefing Photos*, REUTERS, Jan. 5, 2007, <http://secondlife.reuters.com/stories/2007/01/05/anshe-chung-studios-cracks-down-on-griefing-photos>.

³⁰⁸ *Id.*

avatars to the computer users. Following a community uproar, Guntram retracted the takedown notices.³⁰⁹ Thus, although notice-and-takedown systems have their flaws, the Anshe Chung example shows that community norms can influence and shape how such systems are used. The notice-and-takedown approach represents a compromise by which gods may exercise control on behalf of intellectual property holders without opening themselves to liability, and where the density of virtual-world social norms may mitigate the abuses traditionally found in such systems.

B. *Recognition of Virtual Property for Ownership Disputes*

The question of an owner's liability for accidents that happen on virtual property is moderately easy to resolve. If game gods cede or sell control of virtual land to users, the operator of the land and not the game god will be responsible for harm that occurs on the land. To do this, it is necessary to address the fears of game gods, who are concerned that they will be liable to their customers if they sell them land or items. First, it is worth restating that characterizing the sale of virtual objects as provision of a service, rather than sale of a good, does not do any serious good in terms of limiting liability.³¹⁰ Companies are just as liable for negligent provision of services. Thus, the game gods' claim of ownership of all assets and land in a virtual world merely increases their risk of liability.

Consensus is emerging among virtual-world scholars that the benefits of private ownership of property are sufficiently large in virtual worlds (just as they are in the real world) that companies that do permit the sale of virtual property ought to be given distinct legal protection against liability.³¹¹ A statutory virtual property right would permit the free alienability, disposition, and devise of virtual property – a property right good against all the world, except the game god. The game god in turn can trump this interest where it is necessary to maintain the structural integrity of the virtual world. A game god that does exercise this restrained version of power over virtual property would receive safe harbor protection against claims that it negligently failed to use its power to prevent harm to the property. Just as an ISP who adopts a hands-off approach to content is protected against copyright infringement claims, a game god who adopts a hands-off approach to virtual property would likewise be

³⁰⁹ Benjamin Duranske, 'Anshe Chung' Withdraws DMCA YouTube Complaint, VIRTUALLY BLIND, Jan. 21, 2007, <http://virtuallyblind.com/2007/01/21/anshe-chung-withdraws-dmca-youtube-complaint>.

³¹⁰ See *supra* Part II.B.2.

³¹¹ For example, those virtual worlds that wished to permit sales of virtual property would receive the protection of law. See Edward Castronova, *The Right to Play*, 49 N.Y.L. SCH. L. REV. 185, 205-06 (2004) ("As worlds that matter, these open worlds will deserve exactly the same legal treatment as the real world receives. For example, all economic activity inside open worlds will have to be treated as equivalent to economic activity in the real world.").

protected against claims of failure to stop a third-party hacker from stealing virtual property or land.

C. *Stronger User Tools*

A final recommendation is that game gods minimize their police role and devolve social controls to the players. Much of the social policing that game gods currently do can be delegated downward by creating software tools that users can employ to police one another. Some tools, such as the ability to block incoming messages, or log in anonymously, are fairly standard. Others, such as fully developed reputation systems, or the ability to block messages by IP address, are not. Social norms within virtual worlds can have an enormous self-regulatory impact, and absolve the god of the need to meddle in social questions.

This approach has been used in the past, when game gods have faced the problem of detecting bad actors within a broad population. Systems where players may report other players are common. New development in the automation of such systems permits players to take entirely autonomous action to resolve conflicts. For example, in Blizzard's World of Warcraft game, a common and hard-to-detect behavior is remaining idle while other players perform important tasks. It is difficult to determine when a player is truly idle, or whether he is simply not typing. Blizzard implemented a player-flag system so that when active players determined that an idle player was likely free-riding, he would be subject to sanction unless he returned to active play. This is a simple game-based model, but it shows the strength of handing the tools of social policy to players. Once game gods devolve the police role to players, they will have significantly decreased their possibility of liability, and will have taken a large step toward resolving the God Paradox.

CONCLUSION

I reiterate that game gods may legitimately need a lot of control, and they are right to be concerned about legal liability. But somewhere the threads have become tangled. I am convinced from talking to legal experts, in-house counsel, and other academics, that game gods are being told that the more control they assert, the less liability they risk. This is incorrect. Some control may be necessary, but it is necessary for reasons other than liability reduction.

The more power a game god asserts, the more responsibility it will bear if its customers come to harm or infringe the intellectual property of others. This, alone, should be reason enough for game gods to adopt a hands-off approach to information flowing across their networks. But there are other reasons to promote a world in which the owners of information networks do not control every communication from regular conversations to political discussions to intimate encounters. Tens of millions of people now use virtual worlds to communicate. Time will tell whether virtual worlds are the next iteration of internet technologies – the internet in 3D. But it is certain that *some* technology will replace our current means of communication. When it does,

we will need to ask whether the owner of a method of communication should decide what can be communicated. The answer will be important long after virtual worlds are forgotten.