Authorization and governance in virtual worlds by Dan L. Burk

Abstract

Although a variety of formal and informal mechanisms govern behavior in virtual worlds, the proprietors of such worlds increasingly have relied upon formal legal claims to sanction undesired user behavior. A range of such legal claims might be asserted in different factual situations: copyright infringement, or trespass to computers, or circumvention of technical protections. But each of these claims relies upon the authorization status of the targeted user. Authorization is largely an incident of the virtual world proprietor's Terms of Service (ToS). Thus, the ToS is increasingly regarded as a license to access the proprietor's servers; violation of the ToS annuls authorization to access the servers. The result is that any misbehavior by users, in violation of the ToS, can be recast as a violation of copyright, or trespass, or technical circumvention laws, even if the undesired behavior has little bearing on the variety legal claim asserted. This mutation of legal claims is troubling, not only from the standpoint of legal policy, but as a social policy to govern virtual worlds.

Contents

[Introduction](#)
[Governance and cheating](#)
[Modding and governance](#)
[Copyright](#)
[Anticircumvention laws](#)
[Trespass to computers](#)
[Terms of service](#)
[Authorization and authority](#)
[Conclusion](#)

Introduction

Virtual worlds, like any site of human interaction, can be the sites of dispute: disputes among users, and disputes between users and proprietors. Disputes between users and proprietors particularly implicate the governance and control of virtual worlds: who decides what behavior is and is not permissible with regard to a virtual world platform? Such disputes might be resolved by a variety of formal and informal mechanisms, but among the available options is the resort to formal legal process. Virtual world proprietors have shown themselves increasingly willing to assert formal legal claims against unruly users via litigation, and the courts have shown little hesitation in applying to these claims the same law that they would apply to any other software platform or telecommunications service.

But this dynamic is relatively understudied. Some previous commentators have noted the controversies surrounding legal control and ownership of virtual worlds (Taylor, 2006a) or

have discussed certain policy questions related to the ownership of digital objects (Dibbell, 2006; Grimmelmann, 2006). But to date relatively little scholarship has been done regarding the formal legal analysis of such problems. As Benkler (2006) points out, this is because much of the discussion regarding ownership and governance has been distracted by the rendering of the interface. There is a tendency to treat virtual world activity as if it were a phenomenon apart from the rest of society; but the question is how legal claims apply to the activity associated with virtual worlds, and not if.

In this essay I propose to make a small contribution toward bridging the gap between theory and practice in the legal control of virtual worlds. I will focus here primarily on the law of intellectual property and related property regimes. Much of the interactive display that constitutes a virtual world clearly falls within the purview of intellectual property: graphics, sound recordings, and other components of the audiovisual display, as well as the underlying software and constitutive databases. Intellectual property law is intended to facilitate control of the uses to which such creative works are put, on the general theory that granting creators legal control over their works will spur the development of such works. Intellectual property and related legal theories thus become seemingly obvious and natural modality for control of virtual worlds: if one controls the uses to which the output and infrastructure of a virtual world are put, one presumably controls that world.

Virtual worlds and their proprietors span a wide range of technological, social, and business models. Much of discussion here will be directed to multiplayer online gaming worlds, and many of my examples will be drawn from Blizzard Entertainment's recent litigation asserting intellectual property claims. The relative abundance of such examples arises in part because of the commercial success of Blizzard's World of Warcraft (WoW) multiplayer game, and in part because Blizzard has been fairly forward in asserting its legal position. However the analysis here should be more broadly applicable to virtual world scenarios besides multiplayer games such as WoW.

Governance and cheating

Provision of multiplayer games and other virtual worlds poses unique problems of crowd control. Proprietors of virtual world servers are making their facilities accessible to large number of patrons — sometimes numbering in the millions — who interact in real time, often over an extended period. Admittedly, virtual worlds are not entirely unique in this respect. Other businesses offering food, entertainment, lodging, or shopping facilities certainly deal with the oversight problem of patrons who are accessing or using their facilities. Some of these, such as sports stadiums or shopping malls, deal with the control of very large numbers of patrons. Telephone companies and other telecommunications providers deal with the behavior of numerous customers accessing their facilities remotely. However, while it is certainly possible to find aspects of the problems faced by virtual world proprietors in other business ventures, it is difficult to find previous examples of behavioral governance with quite the same array of features.

Online multiplayer games offer particularly complex set of strictures for governance of player behavior, due to the multiple levels of interaction with the game, the mechanisms for delivering the game, and the real-life setting in which the players and proprietors ultimately reside. Some rules will be internal to the “magic circle” of the game: wizards must complete a particular quest before gaining a magical item, or at least three members are required sign up in order to form a new guild. At another level, private, non-game play rules will be implemented to govern the relationship of the player to the infrastructure of the game, for example the use of the proprietor's resources: players must pay a subscription fee in order to be permitted access to the server, or players may not share an account. And at yet another level, game play and server access will be subject to the more general public laws of the society in which they live: players may not defame one another, or players may not copy proprietary software.

As Lessig (1999) famously noted, governance mechanisms may be drawn from a menu of regulatory mechanisms that include norms, markets, architectures, and formal laws. Each of these regulatory modes is apparent and important in governing conduct in virtual worlds. Interaction in virtual worlds, like everyday interactions between physical actors, is largely governed by behavioral norms: for example, in many role-playing games it is impolite, perhaps subject to social sanction, to collect the treasure dropped by a monster someone else has fought. Normative expectations will tend to deter this behavior. In other instances, the proprietor of the virtual world may design the technical architecture of the game so as to

enforce particular rules; for example, programming into the game software a prohibition against picking up treasure dropped by a monster one has not fought.

Market incentives are also an important driver of virtual world conduct. Multiplayer games are typically structured around a reward paradigm; players amass treasure or gain levels or accumulate points. Exchange of virtual goods or services in the pursuit of such rewards has endowed many games with robust internal economies; indeed, aspects of the game design may be structured around such activity. But games are also typically business ventures, generating profits through subscriptions or other mechanisms, linking the game to the larger external economy. These two economies, internal to the game and external to the game, will frequently overlap, in sometimes unanticipated ways. Perhaps the most celebrated — or infamous — example of such interaction may be the practice of “gold farming” by professional game players, who extract virtual items and treasure from the game milieu, sell them in external auctions or transactions for real currency, and deliver the items sold to the purchaser, back in the context of the game (Duranske, 2008).

Most significant for this essay is the role that formal law may play in governing player behavior. To pursue the example of gold farming a bit further, if gold farming is considered a problem, it may be that normative disapproval will somewhat deter or curtail gold farming; it is considered bad form by many gamers. Some technical fixes restricting the movement of virtual objects or treasure in the game may also help deter the practice. Or the proprietor may make adjustments the internal market of the game to provide alternatives to trading on the external market. But increasingly, game proprietors turn to formal legal rules — either contractual provisions in the game’s Terms of Service (ToS) or to intellectual property law such as copyright, to deter or control unwanted behaviors (Duranske, 2008).

A separate but related point that quickly becomes apparent in the examples explored above, is that any of Lessig’s modes of regulation may cut across the multiple levels of governance I have identified: that of the game or world community, that of the proprietor’s terms for transacting business, and that of the broader society at large. For example, the technical architecture of virtual world likely prohibits logging on to the game server without an account password, restricts copying of the game software, and restricts player’s characters from moving through the walls or obstacles depicted in the game graphics. Normative expectations of the community may be the strongest deterrent against software hacks that would compromise the rules of the game, violate the service agreement with the proprietor, and infringe the legal protections on the proprietor’s intellectual property. Market incentives can similarly deter — or provoke — behavior that may be normatively, technically, and legally undesirable.

In the case of on-line games, governance and behavior is intimately connected to the problem of cheating. As Mia Consalvo (2007) has noted, violations of governance structures in online games — the problem of cheating — often arise as participants vie to gain an advantage not only within the terms of the game, but outside of game play as well. To be certain, not all behavioral violations are cheating — the terminology of cheating focuses on a subset of transgressions focused on the expectations of play. Libeling another player, or adopting a character name that infringes the literary properties of *Star Wars* or the *Lord of the Rings*, does not necessarily give a player an advantage in the game. By the same token, in the case of a non-game virtual world, it may be that the nomenclature of “cheating” in the sense of transgressing game play, is not quite the appropriate terminology for behavior that seizes an illegitimate advantage *vis-à-vis* other participants.

But as a subset of antisocial behavior in virtual worlds, cheating, like other transgressive actions frequently extends across the multiple modes and levels of governance identified above. At one level, cheating may simply constitute impolite or antisocial behavior outside the normative expectations of the playing community — taking the treasure dropped by a monster that was killed by another player, or hunting monsters on a map that another player has already occupied. At a different level, cheating may extend outside the formal terms of service as specified by the game proprietor — exchanging game currency for real world currency, or sharing accounts so as to avoid subscription fees. Since many of the “rules” of a virtual world are instantiated in the design of the game’s software, cheating at this level frequently involves modification or circumvention of limitations coded into the software infrastructure of the game. Cheating may therefore ultimately extend to illegal behavior, contravening the legal strictures of society beyond the game and its community, in which case formal law may be invoked as a response.

Modding and governance

Several papers in this special issue address the practice of developing add-on software to modify or “mod” the interface of a game or virtual world (Kow and Nardi, this issue; Postigo, this issue; Scacchi, this issue). Such add-ons typically modify the game’s user interface, altering the display of information, displaying otherwise inaccessible information, and allowing automated game control functions. While a good deal of modding activity would undoubtedly occur without the support or acquiescence of game proprietors, some companies, such as Blizzard Entertainment, have at times chosen to permit and even encourage modding. Consequently, the practice of modding offers a particularly fruitful instance for examining the interactions of governance strategies in the different modes that I have identified above.

A fairly typical example of such an add-on is offered by the CTRaidAssistant (CTRA) mod for Blizzard’s World of Warcraft, as described by Taylor (2006b). A central feature of the Warcraft game is the institution of raiding parties, in which groups of players band together to fight monsters, gain experience, and amass treasure. The leaders of raiding parties will issue instructions to party members to bring certain equipment that may be needed for the task being undertaken. Within the game, such items are costly to procure and to use. Players may be tempted to free-ride off of the preparations of others, trusting or hoping that either the party will be lucky enough that the required equipment won’t be needed, or trusting and hoping that other party members will spend the gold and effort to bring the required equipment. The expected results of such “prisoner’s dilemma” free-riding are well known: if everyone shirks the expenditure, relying on someone else to incur the cost, then of course on one incurs the costs. The raiding expedition will fail because no one will bring the needed items.

It would be a decided benefit to party leaders to be able to verify that the members of the party have complied with instructions and are carrying whatever equipment had been specified for the raid. The CTRA interface modification provides “panoptic” technical tools that allow leaders to do so. Among other features, the mod displays in a handy format the item inventory and pouch contents carried by members of the raiding party, that would not be visible to surface inspection. This allows leaders to curtail shirking, and ensure that the party has the proper equipment to succeed in its objectives.

A mod of this sort might be viewed as relatively innocuous, simply enhancing the enjoyment of the players and furthering the goals of the game. It does not enhance the speed or gaming prowess of the players, or hobble their game generated monsters that are their opponents. It might be viewed as not providing an undue advantage to the player. The mod simply uses information available through the game’s API, displaying the information in a convenient and useful form for the leader of the raiding party.

Or perhaps not. The mod clearly enhances the party leader’s ability to some degree. The ability to remotely inspect the contents of the party’s members clearly enhances the efficiency and efficacy of the party; that is its purpose. Absent the mod, the party leader would have to query the other players and trust their responses, or perhaps engage in time-consuming, invasive, and ineffective inspection procedures. If one took the position that learning to trust the other members of a raiding party one of the game’s important features, or that risking the of other players is essential to the character of the game, then the mod might be viewed as frustrating or circumventing those aspects of play.

Blizzard and other game proprietors walk a fine line between encouraging add-on development that enhances players’ gaming experiences and curtailing add-ons that are detrimental to either player community norms or the proprietor’s business purposes. For example, Blizzard recently promulgated rules that prohibit add-on developers from charging for their software, or from soliciting donations, or advertising by means of the software (Blizzard Entertainment, 2009). The add-on also is not permitted to “negatively impact World of Warcraft realms or other players,” a restriction that explicitly prohibits burdening the game’s technical infrastructure, but which might also extend to add-ons that allow players to cheat or gain unfair advantage, however that might be defined. The determination of a “negative impact” is stated to be at Blizzard’s sole discretion, making it difficult for a mod developer to determine in advance what the acceptable limits of behavior might be under this stricture.

The threat implicit, and sometimes explicit, in promulgating such policies is that add-ons that violate the rules are subject to sanction. The possibility of expulsion or exclusion from the game servers is one option, but unlikely to be effective against generalized distribution of the add-on. Blizzard’s recent legal actions against players perceived to be cheating or

disruptive of game play gives a good indication of the types of legal theories that might be asserted against unwanted add-ons, and the uncertainties that such theories entail.

Copyright

When considering intellectual property regimes that may apply to virtual world activity, an obvious candidate is the law of copyright, which includes within its subject matter creative works such as graphics, music, audiovisual works, and even software (17 U.S.C. § 102). Blizzard has asserted such claims against the developers of some types of add-on programs (*MDY Indus., LLC v. Blizzard Entertainment, Inc.*, 2008; *MDY Indus., LLC v. Blizzard Entertainment, Inc.*, 2009). However, as I have pointed out in previous work, copyright analysis of multiplayer games is potentially complex and indeterminate (Burk, 2009; Burk, 2006).

An initial difficulty is determining the type of work that is at issue. Computer games and virtual worlds entail a series of related but distinct copyrightable works. The most obvious and observable copyrighted work associated with the game is the output viewed on the screen: an audiovisual work incorporating animated images, sound, music, text, and increasingly, voice. This work might seem to be ephemeral; it changes constantly and for that matter differs for every player, depending on the choices they make in playing the game. Copyright law does require fixation of a work for more than a transitory duration in order for rights to attach; however, some courts have indicated that this requirement is satisfied by the storage of computer code in memory, even temporarily (*MAI Systems Corp. v. Peak Computer, Inc.*, 1993). Early video gaming cases indicated that copyright subsists in video output even though the output may change from play to play (*Midway Mfg. Co. v. Arctic Int'l, Inc.*, 1983; *Williams Elec., Inc. v. Arctic Int'l, Inc.*, 1982; *Stern Elecs., Inc. v. Kaufman*, 1982).

However, this game output will itself likely involve multiple overlapping and embedded copyrights. The audiovisual work generated by player interaction with the game may be the subject of copyright, but is also likely comprised of elements that are individually the subject of their own copyright. Graphics depicting objects, background scenes, and non-player characters, as well as musical compositions, sound effects, and explanatory texts will each likely be the subject of discrete copyright for that particular creative element. Copyright in each of these works may belong to the developer, or may be licensed by the developer from another copyright owner. Additionally, some elements, such as voice, may be wholly supplied by the players.

In addition to the game outputs, copyright certainly applies to the underlying software of the game, which generates the visual, auditory, and other interface output in response to the pre-set instructions of the developer and the input of the players. Additionally, the underlying game architecture will typically include some database of values representing the state of the game, including character status and other data objects manipulated by the players. This data may be difficult to distinguish from the gaming software, as the two must necessarily interact during play, and, since bits are bits, the distinction between software and data is never very pristine. In addition, the game software may include or draw upon more static databases that are unaltered by player activity, for example libraries of stock images, such as objects displayed by the game software during the course of the game.

A subsequent complication, closely related to the separation of the different copyrightable works in the game, is the problem of determining the authorship of these different works. The contributions of the game proprietor and the game players create difficulties in assigning works to traditional categories of authorship. In previous work I have discussed the difficulty of classifying avatars and their game narratives under the categories recognized in the Copyright Act (Burk, 2006; Burk, 2008). Game developers have asserted copyright over the characters and narratives created by players incident to the game [1]. Their argument is that players merely draw upon choices provided by the developer. This account of copyright in the game probably understates the contribution of the players to the work that is generated. I have argued that the developer likely holds copyright in individual elements of the game, and can be said to have selected the elements from which players choose, but the options for play are extensive and elements of the game are arranged in fairly complex ways by the players (Burk, 2009). The number of combinations is sufficiently large, and the number of possible play outcomes sufficiently diverse, that it seems likely players have added original expression to develop the audiovisual output of the games — indeed, in a multiplayer setting, many players have collaborated to generate the state of the

game at any given time.

Given the contribution of the players to the game output, and assuming that the players are authorized to engage with the game's copyrighted material, the end product seems likely to be a derivative work, or even a work of joint authorship. Works are the product of joint authorship if two or more contributors combine original expression intending to create a single, unified work (17 U.S.C. § 101). It is somewhat unclear whether this is the case for game output; certainly a game producer must contemplate that players will play the game, and so arrange game elements to perform the audiovisual output. But it may be less certain that the game developer considered the activities of the players as original authorship, or intended the production of an audiovisual work as such. If the game developer's purpose is simply to provide entertainment, or to make money, the intent needed for a joint work might not be present.

Modding of games presents a particularly difficult copyright problem, as mods interact with the API of the game software, but do not directly alter the software; no code in the game software is changed by the operation of the mod software. When the mod is turned off or removed, the game software functions exactly the same as it did when issued by the game proprietor. Some past copyright cases involving video games have held that when software is not permanently modified by a device, no derivative work is created (*Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.*, 1992). However, other cases could be interpreted as holding that the interaction of the underlying software and a game modification creates a derivative work, even if the modification is not permanent (Samuelson, 1993). Certainly the mod typically does alter the audiovisual output of the game, and the same cases suggest that this new "narrative" work is a derivative work in the same sense as a sequel to a textual story would be (*Microstar v. Formgen, Inc.*, 1998).

Mod usage also alters the game database, in which data about positions and characteristics of the avatars and environment is stored and updated. When mods are in use, the database is quite possibly altered in ways that it would not have been altered had the mod not been in operation. But this is typically not directly due to the functioning of the mod, but rather due to the change in play. However, as we shall see in greater detail below, it may be possible to articulate a theory by which database alterations under certain circumstances, such as during the employment of an add-on, are differentiated from database alterations during the usual course of play. In such a case, a copyright claim that the former alterations constitute infringement might lie.

Anticircumvention laws

Consideration of copyright as a means to police behavior related to virtual worlds sets the stage for consideration of a second, related legal regime that may also be used to control certain interactions with games. Recall the observation above that technical design may be deployed to control behavior, and that breaking such technologically implemented rules requires alteration of the code that structures the virtual world (Lessig, 1999; Reidenberg, 1998). Copyright claims might be asserted with regard to the copying of the software that implements such structural controls, since some degree of copying will necessarily occur in altering the code. However, national and international laws often also provide more direct prohibitions on the circumvention of technical controls, in the form of anticircumvention laws that are required by international treaty.

In the United States, such measures comprise a portion of the Digital Millennium Copyright Act, or DMCA (Burk, 2005; Samuelson, 1995). The statute was intended to prevent disabling or foiling technological protection measures, such as encryption protocols or other security mechanisms, that restrict access to and uses of copyrighted works. The DMCA anti-circumvention provisions prohibit the act of circumventing technological measures, or supplying another with the means to circumvent technological measures, that control access to a copyrighted work. The statute also prohibits supplying the means to circumvent a technological measure that controls copying or other acts exclusive to the copyright holder (Reese, 2003). Courts have held that some underlying violation of the copyrighted work must occur in order to trigger anti-circumvention liability, but the prohibition is on circumventing the technology rather than on using the protected work (*Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 2004; *Lexmark International, Inc. v. Static Control Components, Inc.*, 2004).

As some commentators have pointed out, such anti-circumvention laws are in fact

anti–reverse engineering laws, which pose a generalized problem to the competitive creation of interoperable software (Samuelson and Scotchmer, 2002). In the context of the present discussion, these are laws that may deter development of gaming alternatives and add-ons by prohibiting players from creating interoperable gaming software. The impact of these laws has for example become apparent in the lawsuit brought by Blizzard Entertainment regarding the BNED project, a collaborative, open source initiative to create a non–proprietary user network for game play (*Davidson & Associates v. Internet Gateway*, 2004).

The BNED project was intended to network Blizzard games outside the Blizzard networking service. Users who purchased Blizzard games could play them in stand–alone mode, at their own machine, or could network them for multiplayer via Blizzard’s “battle.net” feature. Some players who were dissatisfied with the management of battle.net began developing their own alternative connection system, BTNED.net, as an open source coding project. In order to network Blizzard games, the BTNED.net developers had to emulate a connection protocol used by battle.net; doing so required them to decrypt and reverse engineer Blizzard’s networking software. Blizzard successfully sued the BTNED developers under the DMCA, alleging that the decryption and emulation of the connection protocol was circumvention of a technical protection.

The most striking feature of the case may be the lack of any threat to Blizzard’s copyrights; the open source project was not engaged in copying Blizzard game packages or even substituting an alternative product for the games. Users of the BTNED system would still purchase and own their own copies of Blizzard games. Rather, the DMCA claim was used to suppress a reverse engineered alternative to Blizzard’s networking service, allowing the game publisher to retain exclusive control over multiplayer activity. While there was a copyright element to trigger the DMCA claim — the copying of the software in reverse engineering the “handshake” protocol — the anti–circumvention claim was entirely separate from any copyright claim.

Blizzard has also asserted DMCA claims in a different context, that of game modifications. Here again the issue was not one of illicit copying or displacement of Blizzard games; quite the contrary, alleged infringers in *MDY Industries v. Blizzard* were serving a clientele who were in some senses too determined to play Blizzard games. The product in the case was a software application called “Glider” that would allow players to engage in “botting” or automated play via a software robot that can operate a game character without the involvement of a human. Such activity is often viewed as unfair under the norms of the game, and prohibited by the game proprietor’s ToS, because they allow game characters to gain experience and levels without effort on the part of the player.

Blizzard had placed software safeguards, dubbed “Warden,” on its system to detect and prevent botting or similar impermissible game modifications. The Warden software restricted access to the Blizzard servers by scanning a user’s computer at logon to look for unauthorized programs, and by requesting periodic updates on memory use from the client software during play. Users whose equipment failed either of these automated inspections were disconnected and refused access. In order to function, Glider bypassed the Warden detection features; Blizzard characterized this as circumvention of a technical protection.

The difficulty in the argument lay in determining what Warden might be protecting; if it was not protecting a copyrighted work, or no copying occurred as an antecedent to the circumvention, then a DMCA claim would not lie. The Court’s DMCA analysis indicates the interconnection between copyright and anti–circumvention claims. The analysis rested on the distinctions between client–side and server–side software, and between literal and non–literal aspects of the game code. The literal code of the game software resides on the user’s hard drive and could be copied without accessing the Blizzard server. Although such copying might be a copyright violation, it would not be a DMCA violation of the Warden control program. Similarly, the multimedia content of the game that is generated by the literal code, such as graphics, sound effects, and music, resides on the user’s hard drive and could also be accessed without connecting to the Blizzard server. Since the Warden program did not restrict access to this content on the client side, the anti–circumvention provisions did not apply to them.

However, connection to the server allows the user to experience the multimedia content in real time and to encounter other players. Even though the multimedia content resident on the user’s hard drive can be viewed in isolation, or in limited combinations, it cannot be viewed dynamically without connecting to the server. To access these dynamic features, the Glider software had to evade the Warden restrictions on the Blizzard server. Consequently, the Court held that the anti–circumvention provisions applied to the dynamic nonliteral elements of the game, so that circumventing the Warden software constituted a violation of the statute.

This analysis regarding the “non-literal” elements of the game has potentially broad ramifications. The MDY Court rejected defendant’s arguments that the dynamic nonliteral elements were not subject to copyright because they are not “fixed” in a tangible medium as required by the Copyright Act and, because the dynamic elements of the game were controlled by the users rather than by Blizzard. Significantly, the Court relied upon early video game copyright cases that rejected similar arguments (*Midway Mfg. Co. v. Arctic Int’l, Inc.*, 1983; *Williams Elec., Inc. v. Arctic Int’l, Inc.*, 1982; *Stern Elecs., Inc. v. Kaufman*, 1982). Certainly there is an argument that the holdings in these early cases might be extended to the question of copyright in more modern game output. But it is unclear whether the holdings in cases dealing with stand-alone arcade games are in fact appropriate to the complex interactions and player choices found in current multiplayer games.

Trespass to computers

An alternative to copyright and related claims may be found in claims of trespass to chattels, which Blizzard has asserted against certain offending users, such as players who repeatedly transmitted advertisements over WoW’s chat channels (*Blizzard Entertainment, Inc. v. In Game Dollar*, 2008). Trespass to chattels has been previously asserted against unwanted e-mail or data gathering from Internet computers (Burk, 2000). Unlike the well-known claim of trespass to land, which requires only some contact with real property, claims of trespass to chattels require both “intermeddling” with the chattel and some damage or impairment to the value of the chattel. Courts considering trespass to computers claims have found the intermeddling requirement to be fulfilled by the passage of electrons across the equipment, and damage or impairment requirement to be satisfied by nearly any showing that the some aspect of the equipment was unavailable for other uses — that the contact by the defendant had occupied processor cycles, or used memory capacity (Burk, 2000; Collins, 2006).

A conceptually related claim, under a different legal rubric, is found in statutes that penalize unauthorized access to servers on a computer network. The European Cybercrime Convention, which has become an international multilateral instrument to which the U.S. is signatory, requires signatories to enact laws that prevent unauthorized access. The best known statute of this sort in the United States is found in the Computer Fraud and Abuse Act (CFAA), although many states have their own versions of such statutes (18 U.S.C § 1030). The CFAA creates both civil and criminal causes of action for accessing computers without authorization, or in excess of authorization, in order to “obtain” or “alter” information. The CFAA also entails a damage requirement in a specific dollar amount of at least US\$5000; much like the damage requirement of its common law cousin, trespass to chattels, the CFAA requirement has been satisfied by showing lost employee time or business expenses related to the unwanted access. CFAA claims and trespass claims are frequently asserted together, as the elements of each type of claim require the same or similar factual showing (Galbraith, 2004).

This low threshold for a showing of intermeddling and of harm transformed trespass to chattels, and similarly CFAA violations, into the Internet’s all purpose legal claims, since effectively every use of a computer involves both the passage of electrons across its circuits, and the engagement of some memory or processor capacity. In previous work (Burk, 2000), I have criticized the use of trespass to chattels as an end-around legal strategy to protect content that could not be protected under copyright or other intellectual property regimes. In many of the reported cases, the assertion of trespass claims is clearly less about harm to or interference with the chattel, than about control over the use of the information residing on the chattel. Plaintiffs in such cases were generally the proprietors of publicly accessible servers who hoped to have their cake and eat it too: both to benefit from making the information on the servers publicly available, but also to control the uses to which the accessed information was put. The fiction of “trespass” to their computers provided a convenient theory by which to assert control. I have argued that either general public policy, or specific intellectual property doctrine, ought to prevent such end-runs around the limits of intellectual property law (Burk, 2000).

However, the use of trespass claims in the case of virtual worlds may be more appropriate than in the case of servers that are publicly available on the Internet. Multi-player games and other virtual world services are typically not openly accessible, but require some type of login or other gatekeeping access procedure. Many are subscription services. To the extent that such boundary mechanisms provide notice as to the perimeter of the resource, and

divide users engaging the resource from virtual passers-by, trespass claims seem less of an unbounded remedy in search of a legal harm. This is not to say that trespass claims in the context of virtual worlds are entirely free of the motivation for information control. Certainly the point of such claims is to prevent undesired manipulation of information exchanged with the proprietor's server. But avoiding damage to the integrity of the infrastructure and business model is a more plausible claim where the resource lies behind a technical perimeter than where it is accessible to the general public.

Gatekeeping procedures also provide an opportunity to alert the user to the conditions for access, and for the user to indicate awareness of resource boundary and the conditions that govern its use. The benefits of boundary maintenance and gatekeeping, however, may be double-edged. The downside of gatekeeping is closely related to the problem of privilege. Privilege negates a claim of trespass. Use of or contact with a chattel with permission of the owner is not intermeddling; authorized interaction cannot be trespass. In many past cases of computer trespass, privilege might have been inferred from the circumstances: the server was publicly available and the unwanted user was accessing the server along with the rest of the public (O'Rourke, 1998). Similarly, logon or gatekeeping procedures may exclude users who lack the proper access credentials, but they may also suggest that those within the perimeter are there by invitation, even if they succeed in wearing out their welcome sometime after they arrive.

In past computer trespass cases, the cure for an inference of privilege was taken to be notification (O'Rourke, 1998). An implied privilege may be explicitly revoked. Thus, many Web sites, whether openly available or password protected, relied upon their posted terms of service as explicit revocations of any implied privilege. In the case of sites that required login protocols, the terms could be made available, and acknowledgement of the terms mandatory, as part of the access protocol. But even openly accessible sites, with terms of service (ToS) posted somewhere on the site, would point to the ToS as notification of the terms or conditions under which access was permissible or not. Here again, the majority of games may tend to have a better argument that the ToS served as explicit notice: ToS located somewhere on an open Web site will not be viewed by users until they have actually accessed the site; ToS provided during a login procedure are more likely to have been noticed by the user.

Terms of service

In addition to their role as notice of trespass, ToS may also be relied upon by virtual world proprietors as creating separate contractual obligations on the part of users accessing the server [2]. The ToS may specify actions that the user is permitted or not permitted to take, quite apart from the dictates of copyright or other statutes of general application. Game proprietors may also rely on the ToS to provide contractual solutions to some of the intellectual property issues raised above. For example, to the extent that subscribers may have some copyright interest in the output of the game software, game proprietors purport to use the ToS to transfer such interests to themselves: the ToS may provide that any copyright vesting in the player is contractually transferred to the game owner.

In this capacity, the ToS on MMORPG and other Internet service Web sites are but the latest incarnation of standardized commercial "take it or leave it" contracts accompanying a wide variety of consumer transactions (Hillman and Rachlinsky, 2002). Such "boilerplate" or "adhesion" contractual terms are common in many types of commercial transactions, and courts have been increasingly willing to enforce them in the context of networked computer services, both in the United States and in the European Union (Lemley, 1999; Guibault, 2002). Software publishers years ago adopted such contracts as "shrinkwrap" licenses that were considered effective when consumers broke the shrinkwrap packaging on physical software media, or more recently "clickwrap" licenses considered effective when consumers click an "I agree" icon on the software interface. Some Web site operators have even asserted contractual terms by means of "webwrap" or "browsewrap" licenses that purport to be effective by virtue of the user having accessed the server where they are displayed.

But such "boilerplate" contracts face a conceptual problem under traditional theories of contract, which is that consumers typically neither read the fine print, nor when they do read the fine print, do they understand the terms stated. Contracts were traditionally viewed as agreements embodying a bargained-for exchange, but it is difficult to claim that shrinkwrap and clickwrap licenses meet this definition if the consumer has no meaningful opportunity to know what she is agreeing to, and if indeed there is no opportunity to bargain.

Standardized agreements are perhaps a commercial necessity; it is not feasible for producers to negotiate separate agreements with the millions of purchasers of mass-market products, but the agreements cannot be thought of in terms of classic contractual transactions (Radin, 2002).

Additionally, because they arise out of state law, adhesive contract cannot resolve copyright issues that lie as a matter of federal law — federal statutory requirements may preempt state contract solutions. For example, in the U.S., the copyright statute provides that exclusive rights may only be transferred by means of a “signed writing” (17 U.S.C. § 204). Initially, this required a hardcopy signature, but changes in federal law appear to permit electronic signatures to satisfy the statutory requirement (15 U.S.C. §§ 7001, 7006(5)). Thus, in some ToS situations, this requirement may be satisfied by the electronic version of a signature, such as clicking “I agree” or a similar affirmative signature cognate. Web sites or access logons where the ToS is merely displayed would not meet the requirement. And, even where an electronic signature is obtained, it may be unclear whether such a writing must be specific as to a particular work, or whether it may cover numerous or unspecified works. A major concern lies in the timing of the transfer; it is often unclear whether future works not in existence at the time the writing is executed can be transferred in this fashion. Consequently, the transfer of rights under standardized ToS under may be uncertain.

To maintain the viability of clickwrap and similar legal instruments in the face of these difficulties, a different theory has been adopted — which interestingly, has also become central tenet of open source licensing — that the standardized, unnegotiated shrinkwrap constitutes a conditional license; that is, not a bargained for exchange in the traditional sense of contract, but rather an agreement for the licensor not to sue under certain conditions (McGowan, 2001). The license constitutes a conditional waiver of the licensor’s exclusive rights. Thus the shrinkwrap becomes not so much an agreement between parties as a form of notice; not so much the terms of an exchange, but rather a statement or declaration of the terms under which the licensor will permit the Web site to be accessed, or under which licensor will permit copyrighted content to be manipulated, without triggering a lawsuit. This theory was in fact asserted by Blizzard as the basis for copyright infringement in the MDY case (*MDY Indus., LLC v. Blizzard Entertainment, Inc.*, 2009).

This licensing theory is not limited to a waiver of copyright; trespass and CFAA claims may rest on a similar theory of conditional, rather than contractual, access. Again, the licensing approach holds that the user is granted permission to access and use the virtual world provider’s equipment so long as the access and use remains within certain behavioral boundaries. Violation of those boundaries violates the terms under which access was granted, shifting the user’s access from authorized to unauthorized, or to access in excess of authorization. The violation of the license then becomes the basis for legal recourse by the provider.

Note that the concept of such licenses is predicated upon a set of legal fictions. The first is the fiction of assent: that by taking some action, such as clicking “I agree” or even by remaining connected to the service provider’s equipment, the user manifests assent to the terms of the license. The second is the related fiction of notice: that the user is provided by the fine print of the license with adequate notice as to what behavior is and is not within the terms of the license, such that unauthorized behavior constitutes a breach of the license, triggering legal liability. Neither of these fictions necessarily fits actual actions or expectations of the user, and neither necessarily lends itself to governance of the large and diverse populations interacting in virtual worlds.

Previous commentators have observed that shrinkwrap licensing essentially adopted a model that was developed for transactions between sophisticated buyers and the vendors of bundled software and mainframe or mini data processing systems (Lemley, 1995). That model was extended to mass-market sales of software, involving ordinary consumers with little sophistication regarding the technology they are purchasing, or the terms and conditions of the licensing model itself. Deployment of this model as the ToS of virtual worlds and gaming extends this type of instrument yet further from its origins to govern not simply a commercial transaction, but a set of complex social relations involving persistent real-time interactions of thousands of individuals (Dibbell, 2006; Benkler, 2006). In such a case, we might wonder whether the model has been extended too far from its original purposes to function effectively.

Authorization and authority

Certain themes should be apparent from this review of the different legal theories that might be asserted to exclude certain users or user behaviors from virtual worlds. The first common characteristic is that for most of these approaches, the game ToS serves as a linchpin. Copyright, trespass, and even anti-circumvention statutes define certain exclusive rights, but the allocation and disposition of such rights depends on the contractual terms by which the proprietor's server was accessed. In this regard, it is important to note that the ToS may be serving multiple if related legal functions. In conjunction with the copyright discussion above, the ToS in such cases might for some purposes constitute a "webwrap" license, but for purposes of trespass, the ToS might serve as notice against implied authorization for access.

The corollary theme to the centrality of the ToS is difficult set of questions regarding authorization. This is a common problem underlying each of the approaches reviewed here: assuming that the user has not hacked into the server, but has accessed the server via subscription or other legitimate protocol, does their access remain legitimate when their behavior is unwanted by the server proprietor? What precisely is the scope of permissible conduct by users who have accessed the servers of a virtual world provider?

Circumvention and control of access are defined by statute as actions that are dependent on the authority of the copyright owner. Circumvention is an action taken without authorization by the copyright holder, access to a work is controlled under the authority of the copyright holder (17 U.S.C. § 1201 (a)(3)(A), (B)). For example, in the case of modding, one might argue that a mod that disables or evades restrictive components of the WoW API would not constitute a DMCA violation if the interaction were authorized. One might infer such authorization from the game proprietor supplying the technical information for the interaction, or encouraging modding that included mods of this type, or even failing to object to such mods for a long period of time, especially if such mods were brought to the proprietor's attention.

Similarly, we have seen that authorized access cannot be trespass, so the ToS is relied upon to demarcate privileged and non-privileged access. The CFAA applies only to access without or in excess of authorization. But as Kerr (2003) has pointed out, the meaning of the terms "access" and "authorization" in such statutes is vague and indeterminate, sometimes having been interpreted as any interaction with the computer that is contrary to the owner's interests. Who defines those interests, and how a user might know what those interests might be, is left to *ex post* judicial determination.

In the context of copyright, authorization determines not only the disposition of works, but the classification and character of the work that emerges from game play; authorization demarcates the line between adaptation and infringement. Player's creative input, if authorized, may generate a derivative work (Burk, 2009). But if the players are not authorized to engage with the game's copyrighted material, then what might have been a derivative work or work of joint authorship becomes infringement; an adaptation in violation of the copyright holder's exclusive rights. In the course of normal game playing, one would expect the player-generated output to be authorized: generating an entertaining output is the point of playing, and the developer both expects and facilitates this outcome when making the game available. However, players manipulating the game's elements beyond the authorization given by the game developer may be creating an adaptation without the approval of the copyright holder.

These difficulties are heightened in the case of activities like modding, where a new work is generated actively and deliberately, rather than fortuitously in the course of regular game play. Optimally, of course, we would like authorization for a modder to develop and deploy add-ons to be explicit rather than tacit. Disputes would likely be fewer if the game proprietor gave clear permissions for various types of activity. This is at least in part the point of the ToS, attempting to spell out what actions are permissible and which aren't. But life and gaming are rarely so simple; as a practical matter, the proprietor likely cannot foresee or even stay abreast of all the different and ingenious modifications or behaviors players may develop.

Indeed, contract theory predicts that formal agreements will necessarily be incomplete — drafters can never predict all the possible contingencies that may arise under a contract; attempting to do so would entail prohibitively high transaction costs. In the case of virtual worlds, we can imagine the impracticality of proprietors attempting to draft increasingly lengthy and tortured language to cover the variety of possible actions that subscribers or participants might take while interacting with the provider's servers. Much of this drafting will occur after the fact, adding new language to include surprise activities that were unforeseen in the previous iteration of the ToS, hoping, if not to secure the barn door before the horse is gone, to at least to deter future equine hi-jinks.

Gaps in the ToS means that authorization may not be explicit. In the absence of an explicit agreement, we are instead forced to infer what player activity is likely to fall within or without the parties' expectations. The inference of authorization poses complex legal, factual, and practical difficulties. To draw such legal inferences, we look to the proprietor's actions, including inaction, to infer both the proprietor's likely intent regarding the activity, and to determine the user's reasonable actions in reliance on the proprietor's apparent intent. If the user reasonably relied on the proprietor's actions, then the proprietor's actual intent regarding the activity may be irrelevant. If the proprietor appears to have acquiesced in the activity, and players have come to rely on the game proprietor's inaction as tacit acceptance of the practice, that may constitute a defense to legal claims against the user. Users may even be entitled to continue activity that has become the norm, particularly if circumstances suggest that the activity has come or reasonably should have come to the proprietor's attention, in which case it may be difficult for the proprietor to later take a contrary position.

In this regard, it is important to note that the authorization regime we have just surveyed stands the traditional structure of contract on its head. Because contracts are inevitably incomplete, functioning contractual relationships often depend upon a "gap-filling" statute, such as copyright or trespass law, to cover situations that the parties did not anticipate. Copyright and similar property regimes serve as a default to allocate rights in the absence of contractual direction. But the licensing regime described above makes the applicability of the "gap-filling" statute itself dependant on the contract, with its inevitable gaps — a circular inquiry. When neither the "gap-filler" regime nor the contract are explicit about the definition of authorization, that definition will depend upon the more indeterminate inference of authorization.

Conclusion

A review of the various types of property claims that have been asserted to govern the interactions of virtual world users with the platforms they access suggests that these legal regimes are not well suited to such governance problems. As a specific example, we can see that the difference between sanctioned "modding" and unsanctioned "hacking" is one of degree rather than kind. The nebulous line separating the two, at least for legal purposes, is the line demarcating authorization. Any of the legal claims reviewed here depends upon user authorization, but that status is in turn reliant upon the license by which the user accesses the platform, including both an explicit ToS and implicit norms and courses of conduct between user and proprietor. As a consequence, asserting the types of claims reviewed here for purposes of governance will inevitably result in messy *post hoc* determinations as to the limits of authorization.

This is by no means to say that intellectual property regimes have no role in supporting and fostering the development of virtual world infrastructure. Certainly CFAA or trespass claims are appropriate for clear cases of computer intrusion, where access was never authorized; certainly anti-circumvention claims are appropriate where breach of technical protections rather than breach of contract is at issue. Certainly copyright is appropriate to prevent misappropriation of the software or graphics associated with virtual worlds — the exclusive rights in intellectual property are, for example, likely appropriate tools to manage or deter the proliferation of private servers, which host copied game software as a substitute for the game proprietor's own servers, for which they were intended, rather than for crowd control on virtual world servers.

About the author

Dan Burk is the Chancellor's Professor of Law at the University of California at Irvine, where he is a founding member of the law faculty. An internationally prominent authority on issues related to high technology, he lectures, teaches, and writes in the areas of patent, copyright, electronic commerce, and biotechnology law. Professor Burk holds a B.S. in Microbiology (1985) from Brigham Young University, an M.S. in Molecular Biology and Biochemistry (1987) from Northwestern University, a J.D. (1990) from Arizona State University, and a J.S.M. (1994) from Stanford University. He has served as a legal advisor to a variety of private, governmental, and intergovernmental organizations, including the American Civil

Notes

1. Lastowka, 2008, p. 905.
2. Duranske, 2008, p. 127.

References

15 U.S.C. § 7001 (2006).
15 U.S.C. § 7006(5) (2006).
17 U.S.C. § 101 (2006).
17 U.S.C. § 102 (2006).
17 U.S.C. § 204 (2006).
17 U.S.C. § 1201 (a)(3)A), (B) (2006).
18 U.S.C § 1030 (2006).
Yochai Benkler, 2006. "There is no spoon," In: Jack Balkin and Beth Noveck (editors). *The state of play: Law, games, and virtual worlds*. New York: New York University Press, pp. 180–186.
Blizzard Entertainment, 2009. "UI add-on development policy," at <http://www.worldofwarcraft.com/policy/ui.html>, assessed 31 March 2010.
Blizzard Entertainment, Inc. v. In Game Dollar, LLC, SACV07–0589 JVS (C.D. Cal. Jan. 28, 2008).
Dan Burk, 2009. "Copyright and paratext in computer gaming," In: Charles Wankel and Shaun Malleck (editors). *Emerging ethical issues of life in virtual worlds*. Charlotte, N.C.: Information Age Publishing, pp. 33–53.
Dan Burk, 2008. "Information ethics and the law of data representations," *Ethics and Information Technology*, volume 10, numbers 2–3, pp. 135–147.
Dan Burk, 2006. "Electronic gaming and the ethics of information ownership," *International Review of Information Ethics*, volume 4, at <http://www.i-r-i-e.net/inhalt/004/burk.pdf>, assessed 25 April 2010.
Dan Burk, 2005. "Legal and technical standards in digital rights management technology," *Fordham Law Review*, volume 74, pp. 537–573.
Dan Burk, 2000. "The trouble with trespass," *Journal of Small and Emerging Business Law*, volume 4, pp. 27–56.
Chamberlain Group, Inc. v. Skylink Technologies, Inc., 381 F.3d 1178 (Fed. Cir. 2004).
Kevin E. Collins, 2006. "Cybertrespass and trespass to documents," *Cleveland State Law Review*, volume 54, pp. 41–68.
Mia Consalvo, 2007. *Cheating: Gaining advantage in videogames*. Cambridge, Mass.: MIT Press.
Davidson & Associates v. Internet Gateway, 334 F. Supp. 2d 1164 (E.D. Mo. 2004).
Julian Dibbell, 2006. "Owned! Intellectual property in the age of eBayers, gold farmers, and other enemies of the virtual state," In: Jack Balkin and Beth Noveck (editors). *The state of play: Law, games, and virtual worlds*. New York: New York University Press, pp. 137–145.
Benjamin Duranske, 2008. *Virtual law: Navigating the legal landscape of virtual worlds*.

Chicago: ABA Press.

Christine Galbraith, 2004. "Access denied: Improper use of the Computer Fraud and Abuse Act to control information on publicly accessible Internet Websites," *Maryland Law Review*, volume 63, pp. 320–368.

James Grimmelman, 2006. "Virtual power politics," In: Jack Balkin and Beth Noveck (editors). *The state of play: Law, games, and virtual worlds*. New York: New York University Press, pp. 146–157.

Lucie Guibault, 2002. *Copyright limitations and contracts: An analysis of contractual overridability of limitations on copyright*. Boston: Kluwer.

Robert Hillman and Jeffrey Rachlinsky, 2002. "Standard form contracting in the electronic age," *New York University Law Review*, volume 77, pp. 429–495.

Orin Kerr, 2003. "Cybercrime's scope & interpreting 'access' and 'authorization' in computer misuse statutes,," *New York University Law Review*, volume 78, pp. 1,596–1,668.

Yong Ming Kow and Bonnie Nardi, 2010. "Who owns the mods?" *First Monday*, this issue.

Greg Lastowka, 2008. "User-generated content and virtual worlds," *Vanderbilt Journal of Entertainment and Technology Law*, volume 10, pp. 893–917.

Mark Lemley, 1999. "Beyond preemption: The law and policy of intellectual property licensing," *California Law Review*, volume 87, pp. 111–172.

Mark Lemley, 1995. "Shrinkwraps in cyberspace," *Jurimetrics Journal*, volume 35, pp. 311–323.

Lawrence Lessig, 1999. *Code and other laws of cyberspace*. New York: Basic Books.

Lewis Galoob Toys, Inc. v. Nintendo of America, Inc., 964 F.2d 965 (9th Cir. 1992).

Lexmark International, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004).

MAI Systems Corp. v. Peak Computer, Inc., 991 F.2d 511 (9th Cir. 1993).

David McGowan, 2001. "Legal implications of open source software," *University of Illinois Law Review*, volume 2001, pp. 241–304.

MDY Indus., LLC v. Blizzard Entertainment, Inc., 616 F. Supp. 958 (D. Ariz. 2009).

MDY Indus., LLC v. Blizzard Entertainment, Inc., 2008 U.S. Dist. LEXIS 97696 (D. Ariz., Sept. 29, 2008).

Midway Mfg. Co. v. Arctic Int'l, Inc., 704 F.2d 1009, 1011-12 (7th Cir. 1983).

Microstar v. Formgen, Inc., 154 F.3d 1107 (9th Cir. 1998).

Maureen O'Rourke, 1998. "Fencing cyberspace: Drawing borders in a virtual world," *Minnesota Law Review*, volume 82, pp. 609–704.

Hector Postigo, 2010. "Modding to the big leagues: Exploring the space between modders and the game industry," *First Monday*, this issue.

Margaret Radin, 2002. "Online standardization and the integration of text and machine," *Fordham Law Review*, volume 70, pp. 1,125–1,146.

R. Anthony Reese, 2003. "Will merging access controls and rights controls undermine the structure of anticircumvention law?" *Berkeley Technology Law Journal*, volume 18, pp. 619–665.

Joel Reidenberg, 1998. "Lex informatica: The formulation of information policy rules through technology," *Texas Law Review*, volume 76, pp. 553–584.

Pamela Samuelson, 1995. "Intellectual property and the digital economy: Why the anticircumvention regulations need to be revised," *Berkeley Technology Law Journal*, volume 14, pp. 519–568.

Pamela Samuelson, 1993. "Fair use for computer programs and other copyrightable works in digital form: The implications of Sony, Galoob and Sega," *Journal of Intellectual Property Law*, volume 1, pp. 49–118.

Pamela Samuelson and Suzanne Scotchmer, 2002. "The law and economics of reverse engineering," *Yale Law Journal*, volume 111, pp. 1,575–1,663.

Walt Scacchi, 2010. "Computer game mods, modders, modding, and the mod scene," *First Monday*, this issue.

Stern Elecs., Inc. v. Kaufman, 669 F.2d 852, 855-56 (2d Cir. 1982).

T.L. Taylor, 2006a. *Play between worlds: Exploring online game culture*. Cambridge, Mass.: MIT Press.

T.L. Taylor, 2006b. "Does WoW change everything? How a PvP server, multinational player base, and surveillance mod scene caused me pause," *Games and Culture*, volume 1, number 4, pp. 318–337.

Williams Elec., Inc. v. Arctic Int'l, Inc., 685 F.2d 870, 874 (3d Cir. 1982).