University of Chicago Legal Forum

Volume 2008 | Issue 1 Article 11

Criminal Law in Virtual Worlds

Orin S. Kerr
Orin.Kerr@chicagounbound.edu

Criminal Law in Virtual Worlds†

Orin S. Kerr‡

In the 1990s, the notion of "cyberspace" as a virtual world captivated internet users and scholars alike.[1] The metaphor was attractive in part because accessing the internet really did feel like entering a new world. In those days, internet users connected their modems to phone jacks, dialed access numbers, and waited for the familiar beeps and white noise to bring them up the ramp from the physical world to the information superhighway.

In the last decade, the virtual metaphor of cyberspace has seemed increasingly outdated. Today the internet is everywhere. It is integrated into the physical world through wireless networks, BlackBerries, and cell phones. Most internet users no longer think of spending time in "cyberspace." Instead, the internet comes to them. Connectivity is the norm, and most users experience using the internet as a connection to services rather than entrance into cyberspace.

The major exception to this trend has been the increasingly popular computer programs known as "virtual worlds," such as the now-popular Second Life.[2] These programs have millions of regular players and, for many players, have managed to make the promise of cyberspace a reality.[3] The popularity of virtual worlds has convinced some scholars that they are the next big thing: we better be ready to deal with law in virtual worlds,

---

‡ Professor, George Washington University Law School. Thanks to Greg Lastowka, Chris Yoo, Anthony Rickey, Justin Serafini, and the participants in the *University of Chicago Legal Forum* symposium for thoughtful comments.

[1] See, for example, Lawrence Lessig, *The Zones of Cyberspace*, 48 Stan L Rev 1403, 1403–06 (1996) (discussing how to think about the relationship between virtual worlds and the actual world at a time when "our understanding of what [cyberspace] will become is just beginning").

[2] See <http://secondlife.com> (last visited Mar 31, 2008).

[3] Paul R. La Monica, *Life beyond Second Life*, available at <http://money.cnn.com/2007/06/14/news/companies/virtualworlds/index.htm> (last visited Mar 31, 2008) (discussing the "growing popularity of Second Life and other online worlds").

the thinking goes, because it will soon be tremendously important to millions of Americans. I'm not sure this is true, but if it is, it raises a very interesting (and even fun) legal question:[4] If virtual worlds continue to grow, and they do eventually seem like a true "virtual world" instead of a mere game, how will the law apply in virtual worlds?

This Article will focus on one aspect of the law of virtual worlds that has received only modest attention: criminal law in virtual worlds.[5] It considers two questions. The first is descriptive: When does conduct by an online player in a virtual world game trigger liability for a real-world crime? The second question is normative: In the future, will new criminal laws be needed to account for new social harms that occur in virtual worlds?

Part I of the Article argues that existing laws regulate virtual worlds with little or no regard to the virtual reality they foster. Criminal law tends to follow the physical rather than the virtual: it looks to what a person does rather than what the victim virtually perceives. This dynamic greatly narrows the role of criminal law in virtual worlds. Existing law will not recognize virtual murder, virtual threats, or virtual theft. While these "offenses" may appear to users as the cyber-version of traditional crimes, existing law requires proof of physical elements rather than virtual analogies. With a few exceptions—and the notable uncertainty of the Computer Fraud and Abuse Act (CFAA)[6]—this physical perspective leaves criminal law mostly on the sidelines in virtual worlds. Virtual worlds will be regulated like any other game, but their "virtualness" normally will have no independent legal resonance from the standpoint of criminal law.

Part II turns to the normative question: Are new laws needed? It concludes that legislatures should not enact new criminal laws to account for the new social harms that may occur in virtual worlds. Virtual worlds at bottom are computer games,[7]

---

[4] See, for example, Jack Balkin, *Virtual Liberty: Freedom To Design And Freedom To Play In Virtual Worlds*, 90 Va L Rev 2043, 2045 (2004) ("Precisely because virtual worlds are fast becoming important parts of people's lives, and because they are likely to be used for more and more purposes in the future, legal regulation of virtual worlds is inevitable.").

[5] The primary scholarly work that focuses on this question is Dan Hunter and Greg Lastowka, *Virtual Crimes*, 49 NY L Sch L Rev 293, 294 (2004–05) (exploring the issue of whether "non-consensual appropriation and destruction of virtual properties . . . might be seen as truly criminal"). As this Article was going to print, I learned of a still-forthcoming article that also addresses this topic. Bart J.V. Keupink, *Virtual Criminal Law in Boundless New Environments*, 6 Intl J Tech Transfer and Commercialisation 160 (2007).

[6] Computer Fraud and Abuse Act, 18 USC § 1030 (2000 & Supp 2002).

[7] I use the word "game" in a broad sense to refer to entertainment environments

and games are artificial structures better regulated by game administrators than federal or state governments. The best punishment for a violation of a game comes from the game itself. This does not mean that online virtual worlds are unimportant. To the contrary, games can be enormously important to an individual's identity. As any sports aficionado knows, a game can be a source of tremendous pride, happiness, and (especially for Mets fans) disappointment. But criminal law does not regulate all important things. Criminal law is a blunt instrument that should be used only as a last resort. The state's power to deny individuals their freedom is an extraordinary power, and it should be reserved for harms that other mechanisms cannot remedy.

Online virtual worlds may seem real to some users, but unlike real life, they are mediated by game administrators who can take action with consequences internal to the game. Internal virtual harms should trigger internal virtual remedies. It is only when harms extend outside the game that the criminal law should be potentially available to remedy wrongs not redressable elsewhere.

I. HOW DOES CRIMINAL LAW REGULATE CONDUCT IN VIRTUAL WORLDS?

The tension between virtual and physical perspectives is a recurring theme in the law of the internet.[8] Network transactions can be modeled in two ways: virtually and physically. The virtual approach looks at the virtual facts experienced by a user. Modeling internet transactions from a virtual perspective interprets the facts of the internet from the perspective of an internet user.[9] From this perspective, a user enters a virtual world. He might visit stores to make purchases, enter a virtual chat room to speak to other users, or go to virtual concerts to hear music.

The physical perspective is different. Modeling internet transactions from a physical perspective focuses on what actually

---

rather than in a narrow sense to refer to competitive games. Many virtual worlds do not provide users with a specific purpose such as acquiring property or points. In my view, however, they still count as games. For the distinction between virtual worlds that are more or less structured and game-like, see Bryan T. Camp, *The Play's The Thing: A Theory of Taxing Virtual Worlds*, 59 Hastings L J 1, 4–8 (2007).

[8] Consider Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 Georgetown L J 357 (2003) (discussing the choice between virtual and physical approaches to applying law to the internet).

[9] Id at 359–60 (describing an "internal perspective" as one that accepts as reality those things the participants in a virtual world perceive to be happening).

happens rather than what a user perceives.[10] From this perspective, a user doesn't enter a virtual world. Rather, he logs on to a server located somewhere in the world and then sends and receives electronic communications. The focus stays on what actually occurs via the physical network, rather than on virtual analogies based on user perceptions.

The distinction between virtual and physical approaches is critical to understanding how criminal law applies to virtual worlds. Criminal laws traditionally focus on the physical perspective rather than the virtual one. Criminal laws prohibit committing a series of elements, and those elements must be construed strictly.[11] Whether a person has violated a particular crime hinges on whether the elements have been satisfied. The elements of crimes tend to be physical: they require physical acts, communications between physical places, and impact on real physical people. For example, the crime of homicide prohibits causing the death of a person, not an avatar.[12] The crime of trespass requires physical entrance of a person into a space rather than some kind of virtual entry.[13]

The fact that traditional crimes generally follow a physical perspective means that the virtual meaning of conduct in online games is irrelevant for most criminal laws. What matters is what actually happens from a physical perspective instead of what a virtual world user perceives. Traditional crimes committed using the intermediary of virtual worlds will still be crimes; money laundering via a virtual world economy is still money laundering. But misconduct that draws social significance from its meaning in virtual reality normally will have no resonance with criminal statutes. Virtual rape is not rape, as there is no actual person who is physically violated. It is a story (or an image) of a rape and no more.[14] Although an act may seem like the "cyber"

---

[10] Id at 360 (describing an "external perspective" as one that takes as reality the actual interactions with a computer and a network).

[11] Under the rule of lenity, "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity." *Rewis v United States*, 401 US 808, 812 (1971).

[12] See, for example, Model Penal Code § 210.1. An avatar is "an electronic image that represents and is manipulated by a computer user." See Merriam-Webster Online Dictionary, available at <http://www.m-w.com/dictionary/avatar> (last visited Mar 31, 2008).

[13] Charles Torcia, Wharton's Criminal Law § 331 at 202 (14th ed 1980) (noting that "part of the defendant's person pass[ing] the line of the threshold" is ordinarily required under criminal trespass laws).

[14] See Kerr, 91 Georgetown L J at 372 n 66 (cited in note 8) (describing a situation in a virtual game where one user manipulated the game so that his virtual character raped other characters within the game).

equivalent of a crime, the law focuses on real physical elements rather than virtual analogues.

Consider the federal crime of sending a threat in interstate commerce.[15] The statute requires sending a threat that actually crosses state lines; whether a user might perceive the threat as "interstate" in nature is irrelevant. A young man named Matthew Kammersell learned this lesson when he sent a threatening AOL instant message ("IM") to his girlfriend a few miles away.[16] Although both he and his girlfriend were in Utah, the fact that the IM was routed through AOL's servers in Virginia made the threat an interstate threat.[17] What mattered was the communication's physical path, not Kammersell's perception.

The key implication of the physical perspective is that most misconduct internal to virtual worlds will not count as criminal activity under physical criminal laws. For example, imagine one avatar "steals" valuable data from another avatar. Is this theft? A user might think so, but the law ordinarily won't support that perception. The reason is that the "virtual theft" will often be perceived as part of the rules of the game. At bottom, virtual worlds are games; individuals agree to play them, whether for fun or profit, just like other games. And like other games, virtual world games have artificial rules about what players can or cannot do.[18] Therefore, if what appears to be "theft" from a virtual perspective is actually a permitted move under the rules of that game, it is not any kind of theft from the physical perspective of the criminal law. As Dan Hunter and Greg Lastowka note, "[t]he norms of game play supersede the standard rules of society."[19]

A string of century-old card game cases from Texas illustrate the point.[20] In these cases, individuals lost money in card games

---

[15] 18 USC § 875(c) (2000) (prohibiting anyone from "transmit[ting] in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another").

[16] See *United States v Kammersell*, 196 F3d 1137, 1139 (10th Cir 1999) (holding that an instant message sent from Utah to Virginia and back to Utah is an interstate communication, even though no one outside of Utah saw or could have seen the message).

[17] Id ("A threat that was unquestionably transmitted over interstate telephone lines falls within the literal scope of the statute and gives rise to federal jurisdiction.").

[18] For an example of such a set of rules, see Second Life's Community Standards, available at <http://secondlife.com/app/help/rules/cs.php> (last visited Mar 31, 2008) (prohibiting things such "shooting, pushing, or shoving . . . in a Safe Area," and entitling users "to a reasonable level of privacy with regard to their Second Lives").

[19] Hunter and Lastowka, *Virtual Crimes* at 305 (cited in note 5).

[20] *Hernandez v State*, 63 SW 320 (Tex Crim App 1901) (plaintiff alleged theft after players would not return his bets, though he claimed he was framed as a cheater in a card game); *Palmer v State*, 160 SW 349 (Tex Crim App 1913) (defendant accused of rob-

and tried to keep the money they had lost, either because they thought the game was rigged or because they claimed to have been cheated.[21] When charged with robbery or theft, they argued that the money belonged to them and therefore they had committed no crime.[22] The key point for our purposes is that the courts always deferred to the announced rules of the game to determine who owned what.[23] According to the courts, title did not pass when the prior owner put his money into the common pot: at that point the owner "merely parted with the temporary possession, undertaking to win the 'pot' fairly in accordance with the rules of the game."[24] On the other hand, title passed when a player played his hand and simply lost under the established rules: "If, under the rules of the game they were playing, the [victim] had won the money, and it had passed into his hands under the rules of the game," then ownership in the money passed from the loser to the winner.[25] The rules of the game governed.

Where is the line of criminality if the rules of the game trump? Any kind of cheating should suffice. For example, in one Texas case a man named Dorsey dealt a hand in a card game that required 40 cards.[26] Dorsey told Temple that there were 40 cards in the deck, and Temple agreed to play based on Dorsey's representation.[27] Temple began to lose, and he suspected that Dorsey was cheating and that the deck had 36 cards instead of 40.[28] Temple grabbed the money he had lost and ran out.[29] Temple eventually was caught and charged with robbery, and he sought and was refused a jury instruction on his view that Dor-

---

bery after taking money back from a gambling table where he claims he was cheated); *Temple v State*, 215 SW 965 (Tex Crim App 1919) (appellant charged with theft after taking his money back from a card game where the deck was rigged).

[21] See, for example, *Temple*, 215 SW at 965 ("Appellant's theory was that Dorsey, who was dealing, represented to him that there were 40 cards in the deck, and that he believed that to be true, when, as a matter of fact it was false, Dorsey having but 36 cards in the deck.").

[22] Id ("appellant . . . presents here the view that, if the appellant was induced to part with his money and place it under the control of Dorsey through his deception and fraud, he would not be guilty of the offense of robbery in regaining possession of it").

[23] See, for example, *Palmer*, 160 SW at 352 ("If, under the rules of the game they were playing, the banker had won the money, and it had passed into his hands under the rules of the game, and appellant had subsequently taken the money by force or violence, a case of robbery would be complete.").

[24] *Hernandez*, 63 SW at 321.

[25] *Palmer*, 160 SW at 352.

[26] *Temple*, 215 SW at 965.

[27] Id.

[28] Id.

[29] Id.

sey had cheated him.[30] The Court of Appeals reversed, finding that, if Dorsey had used 36 cards instead of 40, taking the money from Dorsey was not a crime.[31] If Temple's facts were correct, the court concluded, "he was induced to part with his money, not perforce of any game played according to its rules, but by reason of the false and fraudulent representations of Dorsey."[32]

Yet if the rules of the game trump, this raises the important question of what "the rules of the game" in a virtual world actually are. The rules of card games ordinarily are clear. The choices remain narrow and bounded. Each player has a set of cards, and clear rules govern when a player can add or subtract cards. In contrast, virtual worlds are open. In a practical sense, a user has an infinite number of moves he can make. Which moves are permitted and which are not may be difficult to know. In this setting, how should courts determine "the rules?"

Similar issues have arisen occasionally in the context of sporting events. Consider an example from a professional hockey game. In February 2000, Marty McSorley of the Boston Bruins used his hockey stick to hit Vancouver Canucks player Donald Brashear in the head.[33] Brashear fell and suffered a concussion and later experienced memory loss from the incident.[34] McSorley was charged in court in British Columbia with assault on the theory that his hitting Brashear was beyond the rules of the game.[35] The trial judge agreed, finding that McSorley's conduct was beyond the violence that is a part of the game of professional hockey.[36] The judge relied on a Canadian Supreme Court ruling arising from a brawl which held that people cannot consent to serious harm being inflicted upon them, even if they have consented to some physical contact.[37] Applying that reasoning to

---

[30] *Temple*, 215 SW at 966.

[31] Id.

[32] Id.

[33] Tom Spousta, *McSorley Found Guilty; No Jail Time*, New York Times D7 (Oct 7, 2000).

[34] Gregg Joyce, *McSorley Guilty of Assault, But Gets Conditional Discharge*, The Record A01 (October 7, 2000).

[35] Ron Jouard, *McSorley Found Guilty of Assault with Weapon*, (Oct 17, 2000), available at <http://www.defencelaw.com/hockey-assault.html> (last visited Mar 31, 2008).

[36] Id ("The court found McSorley guilty of assault with a weapon, observing, 'Every time a player uses a stick to apply force to another player, the stick is being used as a weapon and not to direct the puck as it was intended to do.'").

[37] Jouard, *McSorley Found Guilty of Assault with Weapon* (cited in note 35) ("the victim's consent to a fair fight did not preclude commission of the offence of assault"), citing *R v Jobidon*, 2 SCR 714, 715 ("the scale tips heavily against the validity of a person's consents to the infliction of bodily injury in a fight").

McSorley's attack on Brashear, the judge held that McSorley's conduct was beyond the game because McSorley had targeted Brashear's head.[38] It would have been a different case if McSorley had aimed for Brashear's shoulder: "[I]f the slash was intended for the shoulder, delivered with the intention of starting a fight," the judge wrote, "my conclusion would be that it was within the common practices and norms of the game" and therefore not an assault.[39]

How might courts determine the "common practices and norms" of virtual worlds? One possibility is that courts will recognize Terms of Service ("ToS") and End-User License Agreements ("EULAs") as controlling, at least when they are clear. The rules of the game will become whatever the game company says they are, much like the rules of a poker game are announced by the house. Courts could assume that anything permitted by code that is not forbidden by the EULAs or ToS is part of the game. Alternatively, courts might try to rely on widely accepted norms of usage among gamers to determine those rules.[40] That is, courts could look to how particular games are normally played, much like the McSorley judge looked to social understandings of hockey to rule his conduct out of bounds.

Although these standards will often lead courts to have a hands-off approach to virtual misconduct, I want to make clear that it is only the "virtualness" of the misconduct that is at issue here. Misconduct that goes beyond the virtual world will trigger criminal liability just as it would in the real world. A recent arrest in Holland provides a helpful illustration. According to news reports, a teenager created fake websites that tricked users into believing that it was a login page for a virtual world game called Habbo Hotel.[41] Users disclosed their user names and passwords to the fake website, and the teenager allegedly logged onto the users' accounts and gave away their virtual furniture to him and his friends.[42] Within the Habbo Hotel virtual environment, virtual furniture could only be purchased with real money and

---

[38] Jouard, *McSorley Found Guilty of Assault with Weapon* (cited in note 35) ("[Players] cannot validly consent to serious violence that clearly extends beyond the ordinary norms of conduct.").

[39] Id.

[40] See, for example, Buster Olney, *Sports of the Times: It's Time for Players To Police Themselves*, New York Times D5 (June 3, 2002)

[41] *Virtual Theft Leads to Arrest*, Nov 14, 2007, available at <http://news.bbc.co.uk/1/hi/technology/7094764.stm> (last visited, Mar 31, 2008).

[42] Id.

could not be "stolen" by other users: the sum of all the furniture that the teenager moved was apparently purchased for thousands of dollars.[43] This conduct properly led to criminal charges because it was an actual theft, not a virtual representation of one.[44] The game itself did not let users transfer property. Rather, the unauthorized use of a password let the teenager access other users' accounts and drain the account of valuable items.[45] This is a traditional theft, closely analogous to often-prosecuted thefts involving unauthorized use of credit cards and ATM cards.[46]

I will end this part of the Article by mentioning the usual wildcard in any discussion of computer crime law: the federal unauthorized access statute, often referred to as the Computer Fraud and Abuse Act ("CFAA").[47] As I have detailed elsewhere,[48] this statute has become the law that threatens to swallow the internet. Precedents on the books in the civil context suggest that it could be applied remarkably expansively to prohibit a very wide range of conduct on the criminal side.[49] The First Circuit's decision in *EF Cultural Travel BV v Explorica*[50] demonstrates the problem. In that case, the court adopted a contractual view of Congress's prohibition on "exceed[ing] authorized access" to a computer.[51] Violating a contractual term to access a website triggered the criminal law.[52]

If adopted widely, this notion would mean that almost all user conduct that violates the ToS or EULA would also trigger felony criminal liability under the CFAA, subject, perhaps, to a

---

[43] Id.

[44] Id ("It is a theft because the furniture is paid for with real money.").

[45] *Virtual Theft Leads to Arrest* (cited in note 41) ("[T]he only way to be a thief in Habbo is to get people's usernames and passwords and then log in and take the furniture.").

[46] Consider *People v Whight*, 43 Cal Rptr 2d 163 (Cal App 1995) (concluding that intentional use of an ATM to withdraw funds from empty account due to error in processing services amounts to theft by false pretenses).

[47] 18 USC § 1030 (2000 & Supp 2002).

[48] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 NYU L Rev 1596 (2003).

[49] Id at 1598 ("[U]nauthorized access statutes broadly criminalize the law of contract involving the use of computers.").

[50] 274 F3d 577 (1st Cir 2003).

[51] Id at 582 (affirming the district court's conclusion that appellees will likely succeed on the merits of their CFAA claim based on an analysis of the confidentiality agreement between the parties).

[52] This theory of contract-based criminal liability, with analysis of *EF Cultural Travel BV v Explorica Inc*, is explored in depth in Orin S. Kerr, *Computer Crime Law* ch 2 at 54–64 (Thomson/West 2006) (section analyzing contract-based restrictions in considering what constitutes authorization).

"public policy" exception that might not pay attention to some conditions in such contracts.[53] Unsurprisingly, several legal disputes involving virtual worlds have raised CFAA claims, although so far none have been resolved by the courts.[54]

The implications of this theory on criminal law in virtual worlds would be profound. At the same time, they seem to be no more profound here than in any other context online. If section 1030 becomes the statute that swallows the internet, the fact that it will swallow virtual worlds along with the rest of the internet says nothing in particular about virtual worlds. As a result, this review of how current criminal law regulates virtual worlds need only end with a caveat: the answer depends heavily on the unsettled scope of 18 USC § 1030.

II. HOW SHOULD CRIMINAL LAW APPLY TO CONDUCT IN VIRTUAL WORLDS IN THE FUTURE?

Let's turn from the descriptive question to the normative one. Are new criminal laws needed to account for the new social harms that occur in virtual worlds? At first blush, this may seem like a strange question. Virtual worlds are in their relative infancy. In the United States, they remain largely the domain of computer geeks,[55] and most look more like bad cartoons than anything approaching "reality." As a result, imagining new criminal laws for virtual worlds may seem fanciful at best. But imagine a future in which this no longer remains true. Imagine a virtual reality of virtual worlds that appear quite real—worlds that look, feel, and sound pretty much like the real thing. If such a future comes to pass, will new criminal laws be needed to regulate virtual harms in virtual worlds?

I think the answer is "no." The reason is not that misconduct in virtual worlds will prove unimportant. If this future comes to pass, we will presumably value our experiences in virtual worlds

---

[53] The First Circuit hinted at this in a subsequent case, *EF Cultural Travel BV v Zefer Corp*, 318 F3d 58, 62 (1st Cir 2003) ("Whether public policy might in turn limit certain restrictions is a separate issue.").

[54] Examples include two lawsuits brought by Blizzard against gold farmers in World of Warcraft. See *Blizzard Entertainment, Inc v In Game Dollar, LLC*, No. 07-0589 (C D Cal 2007); *MDY Indus, LLC v Blizzard Entertainmentt, Inc*, No 06-2555 (D Ariz 2006). In addition, Linden Lab (Second Life) raised CFAA arguments in its counterclaim against Marc Bragg. However, the case was settled, so no court ever addressed the issue. See Adam Reuters, *Linden Lab Settles Bragg Lawsuit*, Reuters Second Life News Center (Oct 4, 2007), available at <http://secondlife.reuters.com/stories/2007/10/04/linden-lab-settles-bragg-lawsuit/> (last visited Apr 2, 2008). Thanks to Greg Lastowka for the examples.

[55] I mean that in the most endearing sense.

much as we do in traditional worlds. Rather, the reason is that virtual worlds at bottom are computer games, and games are artificial structures better regulated by game administrators than governments. Online virtual worlds may someday seem real, but unlike real life they are mediated by game administrators that can take action with consequences internal to the game. Game administrators do not merely act like governments in virtual worlds: they act like gods. They can punish users by changing their virtual environment or even banning them.[56] They can restore life and hit "reset" to start a user over again from scratch.[57]

Given their power to control whatever happens in online environments, game administrators should control and regulate virtual misconduct instead of governments. Traditional governments can continue to deal with non-virtual harms arising out of virtual worlds, such as the theft of virtual furniture in Habbo Hotel. But misconduct arising only in a virtual sense should remain the domain of game administrators.

The problem, in part, is that criminal law provides a terribly blunt and awkward instrument for social control. Criminal law looks powerful and effective on TV: Episodes of *Law & Order* are ubiquitous, and all is well when the bad guy gets locked away. But substantive criminal laws rarely provide a nuanced response to social harms. In the real world, the difficulty of investigating crimes and the personal and societal costs of punishment make criminal punishment a last recourse rather than the front line of defense.

This is a particularly serious problem in the case of computer crimes generally, and virtual misconduct specifically. Consider just a few practical problems inherent in the use of criminal laws to punish online misconduct. First, it must be technically possible to locate the wrongdoer. A clever suspect who wants to commit a crime online can take steps to avoid detection and capture. He can use proxy servers, hacked accounts, and other tricks to disguise his identity and whereabouts; a clever wrongdoer ordinarily will not get caught.

In part, this is a problem for all online investigations: The government usually catches only the dumb ones. Online, the

---

[56] See, for example, *Second Life Terms of Service*, available at <http://secondlife.com/corporate/tos.php> (last visited Mar 31, 2008) ("All aspects of the Service are subject to change or elimination at Linden Lab's sole discretion.").

[57] Id ("All aspects of the Service are subject to change or elimination at Linden Lab's sole discretion.").

tools of criminal investigations are cumbersome and inefficient; user mechanisms for disguising identity are easy. But it's also a particular problem with virtual harms because depending on the virtual world's logging software, and the extent of the wrongdoer's efforts to cover his tracks, there may or may not be an obvious trail of money or contraband for the police to follow. Even if governments enact new criminal laws that broadly regulate user conduct in virtual worlds, those laws will have little to no effect if wrongdoers know that the governments have very little chance of identifying and capturing them.

Second, government investigators must have jurisdiction to investigate criminal activity and resources to invest in each individual case. It is easy for Congress to draft a broad statute with wide extraterritorial application, and Congress has generally done so for computer-related crimes.[58] But this hardly addresses the bigger problem. Individuals in a virtual world could be anywhere, and extraterritorial evidence collection is quite cumbersome. A police officer in Los Angeles has little way of helping a Los Angeles citizen who was injured by someone in Russia through a server in the Netherlands. Extraterritorial evidence collection and extradition are both possible, at least in appropriate crimes, but these processes tend to be complex, resource-intensive, and unreliable. Such procedures work well in high-profile cases that draw intense government interest, but they often block investigations into low-level offenses.[59]

Imagine that a wrongdoer is identified and captured, and then is extradited or voluntarily agrees to come to the jurisdiction investigating the offense. What then? The primary remedies of the criminal law tend to be narrow and specific: fines and jail time. Jail time would prove an awkward remedy for new virtual crimes. What new virtual crime could be so severe that it does not fit into existing law and goes beyond the powers of game administrators to remedy—so much that deterrence or retribution justify putting the virtual wrongdoer in a real-life physical prison? It is hard to imagine such an offense.

---

[58] See Orin S. Kerr, *Computer Crime Law* ch 7 at 582–84 (cited in note 52) (discussing the scope of 18 USC § 1030 under the broadened definition of "protected computer" found in 18 USC § 1030(e)(2), as amended in 2001).

[59] See *Panel: Cybercrimes And The Domestication Of International Criminal Law*, 5 Santa Clara J Intl L 432, 442 (2007) (statement of Assistant United States Attorney Elena Duarte) ("For serious cybercrimes, the United States would probably extradite. But for a lot of the lesser crimes, even felonies, extradition is not a very practical remedy.").

Fines are a better option, but will often provide more of a theoretical punishment than a real one. Most individuals lack the financial ability to pay criminal fines. Even wealthy defendants within a court's jurisdiction often will find ways to avoid payment. In a recent study by the Government Accountability Office ("GAO"), for example, the GAO studied five criminal cases, involving convictions five to thirteen years earlier, in which very wealthy defendants were convicted and ordered to pay fines totaling $568 million.[60] All five defendants took steps to hide their assets, and all five later claimed an inability to pay. The government collected only $40 million from the defendants, about 7 percent of the total ordered.[61] Government officials did not plan on pursuing additional funds because willful failure to pay a fine or restitution is not itself a crime.[62]

More broadly, a strong regime of criminal enforcement would threaten one of the foundational strengths of virtual world games: the ability of each virtual world to define its own terms and to appeal to specific users who want that virtual environment instead of another.[63] Each virtual world is unique, and internet users can pick the ones they enjoy. So long as harms remain virtual ones, each community can define what virtual harms deserve protection and which do not. In contrast, criminal law tends to be one size fits all. The criminal law enacts broad prohibitions, and those prohibitions apply in the same way to each subject.

This leaves two unappealing alternatives for how criminal law can regulate virtual worlds. First, criminal law could force every virtual world to conform to the same standard. In effect, the law could impose rules of the game by statute. But this defeats the efforts by game administrators and game players alike to opt for a game with rules to their liking.[64] One person's virtual harm is another's virtual benefit; the state has no legitimate role in imposing uniformity on such matters of personal taste.[65]

---

[60] Associated Press, *Huge White Collar Fines Go Unpaid* (Mar 3, 2005), available at <http://www.msnbc.msn.com/id/7082314/> (last visited Mar 31, 2008).

[61] Id.

[62] Id.

[63] See Balkin, 90 Va L Rev at 2044 (cited in note 4) ("The inhabitants of these virtual worlds should be given a chance to decide what internal norms will guide them.").

[64] This may raise important First Amendment issues. See id at 2053–58 (classifying design and play in virtual worlds as speech, and discussing other First Amendment issues).

[65] See *Stanley v Georgia*, 394 US 557, 565 (1969) ("[A] State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch.

Second, the law could punish violations of the rules as defined by the game administrators. For example, a legislature could criminalize violating ToS that regulate virtual worlds. This would be "one size fits all" in the sense that it would apply equally to any ToS. Such a law would effectively delegate the line of criminality to private individuals, who could define the scope of criminal law in their virtual world through the ToS. As I have argued at length elsewhere, this is a dangerous and potentially unconstitutional idea.[66] ToS are arbitrary, and can reflect the whims and biases of whoever sets them. As a result, a violation of ToS often has no correlation to a social harm that merits punishment or requires deterrence.[67]

Because criminal law is a blunt instrument poorly suited to respond to virtual misconduct, virtual crimes should trigger virtual remedies. Criminal penalties serve as a last resort in the physical world when misconduct threatens the lives or security of persons or involves property crimes that civil law cannot address. But virtual harms are best dealt with by virtual remedies. So long as misconduct stays virtual, it should remain the domain of game administrators well-equipped to redress harms, rather than governments who have only the crude hammer of criminal punishment.

III. CONCLUSION

John Perry Barlow famously began his essay *A Declaration of the Independence of Cyberspace* with a dramatic call for governments to stay away: "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[68] As general guidance, Barlow's call was rather silly, I think.[69] But if we limit Barlow's call to how criminal law should regulate the "virtualness" of virtual

---

Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.").

[66] See Kerr, 78 NYU L Rev at 1656–60 (cited in note 48).

[67] Id at 1656–58.

[68] See John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Feb 8, 1996) available at <http://homes.eff.org/~barlow/Declaration-Final.html> (last visited Mar 31, 2008).

[69] See, for example, Orin S. Kerr, *Enforcing Law Online*, 74 U Chi L Rev 745, 751–54 (2007) (reviewing a book that discusses the question of enforceability of law over the internet).

worlds, Barlow was exactly right. Criminal law generally should take a hands-off approach to virtual misconduct; virtual wrongs should trigger virtual punishments rather than real ones. The "weary giants of flesh and steel" should mostly leave virtual worlds alone—not because they are not welcome there, but because their mechanisms are ill-suited to respond to purely virtual harms. Criminal law is not a game, and governments should not interfere with virtual worlds that are.