A Virtual Property Solution: How privacy law can protect the citizens of virtual worlds

John W. Nelson
A VIRTUAL PROPERTY SOLUTION: HOW PRIVACY LAW CAN PROTECT THE CITIZENS OF VIRTUAL WORLDS

John William Nelson*

WORKING PAPER
DRAFT

ABSTRACT

Privacy laws can protect virtual worlds and their users where property law cannot. Yet, legal scholars tend to ignore this power in favor of extending the virtual world metaphor in an effort to see the common law of property cover virtual worlds. This article explores how harms against the citizens of virtual worlds are harms against the victim’s mental state rather than his wallet. A review of the types of privacy law applicable to virtual worlds is provided, and those laws are applied to common virtual world scenarios resulting in harm. Finally, privacy law is offered as the most viable and logical approach to dealing with virtual world harms because of its ability to address mental harms without the need for a property loss.

TABLE OF CONTENTS

INTRODUCTION................................................................................. 2

I. A MATTER OF DEFINITIONS ..................................................... 4
   A. THE PROBLEM WITH LABELS: RELABELING ‘VIRTUAL PROPERTY’ AS
      ‘VIRTUAL RESOURCES’................................................................. 4
   B. THE MEANING OF ‘VIRTUAL THEFT’........................................ 5

II. HOW HARMS AGAINST OUR VIRTUAL SELVES ARE HARMS
    AGAINST OUR REAL SELVES, AND HOW THOSE HARMs INTRUDE
    UPON OUR PRIVACY AND MENTAL STATE ..................................... 6
   A. THE STORY OF A ‘VIRTUAL RAPE’ AND THE WAY IN WHICH OUR
      VIRTUAL SELVES BECOME PART OF OUR REAL SELVES............... 6
   B. WHY PERSONHOOD IS IMPORTANT, HOW IT IS RELATED TO IDENTITY,
      AND HOW THIS RELATES TO PRIVACY ...................................... 9

III. PRIVACY AND OTHER LAWS APPLICABLE TO VIRTUAL
    WORLDS AND THEIR USERS.......................................................... 10

* B.A. (2003), University of Georgia; J.D. (2008), Cumberland School of Law at Samford University; LL.M. (2010), University of East Anglia. The author thanks the patience of his wife and daughter as well as his friends and mentors willing to read and provide comments: Brandon Denning, Marcia McCormick, Robert Heverly, Shannon C.P. Skipper, Daithí Mac Síthigh.
INTRODUCTION

It is fashionable in writing about virtual worlds to discuss the similarity of those worlds with our own. These worlds are viewed through the lens of the real, and comparisons are made between the real world and the virtual. Legal writing in this area has followed suit.
A number of legal articles concerning virtual worlds tackle the problem of virtual resources. Couched in the more evocative label of ‘virtual property,’ the value of these resources is examined and the need for property law protections is suggested.\(^1\) A near consensus has led to the presumption that property protections should be granted to these resources, with the only question left being when courts or legislatures will act.\(^2\)

A small number of authors reject the extension of property law to virtual worlds and their resources.\(^3\) This author is one of those. I have argued strongly against extending property rights to the items and objects found in virtual worlds.\(^4\) My most recent article on the subject examined what such an extension might look like and why it should not occur.\(^5\) In essence, the very worlds and resources advocates of this extension seek to protect will, instead, be harmed.\(^6\)

This is the virtual property problem—how can virtual world users be protected against others who seek to harm their virtual world selves? This

---


\(^2\) See, e.g., supra note 1.


\(^5\) Id. at 295-309.

\(^6\) Id. at 307-08.
article argues that the solution to this problem is the application of privacy laws to situations where virtual world users are harmed by the actions of others. Ultimately, privacy laws can protect virtual world users where property laws cannot.

Section I defines ‘virtual resources’ and ‘virtual theft’ and discusses why proper labels are important when examining these issues. Section II argues that cases of ‘virtual theft’ present real harms, and that those harms are against our mental selves and personal identities. Section III examines the common law and sui generis privacy laws applicable to virtual worlds and their users. Section IV briefly reviews other laws that might apply to cases of ‘virtual theft.’ Section V applies privacy laws—both common law and sui generis statutory laws—to two common types of ‘virtual theft’ scenarios. Section VI concludes with why privacy laws are best suited to protect against ‘virtual theft,’ and why we should view virtual worlds through the lens of privacy.

I. A MATTER OF DEFINITIONS

A. The problem with labels: Relabeling ‘virtual property’ as ‘virtual resources’

The label ‘virtual property’ is evocative and often used to describe the items and objects that exist in virtual worlds.\(^7\) It has also been extended to describe a virtual world’s character and his accounts.\(^8\) I discussed the dangers of these kinds of analogies in *The Virtual Property Problem*,\(^9\) but the problems associated with mislabeling are slightly different in this context.

Unlike the problem of baggage in *The Virtual Property Problem*, the danger in this article is a tendency to preclude non-property-based solutions when considering how to protect virtual worlds and their users. James Boyle touches on this type of problem in *Shamans, Software, and Spleens*\(^10\) — an early work on the internet and information age.

Boyle highlighted the struggle to understand the reasons why blackmail and insider trading were illegal by working to understand the

---


\(^8\) *See, e.g.*, supra note 7.


proper classification, or typing, of each act.\textsuperscript{11} To Boyle, each problem depended on the difference between private and public information.\textsuperscript{12} He noted the importance of proper classification because it dictated one’s approach to a problem.\textsuperscript{13} Classifying something one way can lead to certain analogies logically applying, while classifying it another way may preclude one from even considering those same analogies.\textsuperscript{14}

Virtual worlds deserve full, objective consideration. They present new and unique situations that do not neatly fit into current legal frameworks. The best way to ensure that the legal issues facing virtual worlds are placed in the most appropriate legal framework is to keep all legal schemes on the able. Otherwise we may find ourselves forcing a square peg into a round hole because we ignored square holes that might have worked.

Relabeling virtual world objects, characters, and accounts as ‘virtual resources’ rather than ‘virtual property’ may help provide a more full perspective on their legal issues. The ‘property’ label, purposefully or not, helps frame debate and discussion in a property-based manner. The tendency to overlook non-property-based solutions to problems should be reduced if the subject is labeled ‘resources’ rather than ‘property.’ For these reasons, and those presented in \textit{The Virtual Property Problem},\textsuperscript{15} this article will use the term ‘virtual resources’ rather than the term ‘virtual property.’

\textbf{B. The meaning of ‘virtual theft’}

Virtual theft is another evocative label. Accordingly, virtual theft has the potential to carry its own baggage and limit our ability to view beyond a theft-based view of the harmful act we are examining. It is therefore important to clearly articulate what we mean by virtual theft.

For the purpose of this article, virtual theft is any situation where a virtual world user’s virtual resources are accessed and transferred by another without the first user’s consent. This includes situations where accounts are hacked\textsuperscript{16} as well as situations where software exploits\textsuperscript{17} are

\begin{itemize}
  \item \textsuperscript{11} \textit{Id.} at 108-11.
  \item \textsuperscript{12} \textit{Id.} at 109-10.
  \item \textsuperscript{13} \textit{Id.} at 110.
  \item \textsuperscript{14} \textit{Id.}
  \item \textsuperscript{15} Nelson, \textit{supra} note 4, at 284-85.
  \item \textsuperscript{16} Hacking includes the unauthorized access of computers. \textsc{Douglas Downing}, Ph.D., \textit{supra} note 13, at 223 (10th ed. 2009) (describing a hacker as someone who access a computer without authorization). This may also be known as ‘cracking,’ and those who ‘crack’ are known as ‘ crackers.’ \textit{Id.} at 118.
  \item \textsuperscript{17} ‘Bugs’ are unintended features or errors in a computer program. \textsc{See Douglas Downing}, Ph.D., \textit{supra} note 13, at 223 (10th ed. 2009) (describing a hacker as someone who access a computer without authorization). This may also be known as ‘cracking,’ and those who ‘crack’ are known as ‘ crackers.’ \textit{Id.} at 118.
used to get around a virtual world’s intended game mechanics to gain access to virtual resources.

II. HOW HARMS AGAINST OUR VIRTUAL SELVES ARE HARMS AGAINST OUR REAL SELVES, AND HOW THOSE HARMS INTRUDE UPON OUR PRIVACY AND MENTAL STATE

A. The story of a ‘virtual rape’ and the way in which our virtual selves become part of our real selves

The story of a virtual rape is a good example of how our virtual identities become part of our selves. The story has been related a number of times in a number sources. The best telling of the story is the original, and it comes from Julian Dibbell in his popular essay A Rape in Cyberspace—How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society. A full retelling of the story is beyond this article’s scope, but I encourage a full reading of the work. It is powerful, informative, and has influenced a number of virtual world scholars.

The facts, in short, come down to the actions of a character named Mr. Bungles who resided in LambdaMOO, an early virtual world. Mr. Bungles took advantage of code within LambdaMOO that allowed a ‘voodoo doll’ of a character to be created that allowed the doll’s possessor to make it appear as if the copied character was acting in a certain way. For example, if you had a doll named Foo then you could use that doll to have text on the screen state ‘Foo bends down to tie his shoes.’ Absent the doll, only Foo’s user could enter the ‘emote’ command to make the text

DOWNING, PH.D., supra note 16, at 68.


22 Id. at 15 (briefly describing how the voodoo doll works).

23 Id.
appear that describes Foo bending down to tie his shoes.  

Mr. Bungles used this feature of LambdaMOO for actions other than shoe tying. Taking up residence in the most populated room in the virtual world, Mr. Bungles began to describe various characters performing explicit sex acts on both him and their selves. These acts, over time, also became violent in nature. In essence, Mr. Bungles forced characters to appear to act in a certain way without the consent of the individuals who created and controlled those characters.

Mr. Dibbell’s essay on the matter goes on to describe the reaction of both the victims of Mr. Bungle and LambdaMOO’s community. Mr. Bungle’s actions were described as ‘virtual rape,’ although Mr. Dibbell takes pains to emphasize that no one in the community was trying to equate the situation with actual rape. Rather, it was an expedient analogy for the virtual interactions forced upon others without their consent.

This article is not concerned with the technical or social regulation of online communities, however. Other works have explored the contours of virtual and online communities in these areas. Lawrence Lessig explored the technical regulation embodied by the phrase “code is law” in his celebrated work Code and Other Laws of Cyberspace. An entire journal has been created to publish research in virtual worlds, including research on the social dynamics of these worlds. Mr. Dibbell himself touched on the social issues of Mr. Bungle’s actions in his essay and later explored these issues in future works.

24 Id.
25 Id. at 13, 15.
26 DIBBELL, supra note 21, at 13, 15.
27 Id. at 17-30.
28 Id. at 22.
29 Id.
32 One example is his book, MY TINY LIFE, in which A Rape In Cyberspace is reproduced. JULIAN DIBBELL, MY TINY LIFE—CRIME AND PASSION IN A VIRTUAL WORLD, 11-30 (1998). See also JULIAN DIBBELL, PLAY MONEY: OR, HOW I QUIT MY DAY JOB AND
This article, however, is more interested in the reaction of the victims. One victim, a character named exu, found herself calling for vengeance—the virtual castration or destruction of the character Mr. Bungles. Mr. Dibbell relates that the individual behind exu told him that she found herself crying tears as she responded to Mr. Bungle’s actions the evening after they occurred. It is this reaction, exu’s tears, which this article is most concerned about.

The tears shed by exu’s player are emblematic of the value placed on virtual world characters by those who create them. Mr. Dibbell touches on the time spent in LambdaMOO by members of its community. Hours of the day were spent socializing, creating personal ‘rooms’ within the virtual world, designing character descriptions, and acting out those descriptions to create a character’s ‘personality.’ This has not changed as virtual worlds have become more commonplace, more sophisticated, and more graphically intense.

World of Warcraft and Everquest users have been known to spend hours playing each game. They form groups of players called guilds. Sometimes these guilds are focused on game conquests such as defeating rare bosses or winning battles against other human players in arena-like combat. Sometimes these guilds exist as a support group for developing a character’s skills and equipment while providing a social outlet. Regardless, these groups are another example of the time spent by virtual world users in developing their in-game persona.

Attachment to these characters and their personas occurs just as it did for exu’s player in that early virtual world, LambdaMOO. Situations where these characters are destroyed, or where their equipment and items are taken, can result in similarly strong feelings as those experienced in the rape story above. While not exactly similar situations, both consist of situations where a virtual world user has had their persona, their psyche, used in an unwelcome manner and without their consent.

---

33 DIBBELL, supra note 21, 15-16.
34 Id.
35 Id. at 14-15, 29.
37 Reading the stories of hacked accounts that occurred in one World of Warcraft guild, including the comments in response, highlights the feelings players possess for their characters and accounts. See Tarinae, Srs Bsns, A Healadin’s Tear, http://ahealadinstea.wordpress.com/2010/04/01/srs-bsns/ (last accessed Sept. 30, 2010).
B. Why personhood is important, how it is related to identity, and how this relates to privacy

Key to the analysis of how best to protect virtual worlds and their users is the concept of personhood. A person may be defined many ways: the theatrical persona from Latin, or its Roman legal equivalent of an entity possessing legal rights; a Kantian rights-holder; Locke’s thinking being, capable of reflection and see itself as itself; a metaphysical skeptic’s view of a person as a series of perceptions; as well as other philosophical or legal theories. Our U.S. legal system has even created fictional or constructive ‘persons’ out of corporations and companies. Personhood, on the other hand, is the state of being a person or individual—it is the features and qualities that separate us from each other.

Personhood relates to those qualities we use, internally and externally, to define ourselves. The personality and character of exu in LambdaMOO became part of the personhood of the player who created exu. The connection can be seen through her tears in recounting the virtual rape. Mr. Dibbell’s essay also recounts philosophical discussions by LambdaMOO users over where their selves end and the rest of the world begins.

Margaret Jane Radin explored personhood concepts in her article *Property and Personhood*. To Radin, the attachments we develop to some items create separate types of property—personal and fungible. Whereas we may view article money as fungible and readily exchangeable, we might

---

38 Person comes from the Latin word persona, or mask. Masks were used in Roman theater to create different characters. Margaret Jane Radin touches on this in *Property and Personhood*, 34 STAN. L. REV. 957, 962 (1982).
39 “Every being capable of having and being subject to rights was called in Roman law a persona.” HORACE L. WILGUS, 1 CASES ON THE GENERAL PRINCIPLES OF THE LAW OF PRIVATE CORPORATIONS 73 (2d. ed. 1904); see also Radin, *supra* note 38, at 962.
40 See Radin, *supra* note 38, at 962.
41 See id. at 963.
42 See id. at 964.
43 See id. at 962.
44 One recent reminder of this legal fiction is the Supreme Court’s decision in *Citizens United v Federal Election Commission*, 558 U.S. ___ (2010). The Court rejected the notion that the First Amendment only applied to ‘natural persons’ and emphatically extended it to corporations as constructive person. *Id.* at (83?; 26[33] of the unpublished opinion).
45 DIBBELL, *supra* note 21, at 22.
47 Radin, *supra* note 38, at 960.
view our wedding rings as far more personal and less interchangeable.  

Radin develops the personhood view of property in order to examine property regimes and protections in light of the different connections people have in different types of property. Nevertheless, the personhood view of the world can extend to other areas as well. Concepts of identity are behind the development of privacy rights in U.S. common law. Most striking of these privacy rights is the right to control the market for your name and persona—a clear recognition of the connection between one’s privacy and identity. Similarly, moral rights extended to authors in European law work along the same personhood view—the right to control your identity and how it is presented is important.

‘Virtual theft’ intrudes upon the victim’s personhood rights. It violates the virtual identity of the victim. By doing this, it intrudes upon private areas of the victim’s life. These are not harms against the victim’s property; these are harms against the victim’s identity and privacy.

III. PRIVACY AND OTHER LAWS APPLICABLE TO VIRTUAL WORLDS AND THEIR USERS

A. How virtual theft is a mental intrusion and a privacy intrusion

Given the connection between our virtual selves and our own identity, it is not hard to see the harm caused when someone violates another’s virtual identity. The emotional attachments that are created between our selves and our virtual selves can be significant. The question is how should these harms be defined?

No property rights have been violated in the traditional sense. Often virtual world companies seek to restore players to their original, pre-harm

48 Radin, supra note 38, 959-60.
49 Radin, supra note 38, passim.
50 Cf. Samuel D. Warren & Louis D. Brandeis, Privacy, 4 Harv. L. Rev. 193 (1890) (arguing for the need of privacy laws to protect mental harms).
51 See RESTATEMENT (2D) OF TORTS § 652C.
52 The most notable example are the moral rights in Article 6bis of the Berne Convention:

Independent of the author’s economic rights, and even after the transfer of the said rights, the author shall have the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to the said work, which would be prejudicial to the author’s honor or reputation.

Berne Convention for the Protection of Literary and Artistic Works art. 6bis, Sept. 9, 1886.
state if equipment or characters have become lost. The harm appears to be predominantly mental in nature. It is an intrusion into our mental selves, a tampering with our identity by harming our virtual self.

This is where privacy laws can play a role in protecting and defending virtual world users against unauthorized access of their accounts. Harms against mental states and identities are invasions of privacy. They necessarily require access to the victim’s private information. While there may be no traditional ‘property’ harm to speak of, there is a personal interest that has been harmed.

B. The emergence of privacy law as a right to be let alone and a right to be secure in our own information

Privacy rights can be put into three categories in the United States. First, a citizen’s right to privacy against government intrusion is guaranteed by the Fourth Amendment and Supreme Court cases such as Griswold v. Connecticut. Second, a person’s right to privacy against the intrusions of private citizens is not guaranteed, but it is supported in most states through common law developments. Third, sui generis privacy rights have emerged where legislation has sought to protect individual privacy in specific situations. This article is concerned with the second right to privacy category – the so-called “right to be let alone” – as well as the third – legislatively created sui generis privacy rights.


U.S. CONST. AMEND. IV.


Warren & Brandeis, supra note 50, at 193.
1. Common Law Privacy – the right to be let alone – and its application to virtual worlds and their users

The so-called “right to be let alone” has been divided into four distinct types of privacy. Outlined by Prosser in his 1960 Privacy article, these four classic privacy types began to be outlined in the common law with the famous Warren and Brandeis article, The Right to Privacy. The four types of privacy are as follows:

[1.] unreasonable intrusion upon the seclusion of another . . . ;
[2.] appropriation of the other’s name or likeness . . . ;
[3.] unreasonable publicity given to the other’s private life . . . ;
[and]
[4.] publicity that unreasonably places the other in a false light
before the public . . . .

Each of these four types reflect different, albeit sometimes overlapping, privacy principles.

The first privacy type, unreasonable intrusion into the seclusion or solitude of another, is the most relevant for cases of virtual theft and the unauthorized access of a virtual world user account. The act must be intentional, it must intrude into something that is actually private, and it must be highly offensive to a reasonable person. Prosser noted that “[t]he principle was . . . soon carried beyond . . . physical intrusion.”

This right to privacy has already been extended to the online realm. The Third Circuit found this right applied to the unauthorized opening of another’s email. The court stated that “private individuals . . . have a reasonable expectation that their personal mail will not be opened and read by unauthorized persons.” The court further ruled that no publication

59 Restatement (2d) of Torts § 652A. Cf. Prosser, supra note 56, 389 (listing the four types of privacy as “[1.] Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs . . . [:] 2. [p]ublic disclosure of embarrassing private facts about the plaintiff . . . [:] 3. [p]ublicity which places the plaintiff in a false light in the public eye . . . [:] 4. [a]ppropriation, for the defendant's advantage, of the plaintiff's name or likeness.”).

60 Restatement (2d) of Torts § 652B.

61 Meaning that the matter or thing intruded upon cannot be in the public domain. See Restatement (2d) of Torts § 652B; see also Prosser, supra note 56, at 391 (“[i]t is clear also that the thing into which there is prying or intrusion must be, and be entitled to be, private”).

62 Restatement (2d) of Torts § 652B.

63 Prosser, supra note 56, at 390 (noting its use against eavesdropping, peering through windows, revealing bank account information, and more).

64 Vernars v. Young, 539 F.2d 966, 969 (3rd Cir. 1976).

65 Id.
requirement exists for the intentional tort of intrusion upon seclusion and, therefore, the act of intruding itself is sufficient to sustain a claim.66

Similarly, the District of Columbia Court of Appeals recognized, in dicta, the potential for this tort to apply when electronic methods are used for the “unauthorized viewing of personal information such as . . . Social Security number[s].”67 This bolsters Prosser’s earlier recognition that the tort extended beyond physical intrusion and into other, non-physical means of uncovering private information. The case, however, was dismissed on separate grounds.68

Prosser viewed this tort as primarily protecting a mental interest.69 In fact, at the time Privacy was published, Ohio courts substituted the tort of intrusion into seclusion for the tort of intentional infliction of emotional distress.70 This approach to the tort focuses on the harm visited upon the victim rather than trespasses against property. This is one reason why the tort developed to where a physical intrusion is unnecessary for liability.

This focus on the individual rather than his property allows to the tort to factor in non-property interests harmed by the tortious act. This is important for virtual theft cases where there is a real harm to the victim’s interests, yet that harm is not related to a currently property interest. This overcomes the logical, philosophical, and legal need for a ‘thing’ to have been harmed or stolen in order for the victim to sustain a claim.

2. Sui generis privacy laws and their application to virtual worlds and their users

Constitutional privacy and common law privacy are not the only sources of privacy protection in the law. Legislators have carved out specific privacy rights to meet the harms of unique situations governing computers. These sui generis laws seek to protect privacy on both criminal and civil grounds.

Computer invasion of privacy crimes are examples of these emerging sui generis laws. Jordan M. Blanke examined the history of these crimes in Criminal Invasion of Privacy: A Survey of Computer Crimes.71 Many of the criminal statutes surveyed by Mr. Blanke include penalties for the unauthorized access of another’s computer, computer data, or computer

---

66 Id.
68 Id. at 711.
69 Prosser, supra note 56, 392.
70 Id. at 390. Ohio’s supreme court later acknowledged the tort of intentional infliction of emotional distress in Yeager v. Local Union 20, Teamsters, Chauffeurs, Warehousemen, & Helpers of America, 453 N.E.2d 666, 670-71 (Ohio 1983).
accounts. 72

The Computer Fraud and Abuse Act is another example of a sui generis law aimed at protecting computer users. 73 As with the state crimes above, the Act creates both criminal and civil liabilities for unauthorized access of information. 74 Civil remedies only kick in if the losses to a company or individual over a 1-year period add up to at least $5,000 in aggregate value. 75

Similar to common law privacy above, the above sui generis laws focus less on property and more on protected information and the individual or entity harmed. These sui generis laws punish the unauthorized access of a victim’s information, not the theft or harm of tangible property. The prohibited act is an intrusion, not a conversion.

IV. A BRIEF REVIEW OF OTHER LAWS RELEVANT TO VIRTUAL WORLDS

While privacy laws are the focus of this article, it is worthwhile to mention two other areas of law that may provide protections for virtual resources. The first of these areas is the law of theft. The second area is the law of contract by virtue of the third party beneficiary doctrine.

A. A brief analysis of theft’s applicability to virtual world accounts and virtual resources

Theft laws are a popular point of reference for those who advocate viewing virtual resources through a property lens. A brief overview of theft laws and their applicability to virtual ‘theft’ scenarios is relevant for this reason. A more in-depth analysis is beyond the purpose and scope of this article, although it has been done in other papers. 76


74 Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(g) (adding a civil remedy on top of the already existing criminal remedy).


1. The Model Penal Code as a substitute for a fifty-state survey

The Model Penal Code is a collection of criminal laws meant to stand as a model for the development and reform of criminal law in the United States.\textsuperscript{77} First published in 1962, the Model Penal Code lays out a statutory framework for criminal law based upon the original common law and tweaked to represent the author’s views as to how criminal law should be reformed.\textsuperscript{78} The authorial body that developed the Model Penal Code is the American Law Institute, famous for other legal works such as the Restatement of Law series.\textsuperscript{79}

Many criminal law discussions fall back on the Model Penal Code as a point of reference because it is a standardized body of criminal statutes.\textsuperscript{80} In contrast, actual criminal law is composed of a patchwork of state-specific common law and statutory crimes. Relying on the Model Penal Code as a point of reference reduces the need to perform a 50-state survey on a given criminal law area before discussing general criminal law theory.

When using the Model Penal Code in this way, it is important to remember that the Code is not a restatement of criminal law, but rather a model for potential criminal statutes. While certain aspects of the Model Penal Code have been adopted in a number of states, the Code has not been adopted wholesale by any jurisdiction\textsuperscript{81} as have other similar code collections such as the Uniform Commercial Code.\textsuperscript{82} Accordingly, the Model Penal Code is just a starting point, not the final destination.

2. The broadness of the MPC’s theft statute may include the ‘theft’ of virtual resources

The Model Penal Code consolidates a number of theft offenses under a single Article. Theft by unlawful taking or disposition is the section most relevant to ‘virtual theft.’ It is the shortest and most basic theft section in the Code:

\textsuperscript{78} Id. at 323-25.
\textsuperscript{79} Id. at 323.
\textsuperscript{80} Id. at 319-20.
\textsuperscript{81} Id. at 326-29.
(1) **Movable Property.** A person is guilty of theft if he unlawfully takes, or exercises unlawful control over, movable property of another with purpose to deprive him thereof.

(2) **Immovable Property.** A person is guilty of theft if he unlawfully transfers immovable property of another or any interest therein with purpose to benefit himself or another not entitled thereto.\(^8^3\)

The scope of theft is further outlined by the Article’s definition section. Property is broadly defined as “anything of value,” including, amongst others, “interests in or claims to wealth.”\(^8^4\) This is a broad definition of property intended to capture a variety of situations. This intention is also embraced by the definition of “property of another” in the section: “. . . property in which any person other than the actor has an interest . . . regardless of the fact that the other person might be precluded from civil recovery because the property was used in an unlawful transaction or was subject to forfeiture as contraband.”\(^8^5\)

It may be argued that this theft statute covers ‘virtual theft’ scenarios regardless of whether virtual resources are viewed as property by the courts. After all, virtual resources possess value even if they do not possess property protections. In addition, this statute is designed to capture even the theft of property that has voidable title.\(^8^6\) Accordingly, it is not a long stretch to view virtual resources, which possesses value but no ‘title,’ in the same light.\(^8^7\) In practical use, however, this extension runs into problems.

3. **Defining the value of virtual resources is difficult**

Value associated with virtual resources typically comes in the form of gray-market value. Many discussions of virtual resource value look to unauthorized, gray markets where the buying and selling of virtual resources occur.\(^8^8\) At the same time, the buyers and sellers of these virtual

---

\(^8^3\) Model Penal Code § 223.2.  
\(^8^4\) Model Penal Code § 223.1.  
\(^8^5\) Model Penal Code § 223.1.  
\(^8^6\) See Model Penal Code § 223.1.  
\(^8^7\) This view leads to arguments for theft to apply to virtual resources; a position taken by Andrea Vanina Arias in *Life, Liberty, and the Pursuit of Sword and Armor: Regulating the theft of virtual goods*, 57 Emory L.J. 1301 (2008).  
\(^8^8\) The most notable being Edward Castronova’s examination of the EverQuest economy in *Virtual Worlds: A First-Hand Account of Market and Society on the Cyberian*
resources are not guaranteed the continued use of the resource after purchase.

Many virtual world owners explicitly state that virtual resources are not to be considered property and, to the extent they are, the resources are owned and possessed by the virtual world owner.\textsuperscript{89} Further, attempts to buy and sell these resources are prohibited by many virtual world owners.\textsuperscript{90} Getting caught doing so may result in a virtual world user having his access to the virtual world blocked, his account closed, and all of his virtual resources deleted.

This leaves a prosecutor looking to prosecute someone for the theft of virtual resources in a bind. Will a jury view these resources as having value? Can evidence of a highly-fluid gray market value be sufficient? These questions may leave prosecutors looking for offenses that are easier to apply to these types of cases, such as various computer crime statutes.

\textbf{B. Contract remedies through the third-party beneficiary doctrine}

Most virtual worlds require their users to agree to terms of use\textsuperscript{91} and end user license agreements before the user is allowed to enter the world.\textsuperscript{92} These contracts regulate the interaction between the virtual world’s owners and each user. Some of these contracts outline codes of conduct virtual world users are expected to follow. Failure to follow these codes may result in an account suspension.\textsuperscript{93}


\textsuperscript{91} The agreement between the user and software developer governing the user’s access to the virtual world. These are may also be called Terms of Service (ToS).

\textsuperscript{92} The agreement that between a software user and a software developer as a condition of the user installing and using the software. This is abbreviated as EULA. \textit{See} \textsc{Douglas Downing}, Ph.D., \textit{supra} note 16, at 176.

\textsuperscript{93} \textit{See}, e.g., World of Warcraft’s Terms of Use,
These codes are often intended to prevent virtual users from harassing other users and generally making the virtual world an unpleasant place to be. Accordingly, some have argued that the third-party beneficiary doctrine may be one method for protecting virtual users against each other. The most comprehensive review of this idea is by Michael Risch in Virtual Third Parties.94

Virtual Third Parties looks at the contractual relationship that exists between a virtual world user, a virtual world owner, and other users as third-party beneficiaries.95 It further outlines the third-party beneficiary doctrine as it applies to virtual worlds and their users.96 After briefly discussing how the doctrine might apply to specific scenarios that occur in virtual worlds and are typically regulated by virtual world codes of conduct, Mr. Risch concludes with the idea that the third-party beneficiary doctrine may be one solution to provide protections to virtual world users.97

The third-party beneficiary doctrine does show promise in protecting virtual world users from other users. Nevertheless, it only extends to real virtual world users. Hackers who do not truly care whether their own, personal accounts remain active will not fear a remedy that results in their being cut off from the game. This is where the limit of the third-party beneficiary doctrine begins to appear—what punishments does it allow when the bad actor has no care for the contract under which the benefits exist, and through which they are enforced?

V. VIRTUAL WORLD HARMs APPLIED TO PRIVACY LAW

‘Virtual theft’ typically occurs in one of two situations. The first is unauthorized access of a virtual world user’s account. The second is exploitation of software bugs to obtain access to a virtual world user’s game items.

A. Hacked accounts

A hacker steals a virtual world user’s account username and password. Using this information, the hacker enters the virtual world and

---

95 Id. at 415-21.
96 Id. at 422-25.
97 Id.
begins to trade any transferable virtual resources to other users. Items that cannot be transferred are deleted. After everything has been transferred or deleted, the hacker deletes virtual world characters. The virtual user, after re-gaining access to his account, logs in to find all of his characters deleted and all of his virtual resources gone.

1. The privacy tort of intrusion into seclusion

The elements for the tort of intrusion into seclusion are met by the above facts. The hacker intentionally accessed the virtual world user’s account. This was done by gaining access to private information in the form of the user’s account username and password. By logging into the account the hacker accesses private information. The information is private because it is protected by a username and account. Finally, the intrusion is likely to be viewed as highly offensive to a reasonable person. If the hacker’s access using a stolen username and password were not offensive enough, the deletion of all virtual resources, including the game characters, would likely meet this burden.

Presuming a finding against the hacker in court, the victim will be able to recover general damages. Those damages in this situation would be the mental harm suffered by the victim for having his privacy violated. This obviates the need to try and prove the value of the virtual resources when those resources do not enjoy property protections and only have value on questionable, and highly fluid, gray markets.

2. State-specific sui generis laws for unauthorized computer access

State-specific laws regulating computer privacy focus on unauthorized access of computer systems. The above facts involve the unauthorized access of another user’s account. While each state’s computer crime laws vary, the unauthorized access of the system led to access and misuse of personal data. This falls squarely in the ambit of most state computer crime statutes.

3. Computer Fraud and Abuse Act

---

98 Act must be (1) intentional, (2) intrude on something private, and be (3) highly offensive to a reasonable person. RESTATEMENT (2D) OF TORTS § 652B.

99 Blanke, supra note 72, at 449-56 (surveying in detail state laws governing computer privacy crimes).

100 Id.
The Computer Fraud and Abuse Act, while protecting against unauthorized computer access, will be a difficult remedy on the above facts. Key to the civil remedies section of the Act is damages adding up to at least $5,000 in aggregate value.\(^{101}\) Damage is defined as harm to data integrity; loss is defined as reasonable costs to the victim for assessing damages and restoring data or systems to their prior state.\(^{102}\) Further, losses are limited to economic damages only.\(^{103}\)

The user who is a victim of a hacker’s intrusion into his virtual world account is not the entity suffering damages and loss contemplated by the Act. It is the virtual world owner, rather, who suffers damages most relevant to the Act. For these reasons, obtaining a remedy under the Computer Fraud and Abuse Act is not likely on the above facts.

\section*{B. ‘Virtual theft’ through software bug exploits}

Some users of the virtual world Habbo Hotel logged into their virtual apartments one day only to find that their virtual furniture had been swiped.\(^{104}\) Their apartments, once furnished with virtual resources that cost real-world money, were now bare.\(^{105}\) These virtual world users had fallen victim to ‘virtual theft’ because of a software bug. Other Habbo Hotel users exploited this bug to drag furniture and other items out of the victims’ rooms and back to their own rooms to be sold, for real-world money, to other Habbo Hotel users.\(^{106}\) The ‘virtual thieves’ were caught, however, and Dutch police have moved forward with a criminal prosecution.\(^{107}\)

1. The privacy tort of intrusion into seclusion

The elements for intrusion into seclusion are less clear in the above scenario.\(^{108}\) The intent requirement is likely met. The virtual thieves’ actions were not accidental or coincidental. All indications are that their purpose was to remove the furniture from other Habbo Hotel users’ rooms.\(^{109}\) Less clear is whether this is an intrusion into something private.

\(^{103}\) Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030(g).
\(^{105}\) Id.
\(^{106}\) Id.
\(^{107}\) Id.
\(^{108}\) Act must be (1) intentional, (2) intrude on something private, and be (3) highly offensive to a reasonable person. \textit{Restatement (2d) of Torts} § 652B.
\(^{109}\) ‘Virtual theft’ leads to arrest, \textit{supra} note 104.
Habbo Hotel is designed to allow its users to make public rooms.\textsuperscript{110} Indications are that the furniture in question was taken from rooms open to the public and not password protected. Nevertheless, it can be argued that the privacy in question was the user’s ability to change how the rooms look by decorating them with furniture and other virtual resources. Therefore, the virtual theft’s unauthorized access of these virtual resources intruded upon the user’s private rights in representing himself to the world. This, however, is a stretch. Unlike situations involving account hacking, privacy does not easily apply to bug exploitation situations like the one faced by Habbo Hotel users.

The tort of privacy’s difficult in this scenario underlies issues of culpability. Unlike the previous account hacking scenario, software bug exploitation is the result of the virtual owner’s failure to code their world in a way to avoid the actions undertaken by the thieves. The thieves did nothing the computer code didn’t allow; the virtual world’s ‘law’ allowed them to get away with the theft.

This is not simply semantics. The Habbo Hotel scenario involved users violating Habbo Hotel’s user agreement through their actions.\textsuperscript{111} EVE Online, however, has no agreement prohibiting the taking of virtual resources in-game.\textsuperscript{112}

In fact, part of the allure of EVE Online is the very fact that piracy and theft are allowable; the only safeguards against them are friends, a limited computer ‘police’ presence, and better weaponry and armor than the pirates. Real-world value in the form of roughly US$1295 worth of game-time coupons was recently recorded as ‘lost’ to a pirate.\textsuperscript{113} Except for an unlucky random ‘roll,’ the coupons might have survived the raid and ended up in the hands of the pirates.\textsuperscript{114}

A virtual embezzlement occurred in EVE Online as well. The game allows players to pool resources and create banks that trade on the in-game

\textsuperscript{111} Terms and Conditions, Habbo Hotel, http://www.habbo.com/papers/termsAndConditions (last accessed September 22, 2010) (specifically prohibiting stealing furniture or coins from other users).
\textsuperscript{112} EVE Online, http://play.eveonline.com/en/features.aspx (listing piracy and the ability to kill and loot fellow players as one of the game’s features).
\textsuperscript{114} Brendan Drain, \textit{EVE player destroys over $1000 worth of game time}, MASSIVELY, http://www.massively.com/2010/08/08/eve-player-destroys-over-1000-worth-of-game-time/ (last visited September 22, 2010) (reading the article’s comments provides more context as to how this system works).
commodities and stock market. The manager of one such bank transferred eight percent of its funds to his own account and then sold it to others for real-world money approximating £3,115. The manager who stole the money was banned from the game, but it was for selling the game currency for real-world money in violation of EVE Online’s terms of use rather than the in-game act of embezzlement.

Which brings us back to the ability of privacy law to protect users in this situation. In the end it cannot because, ultimately, the failure was the virtual world owner’s inability to enforce, through a properly coded virtual world, their own agreement with the victim that the victim’s virtual resources could not be misappropriated the way in which the Habbo Hotel incident occurred. In such a case, contractual or negligent remedies against the virtual world’s owner appear to be more relevant than privacy claims made against the so-called ‘thieves.’

2. State-specific sui generis laws for unauthorized computer access

Unlike the hacking of a victim’s account, ‘virtual theft’ through the exploitation of software bugs does not appear to be an unauthorized access of victim’s information. At best, the unauthorized access required by state computer crime laws would exist between the exploiter/thief and the virtual world owner. If the terms of use restrict the exploiter/thief’s ability to do what was done then, no matter what the computer code allows, the exploiter/thief has acted without authorization. Nevertheless, this does not afford a remedy to the user/victim.

3. Computer Fraud and Abuse Act

Similar to state computer crime laws above, the virtual world owner appears to be the only one with a claim against the exploiter/thief. The access gained to the user/victim’s virtual resources was beyond the authorization granted through the virtual world owner’s terms of use agreement. Depending on how widespread the exploitation was, and how and who publicized it, the virtual world owner might have a civil case for violation of the Computer Fraud and Abuse Act against the exploiter/thief. There may also be a potential criminal case. Nevertheless, this does not

---


117 Id.
provide the user/victim a remedy.

C. Conclusion: Virtual privacy laws work well at protecting some forms of ‘virtual theft;’ work less well at protecting against others

Privacy laws can protect virtual world users against virtual theft, even if not all forms of virtual theft fall easily under its ambit. Unauthorized access of user accounts appears to be a strong candidate for virtual privacy protection, whereas virtual theft through software bug exploitation appears less weak. Even when the user cannot avail himself of the protection of privacy law, it may be the case that the virtual world’s owner, if he so chooses, can go after ‘virtual thieves’—hackers or exploiters—under sui generis laws at the state and federal level.

VI. Conclusion: Viewing virtual worlds through the lens of privacy creates a sound framework for laws relating to virtual world harms

Privacy laws are not a silver bullet, but they do represent a sound framework for protecting against the types of harms faces by virtual world users. Usage of the common law tort of intrusion into seclusion, for instance, may be available now without the need to substantially alter legal theory or recognize new rights. More importantly, privacy law is logically attuned to these types of harms.

The hacking of a virtual world user’s account doesn’t harm that user’s wallet; it harms his mental state and intrudes upon his private, virtual identity. With the push of a button, the company running a virtual world can restore to a victim anything he lost and, resource-wise, make the victim whole. In fact, this is often done because it just makes good business sense. Nevertheless, there is a harm suffered. These are intrusions into something private, and it is these types of intrusions that privacy laws are intended to punish or remedy.

Remedies based on a property framework are limited by a virtual world company’s ability to restore lost resources with the click of a button. If the harm is based on the value of a resource or contractual right, and that value can be recovered with nearly no cost if the company restores the user’s virtual resources, then the ability to sustain claims either civilly or criminally will be limited. If the harm is instead based on an intrusion into privacy and the unauthorized access of private information, then the ability to sustain either a civil or criminal claim will not falter if the company restores all of the victim’s lost virtual resources.

Leveraging privacy laws to protect virtual world users currently
works. There is no need to extend the common law of property to protect virtual world users if the common law of privacy and *sui generis* privacy laws already apply. Forcing the square peg of property law to fit into the round hole of virtual resources and virtual worlds will create unintended consequences that are unnecessary given the ability of privacy law to provide the sought after protections.

The very foundation of the virtual is the imagination of each individual player. This imagination is highly personal and is the epitome of privacy; it forms the basis for each player’s private virtual identity. Harms against virtual resources are harms against the victim’s imagination and, therefore, his privacy. Viewing these harms through the lens of privacy will help lay a framework for the creation of future laws that will work alongside the imagination of the virtual rather than forcing themselves into a virtual world and destroying that world’s very value—the ability to pretend, to imagine, and to escape the real.

* * *