

Security, Legal, and Ethical Implications of Using Virtual Worlds

Alfreda Dudley¹, James Braman¹, Yuanqiong Wang¹, Giovanni Vincenti¹, Donna Tupper²

Towson University¹
Dept. of Computer and Information Sciences
8000 York Rd. Towson, MD. USA
{adudley, ywang, jbraman, gvincenti, }@towson.edu

Community College of Baltimore County – Essex²
School of Mathematics and Science
7201 Rossville Boulevard. Baltimore, MD. USA
dtupper@ccebcmd.edu

ABSTRACT

Technologies such as virtual worlds have become an increasing area for research over the past several years. Many active internet users are using virtual worlds like Second Life for social interactions of all kinds. These mediums are a growing trend for online communication; the impacts of using this technology are of importance. In this paper, the authors discuss leading areas of concern related to the use of virtual worlds focusing on security, legal and ethical implications.

Keywords: Virtual worlds, Ethics, Second Life, Security Implications, Legal Implications

1. INTRODUCTION

Social interaction online is clearly changing. There is a growing shift of information presented online with a strong emphasis on visualization, user created content and social interaction in particular. Within the context of social interaction coupled with the rise of new technologies and improvements in hardware, many users are turning to virtual worlds to collaborate, share information and to spend time online. While using these 3D based virtual environments has potential advantages over traditional methods of online communication, security, legal and ethical issues associated with behaviors in these virtual environments are mostly overlooked. These issues need to be examined: particularly, with a growing user base in environments such as Second Life, Twinity, and World of Warcraft, just to name a few.

From the early text based virtual worlds to the more advanced and complex graphical based environments of today, there have always been debates as to the ethical and legal implications of virtual worlds. Looking back to the first cyberspace rape in a Multi-User Dungeon (MUD) [1], to the more complex worlds we see today that link real world financial data to virtual economies, the boundaries to real life and the virtual are blurred. It is not clear as to the potential harm virtual actions or online

virtual crimes can have on our real lives. In order to more clearly understand the security, legal and ethical implications and the potential “side effects” of using virtual worlds, the authors have started to investigate the most populated virtual world, Second Life, in particular.

In this paper, the aim is not to solve these issues or propose solutions, but to ask questions and to raise awareness to these problems. The paper is divided up in the following sections: First, a brief overview of Second Life and how it can be used in different contexts. Next, a brief discussion on the potential Security, Ethical, and Legal issues and their implications are addressed. Finally, a discussion on the security aspects of educational delivery is addressed. These sections are then followed by a discussion on our future work and conclusion.

2. IMPACTS OF VIRTUAL WORLDS

Unlike other traditional communication through email, phone and through flat 2D web technologies, virtual worlds imply special references outside of the actual geographic location of the users that are communicating [2]. Couple this feature with the ability to visualize and interact with other users in three dimensions in a realistic manner, provides a powerful medium for social interaction online. With a rise in interest in virtual worlds and the availability to users, these spaces are beginning to have a significant impact on how we communicate and conduct transactions through the Internet. Second Life in particular has been the topic of many such discussions and research endeavors.

Second Life is an Internet based three-dimensional virtual world created by Linden Lab, originally released in 2003. There has been a large increase in users over the last few years, now totaling over 16 million registered accounts [3]. Many other virtual worlds are also popular such as Twinity [4], Active Worlds [5] and There [6] and many more. Some attribute the popularity of Second Life to the large amount of varying in-world activities [7]. Users interact within the environment, with objects and socialize with other users, through their virtual

representation, known as an avatar. The user's avatar can be customized in many ways, allowing flexibility on how we can be perceived to the outside world. One can choose an opposite gender, size, race or even choose to become an animal or other non-human entity. The users of Second Life, or "Residents" as is the preferred terminology can build and create objects, buildings, clothes and much more for their virtual selves. Using the Linden Scripting Language (LSL) objects can be animated and scripted to perform non-static actions creating a more interactive and "real" environment. Virtual worlds and other similar interactive spaces that allow the users to script and create their own content often encourage emergent behaviors. This emergent behavior is what drives creativity, but sometimes leads to problems as the "rules" can be bent in ways the creators did not foresee. Some of these issues are discussed in this paper.

2.1 Security Issues

There has been much debate over the potential security risks related to the use of virtual worlds. As with all software, there is some inherent risk as no software is one hundred percent secure. Putting the actual implementation of the program aside, we focus on interactions and actions of users inside the world as a concern for security. Whereas, the solutions to address security issues in virtual worlds are often non-specific and/or vague, there are particular points to note of the legal impact on security in virtual worlds.

"The security measures that can be taken to help ensure that electronic communications and records satisfy the requirements authenticity, integrity, non-repudiation, writing and signature, and confidentiality may not yet be readily accepted, but their legal effectiveness has already been recognized, (i.e., Uniform Commercial Code)" [8, p. 37].

As users are represented by avatars (that are often changing in appearance and form) other users can only be identified by their respective screen name. Unlike text based representations, other users often rely on the simulated appearance of other users in combination with their name for identification. One problem that can occur is that of an avatar not being embodied by a human user, but instead being controlled by an intelligent agent with self governing behaviors. These software controlled characters often act in realistic ways which cannot always be distinguished as not being a real human user. In the virtual world, these entities appear exactly the same as a human user and one cannot differentiate who is real and who is a machine. Some scholars have argued ethical concerns over the use of autonomous virtual characters as they could potentially harm other users through means of

deception or users basing decisions from information gained through these characters [9].

Another topic of concern relates to social engineering; for instance, users deceiving other users of important and often confidential information. The idea of Phishing online is not a new one as this occurs often on the web when a legitimate and reputable looking website is used in order to steal a user's identification by tricking them into thinking the website is real. In a similar fashion, the same could also occur in a virtual setting through conversations between users. Let's say that an avatar develops legitimate and honest reputation overtime with other users and befriending other players. This avatar overtime could through conversation built of trust, socially engineer other user's real information if it's divulged. It is our observation and experience that users often divulge personal information, location, education level and occupation to other players when there is some establishment of trust between users.

2.2. Ethical Issues

The embodiment of a user through an avatar and its phenomenological experiences in a synthetic environment are essentially considered to be real by many users. The Avatar is essentially who and what the user is, and a representation on how they wish to be perceived online. As Second Life provides a means of communication via text and voice chat, while being able to visualize basic avatar body language, important conversational cues can enhance the realism. Making friends and meeting other users coupled with one's own experiences and reputation makes these "play" environments important. Many users also spend large amounts of time creating online businesses, trying to make an income in real life. Some users also bring much of their real lives into their digital ones. Because of the linking of the real world to the virtual world other concerns arise which include everything from identity protection, virtual theft, addiction and even issues of online stalking. The social repercussions of interacting in these worlds are not simply artifacts that remain in our online fantasies, but can manifest in our real lives as well. "The elements of crimes tend to be physical: they require physical acts, communications between physical places, and impact on real physical people" [10].

Looking within the world of Second Life itself, one can see many interesting areas that touch on many ethical problems that are also often associated with real life. Several topics that should be mentioned include: Censorship in virtual worlds, access to pornography and inappropriate content, online gambling via virtual worlds, promotion of violence and online harassment. To illustrate some of these important issues, the authors have included several images from within Second Life.



Figure 1: Areas that include inappropriate Content

Figure 1 was taken in an area that would be inappropriate in some contexts, that is easily accessible. Educators who use Second Life for educational purposes are encouraged to check out locations prior to class activities or if a class is left to explore on their own accord, to discuss with the class that these places exist and if encountered, to teleport to another location if they encounter inappropriate content.



Figure 2: Gun Kiosk



Figure 3: Jihad Joe

Figure 2 illustrates that virtual weapons do exist in many virtual worlds and are also for sale in Second Life. Usually guns and violence are not a problem and most SL users do not encounter these types of problems. However, griefers often buy items to harass other players by firing weapons and causing a disturbance. Areas within Second Life are divided into regions, in which many prohibit violence. Some players prefer to treat Second Life as a game environment and engage in simulated violence for fun or as part of a role-play activity.

Another issue that is illustrated in Figure 3 is that of a reference to terrorism. This figure illustrates an item which can be bought in Second Life to change one's avatar into appearing as a terrorist. It is described as having a "pipe bomb jacket" and that "He really explodes". Although an explosion in Second Life would

not cause any real damage, many could view this as offensive and promoting the "glamour" of terrorism. It was also reported that terrorist groups could potentially use virtual worlds to collaborate over long distances via their avatars. They could also potentially traffic real money through these mediums if they have the capability to convert real world money into virtual money and then trade the virtual currency back to the real world (though this could certainly be traced).



Figure 4: Copyright Infringement Example

In Figure 4, we can see how issues of copyright could be a problem in virtual worlds as the inhabitants of these spaces often try to import elements from the real world. In this case, the "Barlboro" brand was created with a very similar name and design, as the original "Marlboro" brand of cigarettes. Although many consider user created content to be a feature of many "Web 3.0" technologies, user creations are sometimes direct copies or derivatives of original work that is not their own. Many items in Second Life have parallels in design, logo or naming conventions to products that exist in the real world.

2.3. Legal Issues

Virtual worlds are fast becoming a major aspect in social and commercial activities, which in turn, presents legal issues and concerns. Legal issues that arise in these types of environments usually pertain to purchasing and buying products and services; creating and distributing digital content; and, maintaining and establishing communications. Virtual worlds often invoke questions related to legal issues or at least questions about the application of current laws. It is often complicated to distinguish between elements in physical worlds and elements in virtual worlds. "The line between the real and make-believe is not as easily discernable in the virtual worlds of the 21st century" [11]. Therefore, transference of rules, regulations, and/or policies that would be applicable to elements in physical worlds does not necessarily pertain to elements in virtual worlds. As a result, virtual lives have faced consequences in their real lives. For example, a woman was arrested in Japan after killing her avatar husband in the virtual environment [12]; a woman was charged in Delaware for plotting the real-life abduction of a boyfriend she met through "Second Life" [13].

One other concern relates to scripted objects that could potentially cause harm to other users. Online gambling in the past was legal in Second Life. An Avatar could walk into a virtual casino, play slots or many other available games using the Linden currency. Some players won and some lost, just as in real life. The major difference is that the gambling objects or devices were made by other users, which in turn (as they were unregulated) steal money from players as they were playing by significantly stacking the odds against the player. When large numbers of residents would realize that certain casinos had games that never had any winnings, they would often protest in-world, start campaigns to advertise against certain locations and even start groups to let people know where to avoid. This caused many casino owners to be mindful and to play fairer. As the Linden currency has real value when traded back into the real world, there was a potential for players to lose significant real world money.

2.3.1 Property Rights: Jurisdiction of property rights in a virtual context is not clearly defined or protected. “Imitating real life does not, on its own, create legally cognizable property rights” [11]. Property rights in a physical context can be defined as ownership of something “tangible”. In order to be tangible, it must be a medium fixed or expressed in a physical form in order to be protected. “There are practical limitations to the number of physical objects one can own; e.g., there are natural (and political limitations) to the amount of land that can be owned” [14]. However, property rights in the context of virtual worlds are not as constrained as property rights in virtual worlds. Property created in virtual worlds is easily reproduced and is limitless because it represents intangible objects created using software and hardware technologies.

Virtual properties have been identified as very valuable commodities that make a lot of money for people. However Duranske, indicates that it is important to identify the difference between property and objects in virtual worlds [15]. For example, he states that the object “currency” is handled differently; in the virtual world, currency transactions can take place in a virtual world environment between users or be converted in-world by an outside company. The object “currency” is portable. Whereas, in identifying and protecting virtual land (property), which exist in a virtual world, “...is inherently tied to significant hardware resources that are typically owned by the hosting company” [15 p. 105].

2.3.2 Virtual Property in context to Intellectual Property: Intellectual property is the creation from the intellect (mind). Intellectual property can be defined as “...any unique product of the human intellect that has commercial value” [16]. These facts raise some interesting questions to be considered: Should property acquired in virtual worlds be protected? Is property in virtual worlds intellectual objects or tangible objects?

What rights do property owners have in virtual worlds? These questions in regards to the protection of software have been considered and debated for years among computing scholars and professionals. For example, when considering establishing a learning environment in a virtual world, such as Second Life (SL), there are many intellectual property issues that may arise.

“Two intellectual property issues may arise with classroom use of the Second Life digital worlds. The first such issue has to deal with content produced in the course of a class held in Second Life classroom and the distribution and publication of such material. In November of 2003, Linden Labs issued a press release announcing that Second Life will ‘recognize the ownership of in-world content by the subscribers who make it’ (Linden Labs). Therefore, students and teachers will have to be wary about using created material found in the Second Life world. ...In addition, students and teachers will have to make sure they acquire or purchase permission from the creators to use and distribute materials or designs created in Second Life universe for the class room environment.

One should be mindful that their avatar does not infringe on the rights of others or on any commercial entity. Consider if your avatar looks and acts like a famous actor, or uses unauthorized aspects of a famous person. Though, this is still a “grey area” it is something to consider. Consider a 1992 USA case, *White V. Samsung Electronics America, Inc* [17] where a robot designed to look like Vanna White from the popular game show “Wheel of Fortune” had claim that the robot was violating her right of publicity [18]. Although this case does not illustrate an avatar directly, the implication can be made.

2.3.3 Defamation: In the American culture, freedom of speech is protected by our Fourth Amendment. However, not all speech is protected. For example, the fourth amendment does not provide protection for speech which can result in destruction of character, property, and human life. One way to apply responsible and accountability of freedom of speech is through laws prohibiting defamation. Defamation laws protect individuals and entities from damage to their reputations caused by false statements. The definition of defamation consists of two parts: libel and slander. Libel is described as written and/or visual communication that is defamatory. Slander is described as oral and aural communication that is defamatory. What happens on the Internet/cyberspace has the same, or probably a more profound, personal impact on individuals. Recently, in a news story, a young woman found out that she was being defamed online. This young woman is a successful model and has a vibrant career. One day she found out that there was false libelous information about her being

circulated on the Internet by an individual she did not know. She took legal action against this individual to make them accountable for putting this false information on the Internet. She won her case. It should be noted that individuals have the same recourse if there are false communications about them on the Internet [19].

2.4 Security Aspects for Educational Delivery

The idea of utilizing Virtual Worlds in education is far from new. Many researchers and practitioners have chosen this particular category of platforms to design and deliver their classroom content and laboratory exercises [20]. There are indications that educators are readily accepting virtual worlds as part of their instruction process. Another example uses a common topic in a College Algebra class of exponential/logarithmic functions. The students analyze potential access to data through data mining techniques. A real-life application involves the estimation of time of death. In order to make the topic more "fun", the Multimedia Program at the Community College of Baltimore County-Essex created a game called "The Murder Log" [21]. Based on the popular board game Clue, students need to find the time of death of the victim. Once they have figured out the time of death, a list of suspects is given with the times they entered and exited the room. The suspects include Major Ketchup, Ms. Crimson, Mrs. Sapphire, Mr. Forrest and Madame Ecu. Whoever was in the room at the time of death was the murderer.



Figure 6: The "Murder Log"

This particular educational activity is often associated with the idea of gaming, yet teachers can utilize it to demonstrate the use of notions learned in a classroom and then applied to real-life situations. Given today's state of technology, we can go far beyond the utilization of static 2-dimensional technologies in order to create more interactive simulations. In order to fully take advantage of the potential virtual environments have to offer in conjunction with the ability of hosting multiple users, we propose a lab that centers on identity theft. The purpose of this activity is to create a multi-user virtual environment that can mimic real life and allow students to experience techniques often utilized for identity theft. The simulation contains a built-in information-gathering platform that can then be utilized to mine through the data collected. Such data will be made available to

different courses, to carry out statistical analyses and data mining to uncover patterns.

The lab activity is to be carried out in groups composed of at least 10 students. Each student will receive the assignment of a role. There are two main roles within the simulation: potential victim and thief. Users will carry out activities as the simulation allows. The thief will apply practices of identity theft within the virtual world in order to acquire information about one or more users. The lab activities will last for 2 weeks.

The activities carried out during week 1 below, describes what needs to be performed by users whose role is to serve as potential victims. The user who is acting as thief instead has the ability to perform any of the same functions, and in addition should attempt to steal the identities of others. In an effort to mimic real life and enable each student to carry out the operations described above, each user should have the following material and actions available to them virtually:

- A cubicle, Computer, Desk, Drawers, Books, Bookcase, Trash can (which may or may not be empty)
- An ATM card stored somewhere within their cubicle
 - A PIN number associated with that card
 - Access to an ATM machine within the same simulation
- A credit card account
 - A virtual credit card available to their avatar
 - The account information stored somewhere
 - Written on a piece of paper
 - Stored in a file
 - Photocopy of the latest statement
- Access to at least three web services through their computer: Web Banking, Email-Account, Online bill pay for the credit card
- One PIN/password for each service they have access to which can include: Web Banking, Email Account, Online bill pay, ATM card or Credit Card
- Store at least two of those PIN/password elements within the simulation
 - Example: the ATM's PIN can be written on a piece of paper stored inside a book, at a meaningful page (the avatar was born in December, then the piece of paper may be stored at the fold of page 12)
- Services areas to spend money
 - Virtual Stores and websites

Each object included within the simulation should be able to record at least who handled it, how, and at what time each event occurred. All the data about the simulation will be stored within a data mart, which will be made available to students for the activities reserved for week 2. The simulated environment, in conjunction with the data mart's information, should allow the students to

replay any actions recorded by each object. This will let students review in detail how objects were utilized through week 1's activity. The data and playback features will enable students to take different approaches to the analysis of the identity theft attacks. As an example, computer science students may be able to review how the application of social engineering concepts allows thieves to assume one's identity. Students in mathematics instead may utilize statistical models to review the data and identify potential behaviors and sequences of events. Both domains may study the data through data mining techniques.

3. CONCLUSION

As virtual worlds become more pervasive in our social structures, these topics and issues will continue to have a significant impact on the applications, individuals, and organizations involved. In this paper, the authors examined various aspects of security, ethical and legal issues related to the use of virtual worlds. Specifically, the authors examined Second Life due to its flexible nature and popularity as a new medium for online interaction and collaboration.

It is the intention of the authors to continue research in these areas, which have profound implications on virtual worlds. In future studies, the authors will include Second Life's voice chat feature to better mimic real-life dynamics. Using such technology may be beneficial to adding more realism and further engaging individuals. In addition, through the modification of the appearance of avatars, in combination with all voice/text chat instead of verbal communication, we could observe more accurate results. Through our studies, we will explore the use of Second Life and immersive activities in other domains. More in-depth studies are needed to see if Second Life would be beneficial to simulating security, legal, and ethical concepts.

4. REFERENCES

- [1] Dibbell, J. (1993) 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. *The Village Voice*, December 23, 1993
- [2] Geser, H. (2007) A Very Real Virtual Society: Some macrosociological reflections on "Second Life" In: *Sociology in Switzerland: Towards Cybersociety and Vireal Social Relations*. Zuerich, May 2007 http://socio.ch/intcom/t_hgeser18.htm
- [3] Linden Research. (2008), User Statistics. Retrieved November 23, 2008, from <http://www.secondlife.com>
- [4] Metaversum GmbH. (2009). Twinity [Computer software]. Available at <http://twinity.com/>
- [5] ActiveWorlds. (2009). ActiveWorlds [Computer Software]. Available at <http://activeworlds.com/>
- [6] Makena Technologies. (2009). There [Computer software]. Available at <http://there.com/>
- [7] Wagner, M (Sept 2008), "Second Life's Popularity Rests on Breadth of Activities." *Information Week*.http://www.informationweek.com/news/personal_tech/virtualworlds/showArticle.jhtml?articleID=210602197
- [8] Smedinghoff, T (1996) *Online Law: The SPA's Legal Guide to Doing Business on the Internet*. Thomas J. Smedinghoff, Editor, Reading MA: Addison-Wesley Developers Press 1996.
- [9] Thalmann, N. Thalmann, D (2007) *Autonomous Virtual Characters: Realistic Inhabitants of Artificial Worlds*. *ACM Computing Reviews*.
- [10] Kerr, O. (2008) *Criminal Law in Virtual Worlds*. University of Chicago Legal Forum Retrieved Jan 31, 2009.http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1097392
- [11] Dougherty, C., *E-Commerce Law & Policy*. (July, 2007). Vol. 9, Issue 7.
- [12] Winder, D. (Oct. 2008) Arrested: Virtual wife who murdered avatar husband. *iTWire*. Retrieved Feb. 12, 2010,<http://www.itwire.com/business-it-news/networking/21334-arrested-virtual-wife-who-murdered-avatar-husband>
- [13] Associated Press. (2008). Woman Charged With Plotting to Kidnap Boyfriend She Met on 'Second Life'. Retrieved Feb. 12, 2010, <http://www.foxnews.com/story/0,2933,410781,00.html>
- [14] Tavani, H. T. (2007). *Ethics & technology: ethical issues in an age of Information and communication technology*. (2nd ed.). Danvers, MA: John Wiley & Sons, Inc.
- [15] Duranske, B. T. (2008). *Virtual Law: Navigating the Legal Landscape of Virtual Worlds*. American Bar Association.
- [16] Quinn, M. (2006). *Ethics for the Information Age*. (2nd ed.). Boston, MA: Pearson Education, Inc.
- [17] *White v. Samsung Electronics America, Inc.*, 971 F.2d 1395 (9th Cir. 1992)
- [18] Barfield, W. (2007) *The Right of Publicity in Virtual Reality*. *Virtual Reality 11:69-70* Springer-Verlag.
- [19] (<http://news.cnet.com/the-iconoclast/>).
- [20] Vincenti, G., & Braman, J. (Eds). (2010). *Multi-User Virtual Environments for the Classroom: Practical Approaches to Teaching in Virtual Worlds*. Hershey, PA: IGI Global.
- [21] Community College of Baltimore County – Essex. (2010). *The Murder Log*. <http://student.ccbcmd.edu/immt/PLP/MurderLog/MurderLog.htm>