Privacy in Virtual Worlds: A US Perspective to a Global Concern

Jeannie Pridmore and John Overocker

> *Y'know, watching government regulators trying to keep up with the world is my favorite sport.*
> (Stevenson, 1992: Snow Crash)

1 Introduction

In the first decade of the twenty-first century the number of people connected to the Internet increased from 350 million in 2001 to more than 2 billion in 2010. By 2025, the majority of the world's population, the majority of eight billion people, will be connected to the Internet (Schmidt & Cohen, 2013).

The promise of exponential growth along with technology improvements such as increases in immersion and sensory reality unleashes the possibility that VW could make online experiences as sensuously rich as the physical world. Or perhaps VW could produce an environment that surpasses the real world because of the super-human senses and abilities that are embedded within them such as flying, walking through walls, and 1 day being able to experience all five senses through the VW.

As this space grows larger, VW will allow an increasing amount of people to live their lives by blending their real world life with their virtual life in a way that could erase the differences between the two completely. The blending of virtual lives and real lives raises questions of how privacy rights should be applied in VW?

The basic conceptions of a particularized right to privacy could be said to have existed for centuries. The argument could be made that the concept of ordered liberty would be impossible without the implied right of privacy. Nevertheless, the first significant mention of the "Right to Privacy" was a landmark Law Review Article authored by Justice Louise Brandeis and Samuel Warren in 1890.

Justice Brandeis considered privacy as the "most comprehensive of rights and the right most valued by civilized men (Brandeis, 1928)." In 1986, Mason predicted

J. Pridmore (✉)
University of West Georgia, Carrollton, GA, USA
e-mail: jpridmor@westga.edu

J. Overocker
Public Defender's Office Coweta Judicial District, Carrollton, GA, USA

Y. Sivan (ed.), *Handbook on 3D3C Platforms*, Progress in IS,
DOI 10.1007/978-3-319-22041-3_6

that the advent and use of Information and Communication Technology (ICT) would lead to four major concerns about the use of information: (1) Privacy, (2) Accuracy, (3) Property, and (4) Accessibility (Bélanger & Crossler, 2011). Since information often flows based on what is technologically possible rather than on what is socially or legally acceptable (Sundquist, 2012), privacy in particular has been a subject of increasing concern over the last few years for both individuals and organizations. In addition, Erik Snowden's revelations about the extent to which the United States' National Security Agency (NSA) has infiltrated both foreign and domestic organizations (governmental and non-governmental,) the Internet and the ability to protect the information we transfer and store on it have become a topic of international interest. It had been estimated that the NSA has the ability to intercept and download electronic communications equivalent to the contents of the Library of Congress every 6 hours (Mayer, 2011).

A recent survey showed that one in four young adults have exposed things through ICT that they fear could be used against them when it comes to employment, and among 18–34-year-old ICT users, 29 % say they feared that their photos, comments, or other personal information could come back to hurt them—either by causing a prospective employer to turn them down for a job, or by giving a current employer a reason to fire them (Croteau, 2013).

While individuals believe they should protect and control their personal information online (Deloitte Touche LLP & Ponemon Institute, 2007), people are posting, disclosing, and living out their lives online at ever increasing rates. This creates an enormous amount of personal data that are easily monitored and stored. Thereafter, data that was not intended to be public are, in some cases, accessed by other individuals, organizations, and governments.

Moreover, most of the basic business models of some of the largest companies operating online revolve exclusively around the collection and cultivation of this information. Most consumers operate under the misconception that they are the customers of their e-mail provider or social networking sight. The sobering reality is that the average "consumer" is in fact the product.

These companies provide services for free to the consumer and in turn collect information, which can be sold to third parties or handed over to governments. This exchange is often if not exclusively done without the knowledge of the "User."

The debate between privacy and security, as well as the trade-off between free or inexpensive services versus protection of private information will only heat up as more information is transferred from the Physical World (PW) to the VW for storage and transmittal. While economic theory suggests people have an ability to process the stream of privacy threats and trade-offs in the virtual world, people simply cannot be expected to navigate this uncertain terrain on their own (Acquisti & Grossklags, 2005). The lack of regulatory action and the growth of technology allows for potentially more privacy violations on a faster and larger scale.

VW are not lawless; however, VW technology presents new and unique situations that do not fit neatly into current legal frameworks (Nelson, 2011) or with other online privacy issues. The law that is applied is ill-fitted and in some situations illogical (Chambers-Jones, 2013). Overall, VW are under-regulated and

deserve full and objective consideration in terms of privacy. They should not be grouped with the other ICT. The focus of this chapter is twofold.

1. Explain why VW should be considered separate from other ICT.
2. Grasp the current state of privacy rights for VW users in the US.

In conclusion, critical issues are identified that needs to be addressed in future research projects.

2 Virtual Worlds

The technology used in VW can be seen as another layer of coding that exists within the Internet. VW began as multi-user dungeons (MUD) and MUD object oriented (MOO), which were early text-based multi-user environments that combined role-playing with social chat rooms. From these early proto-ancestors evolved the graphically complex and highly immersive massive multiplayer online games (MMORPG) that serve as today's VW.

Today, VW are not just for game play. They provide a platform for users to explore, work, educate, and research. Users, in their virtual form as avatars, can wander around and experiment in an unstructured goal free environment or engage in purposeful activities.

For example, in Second Life, users in the form of an avatar can spend the day visiting Paris, flying over the ocean, relaxing on a secluded beach, or build their own virtual property like houses, cities, clubs, or a business store front in which virtual goods can be exchanged for real money.

Second Life avatars, if their users are so inclined, can even engage in virtual sexual activity or violence (Blitz, 2009). While some might argue that these virtual acts or virtual properties mean nothing in the real world, real world harm, either physical or financial, could be inflicted through the use of a VW.

In addition, VW allow for the PW and the VW to interchange. For example, some VW allow business employees to begin a conference call in the real world, and then continue it in the VW where the avatars cannot only share ideas but can also explore business models in a 3D space (Blitz, 2009). VW are thus an expansion of the quasi-physical world and should reflect the social norms and cultural of their society.

A vast amount of personal information can be recorded, stored, and analyzed in VW in a way that is simply not possible in the PW. VW technology has been specifically developed to store and analyze everything that its users do, so the VW can adapt around what the user is doing or has done. This information includes body movements, facial expressions, the people they interact with, what the interaction was about, the times the interaction took place, and consumer preferences.

These records can be connected to specific users and can sometimes be connected to their physical self. In addition, users who work or play in VW tend to be connected for several hours every day because of the immersive nature of

VW. This means much more data can be collected than with other ICT along with an easier and usually more accurate way of connecting the VW avatar with the real life person.

When creating a VW account, there is usually no process or procedure to verify the identity of the individual who is creating the account. Using someone else's identity to create an account and an avatar is very easy. The avatar identity could be completely fabricated, or it could be an entity using it to spy on others. Someone could a fake identity or steal a person's identity to purposefully or inadvertently do harm.

VW technology can also enable other individuals to spy on users without them ever knowing. This means that someone can collect and store information about users without that person being aware of it or without them being a willing subject. Furthermore, users have a level of anonymity when living as an avatar in a VW. This could lead to users disclosing more personal information than in other virtual environments.

Lastly, user driven content is another reason why VW are different than other ICT. Users build houses and businesses were they live and conduct business as if they were in the real world. Avatars can have families and dogs. They can watch movies and go on dates. Businesses create virtual goods which can be sold. Some individuals have even developed cities for their avatar and other avatars to live inside. Many real world universities and organizations conduct daily activities through VW. Users and organizations are constantly creating and adding to the VW in which they live and work.

Therefore, today's VW pose new and specific privacy concerns that are at times far greater than those arising in other ICT interactions. It is necessary to investigate the possible issues that affect privacy in VW. Zarsky (2006) identified two basic categories.

1. Privacy concerns that result from moving personal information between the VW and the physical world.
2. Privacy concerns that pertain to the collection, analysis and use of personal information exclusively within the VW.

The various forms of privacy concerns depend on the level of access to the flow of personal information available in VW. VW owners and their business affiliates have easy access to the entire scope of data described above. Using this data an overall profile of the user could be very accurately constructed as well as easily being linked to their real life identity.

3 The Right to Privacy in the United States

Before discussing privacy in VW, the legality of privacy in the US needs to be explained. The right to privacy in the United States is far too broad a topic to be tackled in one paper.

There is, to a certain extent, even a debate as to whether a right to privacy exists in the United States. *See Griswold v. Connecticut,* 381 U.S. 479 (1965) (*J. Black dissenting*.) In which Justice Black makes the case that there are no specific protections of a citizen's privacy only instances when privacy protection is a peripheral effect of the enforcement of other rights. The emergence of the right to privacy is of very recent origins (Rubenfeld, 1989). The fact that personal information is now much more of a commodity (more so than in 1890, or 1990, for that matter), may require privacy rights to be examined more as individual property. However, for the purposes of this chapter, the writers take the view that a right to privacy does exist, (*J. Goldberg concurring*).

This chapter will focus primarily on the Expectation of Privacy. This Expectation, which varies from place and situation, is the method by which the Courts determine Government action as reasonable under the protection of the Fourth Amendment.[1] The right to privacy protects an individual's right to be protected from unreasonable or offensive intrusion into their private affairs and concerns.

This right protects both physical privacy and other intrusions, such as the prevention of eavesdropping, restrictions on persistent, unwanted telephone calls, and prying into some forms of personal records. Privacy concerns generally involve at least one of three groups:

1. Government
2. Private Entities
3. Other Individuals

The US Constitution is a limiting document on the government's power and does not protect individual's privacy from the invasion by private citizens or entities. This holds true even if the information or property is later handed over to the government, unless the third party was operating under government instruction.

The Fourth Amendment states, "(t)he right of people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The Fourth Amendment protects against *unreasonable* search and seizure by the government.

A Seizure occurs when the government takes possession of items or detains people. A search is any intrusion by the government into something in which one has a reasonable expectation of privacy. Typically, eavesdropping or wiretapping of communications can constitute an illegal search and seizure. Though the Fourth Amendment only protects privacy from the government, it is important to highlight what it does and does not include in Table 1 (adapted from "Fourth Amendment", 2013). These details illustrate some of the complications in the right to privacy topic.

[1] The Supreme Court applied the Fourth Amendment to the individual states in the landmark case *Mapp v. Ohio*, 367 U.S. 643 (1961).

Table 1 Fourth amendment privacy details

Area	Protected	Not protected
Residences	Individuals in their homes have the highest expectation of privacy.	Conversations or other sounds inside a home that a person outside could hear, or odors that a passerby could smell without technological help to do so. If an individual opens their house to the public for a party, or some other public event, police officers could walk in posing as guests and look at or listen to whatever any of the other guests could.
Business premises	Individuals in their offices have a reasonable expectation of privacy if the office is not open to the public.	But if there is a part of the office where the public is allowed, like a reception area in the front, and if a police officer enters that part of the office as any other member of the public is allowed to, the officer can look at objects in plain view or listen to conversations there.
Trash	None	The things left outside a home at the edge of the property are unprotected by the Fourth Amendment.
Public places	Fourth Amendment challenges have been unsuccessfully brought against police officers using monitoring beepers to track a suspect's location in a public place, but it is unclear how those cases might apply to more pervasive remote monitoring, like using GPS or other cell phone location information to track a suspect's physical location.	Individuals have little to no privacy when in publications, movements, and conversations are knowingly exposed to the public—even if the individual thinks they are alone, they can be watched and recorded.
Infiltrators and undercover agents	None	Public meetings of community and political organizations, just like any other public places, are not private. Importantly, the threat of infiltrators exists in the virtual world as well as the physical world: for example, a police officer may pose as an online "friend" in order to access private social network profile.
Records stored by others	None	According to the US Supreme Court, information obtained and revealed by a third party to Government authorities is legal, even if the information was revealed on the assumption it would only be used by the third party for a limited time and for a specific purpose.

(continued)

Table 1 (continued)

Area	Protected	Not protected
Opaque containers and packages	The contents of any opaque (not see-through) clothes or containers—laptops, pagers, cell phones and other electronic devices.	Anything exposed to the public is not protected. For example, if an individual in a coffee shop uses their laptop and an FBI agent sitting at the next table can see what is being written in an email; or if they open their backpack in a way that the FBI agent can see what is in the backpack.
Postal mail	If using the U.S. Postal Service, a package sent using First Class mail or above is protected, and a search warrant is needed to open the package.	There is no expectation of privacy in regard to the "to" and "from" addresses printed on the package, or what is written on a postcard.
Electronic surveillance	None	This is still being debated, but currently the US government can use electronic devices that are available to the public to monitor individuals without a warrant since this can be done without having to enter a private dwelling or use equipment not available to the public.

Adapted from Fourth Amendment (2013)

Technology has added complexity to this topic, and is proving to be a substantial challenge for law makers to understand how technologies can and should be used in keeping with the right to privacy. The Supreme Court has offered little guidance by distinguishing between technology such as powerful binoculars that simply enhance an individual's senses and technology that creates new superhuman powers such as spyware. At times, they have relied on a distinction between sense enhancement and sense creation, a superficial distinction that fails to delineate when new surveillance technology is problematic.[2] *Katz v. United States,* 389 U.S. 347.

At other times, the Court has used language indicative of past Fourth Amendment doctrine requiring some sort of physical trespass in order to elicit the warrant requirement. The Court rejected that doctrine in *Katz*,[3] when it recognized that new technologies can make a private space versus public space impracticable to discern.

[2] *Katz v. United States*, 389 U.S. 347 (1967).

[3] In *Katz*, *supra*, the Supreme Court found that "the Fourth Amendment protects people, not places." Thus when a person enters a telephone booth, shuts the door, and makes a call, the government cannot record what that person says on the phone without a warrant. Even though the recording device was a public infrastructure phone when Katz shut the phone booth's door he reasonably expected no one would hear his conversation and it was protected from government intrusion.

In addition, the Courts have found that email enjoys the same level of protection as traditional mail.[4] However, the Court's failure to clearly explain the concerns about new technology and arbitrary use of language has confused the lower courts (Fairfield, 2009).

Since the Fourth Amendment applies to the government, the biggest concern for privacy of US citizens would be that of private organizations collecting, storing, and possibly selling personal data. However following the events of September 11, 2001, Congress passed the Patriot Act. The Patriot Act has been touted as necessary for law enforcement, providing the tools to prevent future acts of terror. Still, the Patriot Act gave the US government unprecedented authority to conduct surveillance. Thus privacy intrusions and government overreach have been a concern since its passage. The Patriot Act increases the government's surveillance powers in the following areas ("The US Patriot Act").

1. It increases the government's ability to look at an individual's records being held by third parties (Section 215).
2. It increases the government's ability to search without notice private property (Section 213).
3. It widens a narrow exception to the Fourth Amendment that had been created for the collection of foreign intelligence information (Section 218).
4. It extends the Fourth Amendment exception for spying and gathering "addressing" information about the origin and destination of communications, as opposed to the content (Section 214).

Government officials say that these powers are only invoked on people of interest or individuals who are suspected of wrong doing or are associated with known terrorists. However, critics have raised concerns about the possible over reach and unchecked government power to electronically track individuals with little or no evidence. These concerns are based the following issues:

1. The government no longer has to provide proof that the subjects of search orders are an "agent of a foreign power," previously this requirement protected Americans against abuse of this power.
2. The government does not have to provide reasonable suspicion or "probably cause" that the records are linked to criminal activity. The government simply has to make a broad assertion that the request is associated to an ongoing terrorism or foreign intelligence investigation.
3. Judicial oversight of these new powers is basically non-existent. The government must only certify to a judge that the requested search meets the statute's broad criteria, and the judge does not have the power to reject the request.

[4] *Randolph v. ING Life Insurance and Annuity Company*, 486 F.Supp.2d 1 (D.D.C., 2007) limits prospective liability where a loss or theft of personal data presents no more than a speculative threat of invasion of privacy, identify theft, or fraud. The case, which was resolved on a motion to dismiss, reflects the trend in U.S. case law that data controllers will not necessarily face liability for losing control of personal information if the loss did not cause actual harm.

4. Surveillance requests can be based partly on a person's First Amendment activities, such as Web sites visited, books read, or editorial letters written.
5. If a person or organization is forced to turn over records, they are prohibited from disclosing the search to anyone. As a result, the subjects of surveillance might never know that their personal records have been investigated by the government. That undermines an important check and balance of this power: the ability of individuals to contest illegitimate searches.

Again, the US government has continued to assure the public that these new powers are only utilized against those who have displayed concerning behaviour. However if the revelations of Eric Snowden are to be believed, they show the ease with which the government tracks and stores Internet activity. According to Mr Snowden, the NSA has operatives currently working undercover using fake online personas in VW such as Second Life, World of War Craft, and Eve for surveillance purposes.

In addition, Mr Snowden has informed the world that the US government has worked with major organizations such as Apple, Microsoft, and Google, to name but a few, to influence their encryption techniques. We believe this is, so far, to be the most concerning revelation. These are multi-national corporations with products at every corner of the globe, and the security of those products are suspect at best.

This leads many to wonder if the US government could have access to every Internet transaction that occurs without ever having to ask for that information from a third party. Thus, the US government could essentially have a back door into a number of Internet technologies in order to track anyone on Earth who us online they want.

So far, the information shared by Mr. Snowden have not been the catalyst for any changes to the Patriot Act, interpretation of the Fourth Amendment, or led to the creation of new laws. Still, Mr. Snowden has made the world aware of the extent to which the United States Security establishment has gone to track online activity and how few safeguards exist. Even President Obama during his 2013 end of the year press conference stated that a review of procedures and powers should take place in 2014, and that specific policy questions needed to be asked and answered.

For instance, should policies be based on what is possible for the government to do or what they should do? Notably, the President did not call for a stop to the practice of collecting information. President Obama merely suggested that the personal data collected should not be mined for information without just cause for US citizens. This "privacy protection" would not apply to international citizens.

From a third party, or private party, perspective, the Second Restatement of Torts (2000) states that an individual will be liable for unreasonable intrusion if he intentionally intruded upon the solicitude or seclusion of another and the intrusion is highly offensive to a reasonable person. This cause of action has been used primarily to prevent information gathering that reasonable people would find offensive. An individual may have a claim against a speaker who publicizes a

private fact that does not have public concern and the disclosure of which a reasonable person would consider offensive.

In summary, privacy rights fall into three categories in the United States.

1. A citizen's right to privacy against government intrusion is guaranteed by the Fourth Amendment and Supreme Court cases such as Griswald v. Connecticut[5] (1965).
2. 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 (Prosser, 1960).
3. *Sui generis*[6] statutes emerge when legislatures seek to protect data in specific situations (Blanke, 2001).

Sui generis, or the so called right to be left alone, has been further divided into four categories (Prosser, 1960).

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
4. Publicity that unreasonably places the other in a false light before the public

These principles are currently the most relevant to privacy in VW.

4 The Right to Privacy in VW

What does all of this mean to the right to privacy in VW? Is there a reasonable expectation of privacy when in a VW? If there is, what is it? A reasonable expectation of privacy only exists if an individual can expect privacy, or if the expectation of privacy is one that society considers legitimate.

To date, courts have not reached a consensus on what constitutes a reasonable expectation of privacy online (Fairfield, 2009). A point of contention is whether reasonable expectations of privacy are determined by what the government can collect or what it should collect (Fairfield, 2009). It is important to note that an individual, either a private individual or a government agent, could join a VW with a fake identity and monitor whomever they wanted without ever obtaining a search warrant or having to reveal who they really are. Again, according to Mr Snowden, this has been going on for several years now.

[5] In *Griswold*, *supra,* the Court held that the right of privacy within marriage predated the Constitution. The ruling asserted that the First, Third, Fourth, and Ninth Amendments also protect a right to privacy.

[6] A law created by the legislature to protect intellectual property that might not otherwise be protected. See Black's Law Dictionary (8th Edition).

The Supreme Court has found there is no reasonable expectation of privacy for information an individual "knowingly exposed" to a third party—for example, bank records, telephone records, or possibly even VW records—even if it was intended for the third party to keep the information private (Fourth Amendment, 2013). By engaging in transactions in a VW, the Court contends, individuals are assuming risk that the third party will share that information with the government or other third parties as stated in the user agreement.

When an individual signs up for a VW and creates an avatar, normally they must agree to the terms of the VW owners. These agreements are typically referred to as End User License Agreements (EULA), Terms of Service (TOS), or simply set out in lesser documents such as Codes of Conduct and Reimbursement Polices (Lim, 2008). Many commentators criticize these contracts as being too one-sided and argue for the courts to acknowledge traditional common law rights (Cifrino, 2014).

An individual may "knowingly expose" more than they know or intend to due to the terms of the agreement. By signing this agreement users agree to the privacy terms the VW owners and operators. All of the data collected, stored, and analyzed are done with the user's permission. All rights are waivable thus this collection is probably not protected by the Fourth Amendment under current law. There may be privacy statutes that protect against the sharing of this information—some communications records receive special legal protection, for example—but there is likely no constitutional protection. Thus, if so inclined the government may easily obtain that information without the individual ever being notified.

The users of VW are bound by the rules put forth by the VW owners in the EULA, TOS, or Codes of Conduct and Reimbursement Polices. These agreements are lengthy and, complicated. With increasing frequency VW's require users waive significant rights before they may use their products. Some have argued that these agreements are not efficient, not legally secure, and give the VW owners all of the control (Roquilly, 2011).

It has long been said that the biggest lie told on the Internet today is "Yes, I have read and agree to the terms" (Finley, 2012). To illustrate how users are becoming aware of the one sided nature of these interactions, websites and even a Facebook page exist, dedicated to the topic of unfair, long, and confusing TOS agreements.

This is not to say that the Internet or VW are devoid of laws or regulation. The US currently uses a "3-E Approach" (**E**ducation, Targeted **E**nforcement, **E**xisting Legal Standards) in regard to online privacy. The US realizes the need for adaptation for online privacy due to the complications that arise from different technologies, different uses and different situations.

The "3-E Approach" presumes the impossibility of crafting a single, universal solution to online privacy concerns. It aims instead to create a flexible framework to help individuals cope with a world of rapidly evolving technological change and shifting social and market norms as they pertain to information privacy (Thierer, 2013). One problem with the "3-E Approach" is that most of the responsibility is on the user. As a possible result of this, no other countries seem to be taking the US' "3-E Approach" as a guide to online privacy. The European Union has drafted their

own policy which seems to be having a more immediate global impact (Thierer, 2013).

Overall, there seems to be two main camps when it comes to how privacy rights should be set for VW. One camp believes privacy rights should be set by the "market" referred to as "separatists" (Chambers, 2012). This group believes that market pressures or industry pressures from users or society will force self-regulation that will ultimately create the best outcome.

The second camp believes privacy rights should be regulated by the government or "inclusionists" (Chambers, 2012). While education and user empowerment is important, some government regulation will be critical moving forward. It will be interesting to see what impact if any the Snowden revelations will have on privacy policies moving forward.

Given the diverse needs and use of VW technologies, no silver bullet, all in one solution is likely to be forthcoming. Both sides require scrutiny and consideration in order to develop privacy education for all users. This would include the importance of TOS, empowered users who understand how critical they are to the success of VW, and legal professionals who can impart upon law makers which privacy laws and rights are essential for online user protection.

5 The Future of Privacy in VW

Future debate and research is critical for the field on privacy rights in VW, and this debate needs to happen now not only from a US perspective but also as a global concern. People need to understand how the virtual world works and the regulations/laws that apply them in the virtual world. Even the European Network and Information Security Agency has stated that privacy is a major risk from Avatar identity theft and fraud to the amount of personal data being exchanged in the virtual world (Farahmand, Yadav, & Spafford, 2013).

Can a reasonable expectation of privacy ever exist for data in VW, and could this data ever be protected by the Fourth Amendment? How is the answer to the previous question affected by the fact that sometimes the data was "knowingly exposed" to a third party, other individuals, or to the public at large? To attempt to answer this question, three main areas of future research are put forth in Table 2.

5.1 Private Space Versus Public Space

First it is critical to realize if a private space could ever exist in a VW. This is an important point in determining privacy rights in VW. Previous court cases have found phone calls on public pay phones are private conversations. Similarly, email is afforded the same protection as United States Postal Mail service. A logical conclusion could be that certain parts of VW might also be afforded such rights and

Table 2 Future research areas

Private space versus public space	(1) Could user driven content areas be seen as private spaces? (2) If so, is there a level of privacy that someone could reasonably expect when entering a "private space" in a VW?
Online persona	(1) Since avatars are the virtual representation of a real person, could real life privacy laws be applicable?
Online persona and property rights	(1) Could privacy laws be the answer to virtual property theft? (2) Could privacy laws be used to protect users' intellectual property rights?
Global privacy concerns	(1) Could privacy regulations exist on a global level? Would this be enough to ensure protection? (2) Is there a market for privacy services to be bought on an individual basis worldwide? If so what would those services look like?

protection. For example, if user driven content areas such as houses or business could be considered private property inside a VW, it is possible that the data exchanged in those areas could maintain the same rights as in the PW.

Since users can build and live in houses and run businesses in VW as well as being able to perform very personal private acts in VW, it could be argued that there is a reasonable expectation of privacy in specific situations even though the actions are being conducted online in a VW. In these situations, individuals probably have a sense of privacy, and that could be a very strong case for the right to privacy of the user while in a "private space" of a VW. This creates questions that need to be answered.

1. Could user driven content areas such as houses, businesses, etc. be seen as a "private space"?
2. If so, is there a level of privacy that someone could reasonably expect when entering a "private space" in a VW?

It is not easy to answer questions like these. First, there must be a discussion if it is possible to distinguish between a public and private space in VW? This has been a much debated topic. On one side of the debate, some have argued that VW are, in fact, public spaces as they represent the essence of public spaces (Oliver, 2002).

Others have argued that VW are not public spaces as they are carefully controlled with certain rules and regulations crafted by the owners of the VW environment (Taylor, 2002) and a large part of the success of a VW can be attributed to user driven content. In terms of corporate ownership, user driven content and intellectual property rights, VW and spaces contained in them could function as "private spaces".

A PW comparison of a VW could be similar to a shopping mall, meaning a private space that is often perceived as being a public space. However, if a person owns and operates a business space within the shopping mall, the only part of that business that is considered public is the area where the public is welcomed. Could this distinction also be made in a VW business? What about a house in real life?

Every individual has a right to privacy in their home. What about the right to privacy in a virtual house?

If these two situations can be interchanged between the VW and the physical world, then should the same privacy rights extend to the VW as it does to a real world? Further, since information in briefcases and backpacks carry privacy protections, why should virtual identities created with user driven content such as photos, email addresses, and correspondences not carry the same privacy rights?

For the user, the distinction between whether a VW space functions as a public space or as a "private space" could be an important factor in determining the expectation of privacy when living in a VW. Since Privacy is based on what is "reasonable" or what a "reasonable person" expects, it could be reasonable to poll people as to what they expect from both a US and global perspective. For now, users who lack a proper understanding of what "private spaces" or public spaces are in VW will continue to expose information that they otherwise would protect. After realizing the information has been revealed they may feel as if their privacy has been violated when in fact those protections did not exist or have been waived by the users. A more formal clarification or distinction between what public and private spaces will continue to be ambiguous until users of VW force the conversation with the VW owners and operators and possibly demand action to regulate on their behalf. Until then, users should take reasonable precautions and assume that their information is vulnerable.

5.2 Online Persona

It has been suggested that the best way to protect VW users is through the concept of personhood or persona (Nelson, 2011). An online persona consists of an individual's attributes that identify them to a reasonable third party and is comprised of their name, signature, photograph, image, likeness, and voice (Kutler, 2011). Therefore, an online persona identifies a person to others (third parties, government entities, or private individuals) through email accounts and online identities such as VW avatars. Especially in VW where the avatar becomes an extension of the physical person's self from the formation of the avatar's interest and actives to their personal relationships (Blitz, 2009).

The online persona is an intangible, yet legally protectable asset (Kutler, 2011). However, avatars do not maintain the same online privacy rights as their physical selves do. From a government perspective, this could be explained by not having to physically infringe upon the person to collect the data. From the private third party perspective, the individual agreed to the terms of service by clicking the "I Agree" button. If it could be argued that the avatar is truly an extension of the physical person, then should the same privacy rights be extended to the avatar in a VW as they are applied to the individual in the physical world?

In addition, what if someone takes another person's name, builds a VW avatar, and lives in the VW as that other person. Even if the VW is contacted and this

offense is covered in the VW TOS, what penalty is imparted for this invasion of persona and right to privacy? At best, the account will be removed, and the VW might be able to block that user from ever creating another account. Should that individual be held accountable in the real world? What if that person caused mental or physiological harm on the person whose identity they took in the real world? Given the connection between the online persona and the physical persona, it's hard not to understand that real world harm could be inflicted in this given scenario.

What if the fake account was created to steal virtual property from the user? It has been argued that privacy laws could be used as an efficient way to protect users against virtual property theft. Virtual property theft violates the persona of the VW user because it invades the private areas of the victim's identity and privacy (Nelson, 2011). One possible reason as to why privacy could be an efficient way to govern the theft of virtual property is that it is hard to assign value to virtual property, but it is much easier to understand the personal connection to the loss of property even if it is virtual property.

5.3 Privacy in VW: A Global Concern

Since VW are global entities, it would be short sighted to consider it only from a US perspective and not discuss it as a global concern. As Eric Snowden has made everyone aware, now is the time to stand up for online privacy rights on a global level. Is it possible to create a code of privacy or a right to privacy on a global level? What would be or should be included in a global privacy policy?

Google has encouraged the UN to set global privacy rules since so much data is sent around the world to countries that do not have any privacy regulations (Johnson, 2007). The possibility that the UN might try to step in is causing opposition from many organizations and countries worldwide (Thierer, 2012). There are policy groups such as the Global Internet Policy Initiative (http://www.internetpolicy.net/) which is a non-profit organization that collects Internet policy information to help transitional countries develop policies such as privacy rights to protect their citizens.

Lastly, could the right to privacy be something people are willing to pay for on an individual level worldwide? Would someone be willing to pay $3 or $5 a month to ensure that their virtual information would not be tracked? Would or could these kinds of privacy services emerge if users demanded it? What would be included in services like this, and could they actually guarantee privacy on a global level? How would individual privacy compared to the public's right to know or information for the greater good be balanced? Is this possible? Some countries around the world are hoping this could be possible and could serve as a source of revenue (Thierer, 2012).

6 Conclusion

Currently privacy rights of VW users are set up and defined by the TOS of the VW. The argument is put forth that privacy rights in VW need to be reconsidered from a legal stance and a user rights perspective. This should be approached in two ways, from the VW users working with the VW to improve their rights in the TOS and improved government privacy regulation as called for by the VW community. As in the days of the Wild West, the law has been slow to make its way into the realm of VW. Privacy laws or the right to privacy is critical at this point in the development of VW for several reasons.

For one, technology is advancing so fast, it is important to begin this process today if there is any hope in being able to keep up with new technology as it is introduced. Secondly, with the global aspects of VW and the rise of the Internet population from developing countries VW may soon be experiencing a flood of users that may not share the same concept of privacy as most "Western" users because of cultural and legal differences. Setting the foundation for future growth in the definition of online privacy is a critical subject that needs to be addressed now. Without established standards in place this large influx of new users who may not be concerned or share the same concept of privacy could detrimentally impact the expansion and definition of privacy rights and protection to VW users.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy, 3*(1), 26–33.

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly, 35*(4), 1017–1042.

Blanke, J. M. (2001). Criminal invasion of privacy: A survey of computer crimes. *Jurimetrics Journal, 443*, 449–456.

Blitz, M. J. (2009). A first amendment for Second Life: What virtual worlds mean for the law of video games. *Vanderbilt Journal of Entertainment & Technology Law Journal, 11*, 779–822.

Brandeis, J. (1928). Olmstead v. United States, 277 U.S. 438, 478 (dissenting).

Chambers, C. (2012). Can you ever regulate the virtual world against economic crime? *Journal of International Commerical Law and Technology, 7*(4), 339–349.

Chambers-Jones, C. (2013). Virtual world financial crime: Legally flawed. *Law and Financial Markets Review, 7*(1), 48–56.

Cifrino, C. J. (2014). Virtual property, virtual rights: Why contract law, not property law, must be the governing paradigm in the law of virtual worlds. *Boston College Law Review, 55*(235), 235–264. http://lawdigitalcommons.bc.edu/bclr/vol55/iss1/7.

Croteau, M. (2013). *A quarter of young people have facebook or other social media postings they may later regret, says New FindLaw.com survey*. Retrieved from http://company.findlaw.com/press-center/2013/a-quarter-of-young-people-have-facebook-or-other-social-media-pos.html#sthash.49cjPJ1z.dpuf

Deloitte and Touche LLP, & Ponemon Institute LLC. (2007). *Enterprise@Risk: 2007 privacy & data protection survey*. Retrieved from http://www.deloitte.com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf

Fairfield, J. (2009). Escape into the Panopticon: Virtual worlds and the surveillance society. *The Yale Law Journal Pocket Part, 118*, 131–135.
Farahmand, F., Yadav, A., & Spafford, E. H. (2013). Risks and uncertainties in virtual worlds: An educators' perspective. *Journal of Computing in Higher Education, 25*(2), 49–67.
Finley, K. (2012). Putting an end to the biggest lie on the internet. *Tech Crunch*. Retrieved September 29, 2013, from http://techcrunch.com/2012/08/13/putting-an-end-to-the-biggest-lie-on-the-internet/
Fourth Amendment. (2013). Legal Information Institute, Cornell University of Law School. Retrieved August 1, 2013, from http://www.law.cornell.edu/wex/fourth_amendment
Griswold v. Connecticut (1965). 381 U.S. 479, pp. 483–484.
Johnson, B. (2007). Google urges UN to set global internet privacy rules. *The Guardian*. Retrieved from http://www.theguardian.com/technology/2007/sep/14/news.google
Katz v. United States. (1967). 389 U.S. 347, 358–359.
Kutler, N. (2011). Protecting your online you: A new approach to handling your online persona after death. *Berkeley Technology Law Journal, 26*, 1641–1668.
Lim, H. Y. F. (2008). Who monitors the monitor-virtual world governance and the failure of contract law remedies in virtual worlds. *Vanderbilt Journal Entertainment & Technology Law, 11*, 1053–1073.
Mayer, J. (2011, May 23). The secret sharer: Is Thomas Drake an enemy of the state? *New Yorker*, pp. 47–49.
Nelson, J. W. (2011). A virtual property solution: How privacy law can protect the citizens of virtual worlds. *Oklahoma City University Law Review, 36*, 395–420.
Oliver, J. H. (2002). The similar eye: Proxy life and public space in the MMORPG. In *Proceedings of the 2002 Computer Games and Digital Cultures Conference* (pp. 171–184).
Prosser, W. L. (1960). Privacy. *California Law Review, 48*(3), 383–423.
Restatement (Second) of Torts (2000) § 625C.
Roquilly, C. (2011). Control over virtual worlds by game companies: Issues and recommendations. *MIS Quarterly, 35*(3), 653–672.
Rubenfeld, J. (1989). The right of privacy. *Harvard Law Review, 102*(4), 737–807.
Schmidt, E., & Cohen, J. (2013). *The new digital age: Reshaping the future of people, nations and business*. New York: Knopf.
Stevenson, N. (1992). *Snow crash*. New York: Random House Digital.
Sundquist, M. (2012). Online privacy protection: Protecting privacy, the social contract, and the rule of law in the virtual world. *Regent University Law Review, 25*(153), 1–29.
Taylor, T. L. (2002). 'Whose game is this anyway?' Negotiating corporate ownership in a virtual world. In *Proceedings of the 2002 Computer Games and Digital Cultures Conference* (pp. 227–242).
The USA PATRIOT Act: Preserving life and liberty. Retrieved October 15, 2013, from http://www.justice.gov/archive/ll/highlights.htm
Thierer, A. (2012). *Does the internet need a global regulator?* Retrieved from http://www.forbes.com/sites/adamthierer/2012/05/06/does-the-internet-need-a-global-regulator/2/
Thierer, A. (2013). Privacy, security, and human dignity in the digital age: The pursuit of privacy in a world where information control is failing. *Harvard Journal of Law & Public Policy, 36*, 409–915.
Toney v. L'Oreal USA, Inc. (7th Cir. 2005). 406 F.3d 905, 908-09.
Zarsky, T. (2006). Privacy and data collection in virtual worlds. In J. M. Balkin & B. S. Noveck (Eds.), *State of play—Law, games and virtual worlds* (pp. 217–223). NY: NYU Press.