Violent Victimization in Cyberspace: An Analysis of Place, Conduct, Perception, and Law

by

Hilary Kim Morden

B.A. (Hons), University of the Fraser Valley, 2010

Thesis submitted in Partial Fulfillment
of the Requirements for the Degree of Master of Arts

IN THE

SCHOOL OF CRIMINOLOGY

FACULTY OF ARTS AND SOCIAL SCIENCES

SIMON FRASER UNIVERSITY

Summer 2012

Approval

Name:	**Hilary Kim Morden**
Degree:	**Master of Arts (School of Criminology)**
Title of Thesis:	***Violent Victimization in Cyberspace: An Analysis of Place, Conduct, Perception, and Law***

Examining Committee:

Chair: Dr. William Glackman, Associate Director Graduate Programs

---

Dr. Brian Burtch
Senior Supervisor
Professor, School of Criminology

Dr. Sara Smyth
Supervisor
Assistant Professor, School of Criminology

Dr. Gregory Urbas
External Examiner
Senior Lecturer, Department of Law
Australian National University

Date Defended/Approved: July 13, 2012

Partial Copyright Licence

Abstract

The anonymity, affordability, and accessibility of the Internet can shelter individuals who perpetrate violent acts online. In Canada, some of these acts are prosecuted under existing criminal law statutes (e.g., cyber-stalking, under harassment, s. 264, and cyber-bullying, under intimidation, s. 423[1]). However, it is unclear whether victims of other online behaviours such as cyber-rape and organized griefing have any established legal recourse. Examples of virtual violence in social networking sites, immersive games, and metaverses are critically examined against the backdrop of cyberspace as place, psychology of the constructed persona, and violations of trust online. These examples are then discussed with reference to current criminological theory and relevant Canadian and American legislation

Keywords: cyber-stalking, cyber-bullying, cyber-rape, cyber-assault, online victimization, Internet violence, victims, perpetrators

For Granny Evelyn Fingarson, who always saw the bright side and for whom the words "this cannot be done" were meaningless.
You taught me well.

Acknowledgements

In my attempt to “capture Niagara Falls in a test tube” I am immensely grateful to my supervisors, Dr. Brian Burtch and Dr. Sara Smyth for guiding me from a loose collection of thoughts and ideas to a more coherent, structured, and forceful argument. I would also like to thank my external examiner, Dr. Gregor Urbas, for asking the hard questions, and Yolanda Koscielski, Liason Librarian (Criminology, Computing Science, and Engineering Science) for her unflagging willingness to help me find the answers to my obscure and sometimes incomprehensible research questions.

This thesis was supported by research funding from the Canadian Federal Government through the Social Sciences and Research Council (SSHRC) and an entrance scholarship from the Modelling of Complex Social Systems (MoCSSy) at Simon Fraser University.

Most importantly, I am thankful for the blessings of my husband, Michael, and our children, Lawrence and Grant, and all the friends and colleagues who gave me the space and time to gather my thoughts and unending encouragement when the task seemed too daunting to complete.

Table of Contents

Glossary

Advanced Research Project Agency (ARPA): A government agency formed in the 1950s, initially responsible for space defense, global surveillance and later, a broad-based mandate of research and development (Hafner & Lyon, 1996).

AT FULL FORCE: Used by griefing groups as a public announcement asking all available individuals to join in an online attack of an "identified enemy". Taken from traditional military language commonly used by police, firefighters, and others to indicate that individuals are to fight to the best of their ability. Always posted in capital letters to capture attention (The Free Dictionary, 2012).

Avatar: An "incarnation, embodiment, or manifestation of a person or idea; a movable icon representing a person in cyberspace or virtual reality graphics" (Oxford, 2004) that is placed and manipulated in online role-playing games such as World of Warcraft and adjunct lives/metaverses such as Second Life (Blascovich & Bailenson, 2011).

Clickwrap agreement: An agreement between player and company hosting the game that the player must click "I accept" to be permitted to play. Clickwrap agreements spell out terms of service and acceptable use policies as well as any other pertinent rules or conditions (Tseng, 2012).

Denial of service attack: Caused through a deliberate attempt, by attackers, to prevent users from accessing a network by flooding it with more electronic requests than it can handle (Software Engineering Institute of Carnegie Mellon, 2001).

Distributed denial of service attack (DDOS): A concerted effort by a large number of disruptors (either a large number of individuals or single/few individuals using automated computer programs) that seeks to interrupt the normal function of a targeted computer network with the goal of rendering it unavailable to legitimate users. A DDOS is achieved by flooding the target with requests for information that prevent legitimate users from accessing the target or by impeding the speed with which the target can respond to legitimate requests (WhatIsMyIPAddress.com, 2000-2012).

Doppelgänger: Any double or look-alike of a person (Bailenson &

	Segovia, 2010).
End user license agreement (EULA):	The contract between licensor and purchaser/ user, establishing the purchaser or user's right to use the software. In games and metaverses the EULA can also include rules for entering and participating in the virtual space (Castronova, 2004).
EVE Online:	A highly intricate, online immersive game set in outer space in which players can take on any role they wish in pursuit of money, fame, and adventure. EVE has an in-game market, money exchange, and educational facilities in which to learn trades and skills (EVE faq, 2012).
EverQuest II:	A massively multiplayer, persistent game set in a fantastical world. According to the website description, it is "the ultimate blend of deep features, heritage, and community." Its estimated U.S. subscription basis is 150,000 players (EverQuest II Homepage, 2012).
Facebook:	A social networking site, founded in 2004. Its stated mission is "to make the world more open and connected. People use Facebook to stay connected with friends and family, to discover what's going on in the world, and to share and express what matters to them" (Facebook, Key Fact, About, 2012).
Flaming:	The uninhibited expression of strong, inflammatory opinion, communicated via computer-mediated communication (Moor, Heuvelman, Verleur, 2010). Flaming uses inappropriately expressed criticism when communicating with others on message boards or other open access sites such as YouTube. This criticism is often in the form of personal attacks rather than criticism of the topic (Forsyth, 2006; Urban Dictionary, 2012).
Folkways:	Commonly accepted practices in emerging societies that become accepted and followed by all who belong (Griffiths, 2007).
Gauntlet:	One of the first fantasy-themed, multi-player games. Not considered particularly sophisticated as it relied on simple attack and killing to progress through levels. Based on the Atari arcade game from the 1980s. Gauntlet is no longer available for online play (Wikipedia, 2012).
Google bombing:	The attempt to manipulate the Google search

	engine by exploiting its page-rank algorithm to ensure specific posts/sites emerge in the top search results. This is accomplished by posting multiple threads, linked to a consistent anchor text, on message boards or similarly functioning websites, providing the appearance of high levels of activity and importance which, in turn, raises its ranking in Google's search results (Margolick, 2009; Ogles, 2004).
Griefers:	Players or other individuals in online environments whose aim is to destroy others' enjoyment of the game, social network or metaverse for their own amusement (Dibbell, 2008).
Griefing:	A deliberate and willful antisocial behavior perpetrated by individuals or groups in immersive games and metaverses. Aimed at destroying others' enjoyment of the game for their own amusement, griefers will disrupt play by violating fair rules of combat, or by stealing, looting, and destroying others' equipment and avatars. Griefing was first thought of as an annoyance caused by immature players; however, more recently it is thought to consist of organized group attacks as well as ponzi schemes, organized theft rings, and bait and cheat tactics (Adrian, 2010; Dibbell, 2008; Lin & Sun, 2005).
Guilds:	Online groups, formed within massive multi-player online role-playing games, with a hierarchical leadership structure that allows players to act as a unified group to solve joint missions. Some guilds are less formal; however many are well-organized, coordinated teams with established design goals and missions (Yee et al., 2007).
Immersive online games:	Three-dimensional (3D) computer games, set in perpetual worlds, that give the player a feeling of entering game space and losing themselves into the world of the game (Jennett et al., 2008).
IP Address:	The Internet protocol address that uniquely identifies a computer on the Internet. This number facilitates communications between a computer and the rest of the Internet (whatsmyip, nd).
Kaneva:	A social networking-metaverse blend that links the physical self to virtual representation through photos, allowing for identification of the self by location and activities in geographic space in real time (Kaneva, About, 2012).

Linden Lab:	The maker and developer of Second Life (Mann, 2008).
LinkedIn:	A business-oriented social networking site with over 150 million users. The purpose of the site is to "Stay informed about your contacts and industry. Find people & knowledge you need to achieve your goals. To control your professional identity online" (LinkedIn, Homepage, 2012).
Lulz:	Initially a plural variant of lol (laugh out loud), lulz is now commonly used as a noun meaning that something was interesting or funny on the Internet. Considered the one good reason to do anything online from trolling to cyber-rape and often used as the reason for committing an online raid or invasion (Urban Dictionary, 2012).
Magic circle:	A boundary drawn between game space and non-game space in an online game. The magic circle has three functions: to protect the virtual play; to protect stories and speech; and to protect the level playing field of a game by separating fantastical play spaces from spaces that are an extension and augmentation of physical world life (Castronova, 2004-2005).
Massively multiplayer online role playing games (MMORPG) aka MMOG (Massively multiplayer online game):	Online, immersive games, usually set in a virtual world with large numbers of players (often in the thousands or hundreds of thousands) (Jennett et al., 2008).
Metaverse:	A term created and defined by Neal Stephenson in 1992, describing a unified avatar-mediated virtual context that reflects the physical world, where individuals interact in three-dimensional (3D) space (Stephenson, 1992).
MOO (MUD, object oriented):	A text-based, multi-user, real-time virtual world that uses object-oriented techniques to organize the objects in the database. This allows the creation of new objects by the players (Dibbell, 1993).
Mores:	Morals or official rules that, when broken, violate rights and cause social injury (Griffiths, 2007).
MUD (Multi-user Dungeon/Domain):	A text-based, multi-user, real-time virtual world (Dibbell, 1993).
MySpace:	A social networking and entertainment website. MySpace provides a platform for social interaction by connecting people to friends, music, celebrities, TV, movies, and games via computer, cellular

	phone, and offline events (MySpace, About Us, 2012).
Newbie:	An individual who is new to the Internet or online game (Barber, 2004).
Occupy Wall Street:	A protest that began September 17, 2011 in Zuccotti Park, in New York City's Wall Street financial district. Initiated online by the Canadian activist group, Adbusters, this movement led to Occupy protests and movements around the world and in cyberspace. Protest was over social and economic inequality, greed, corruption and the undue influence of corporations (predominantly financial) on government (Adbusters, 2011).
Patriotic Nigras:	Formed in 2006 expressly for the purpose of organized griefing and trolling in Second Life and more specifically to target the "furfags" (individuals who like to dress up their avatars as furry creatures and have virtual sex with other furry avatars). The goal of this group is to make fun of others and harass them until they quit playing the game or metaverse out of frustration. Their amusement is others' fear, anger, and rage caused by the mayhem they produce which ruins the immersive, metaverse experience for other users (Bakioglu, 2009; Dibbell, 2008).
Posttraumatic stress disorder (PTSD):	An anxiety disorder that generally develops subsequent to a life-threatening or traumatic stressor. Those suffering will often re-experience the event as a strong memory or flashback, resulting in a range of symptoms including fear, helplessness, horror, and disorganized or agitated behavior. Those suffering from PTSD will often avoid any stimuli that may trigger a flashback. Impairment in social functioning is common (APA, 2000).
Second Life:	An online, virtual world developed and produced by Linden Lab. According to the company's description, "Second Life is a place to connect, a place to shop, a place to work, a place to love…explore…be different…be yourself…free yourself…free your mind…change your look, love your look, love your life." It was launched in 2003 and currently has approximately 1 million active users. It is intended for those over the age of 16 and allows for both free and paid members (Second Life *FAQ*, 2012).

Sims Online:	Is an online, interactive, virtual world in which players control the life of one person and work to earn money to progress through levels (Martey & Stromer-Galley, 2007).
Social networks:	Online communities formed of individuals who share common interests and use the website or other technologies to communicate with one other. A social network may be solely social (e.g. Facebook) or may be business-oriented (e.g. LinkedIn) (Facebook, About, 2012; LinkedIn Homepage, 2012; MySpace About Us, 2012).
SOPA (Stop Online Piracy Act):	A protest against two pieces of proposed legislation (United States, Bill/H.R. 3261 and Canada's, Bill C-11, Copyright Modernization Act) aimed at curbing access to overseas websites that traffic in pirated content and counterfeit products such as movies and music. These bills were effectively stopped by online protests, led by technology companies and individuals concerned about limits being placed on their Internet freedoms. Protestors claimed that the bills would undermine freedom, be difficult to prosecute, and would cost companies and individuals billions of dollars per year (Melvin, 2012).
Star Wars Galaxies:	A massively multi-player, online, role-playing game based on the popular Star Wars trilogy, developed by Sony for LucasArts (Star Wars Galaxies, Homepage, 2012).
Subprogram (aka subroutine):	A function, sub-routine, or other part of the source code within a larger computer program. Its purpose is to perform a specific task related to the rest of the code (Barber, 2004).
TCP/IP (The Internet Protocol/Internet Protocol):	A standardized system allowing for a global network of interconnected systems (Hafner & Lyon, 1996).
Terms of Service (ToS):	In metaverses, social networks, or immersive games, an agreement that spells out appropriate use and unacceptable content guidelines (Tseng, 2011).
Toading:	In a virtual reality, role-playing game or multi-user domain, to be ejected, deleted, or killed (Urban Dictionary Online, 2007). In other communities it means that all identifying characteristics of the character are deleted and replaced with those of a slimy amphibian (Dibbell, 1993).

Twitter:	A social network that provides a platform that is a "real-time information network that connects you to the latest stories, ideas, opinion and news about what you find interesting" (Twitter, About, 2012).
Virtual world:	Internet-connected, shared, persistent, open-ended, three-dimensional (3D) spaces.
WELL (Whole Earth 'Lectronic Link):	A "computer conferencing system that enables people around the world to carry on public conversations and exchange private electronic mail (e-mail)" (Rheingold, 2000, p. xv).
White-eyed players:	The same as griefers (players or other individuals in online environments, whose aim is to destroy others' enjoyment of the game, social network or metaverse for their own enjoyment) but thought to be younger players who do not know better (Lin & Sun, 2005).
Wizard:	An individual who maintains social and technical control of the online community or game. They are usually capable of rewriting the software that underlies the MUD to eliminate commands that chronically lead to objectionable behavior, filter out objectionable behaviors through gag commands, temporarily restrict the rights of those who transgress within the community, shame and humiliate transgressors in public rituals, banish transgressors from the community, both permanently and temporarily, as well as register identities and lead regulatory committees (Dibbell, 2008).
World of Warcraft:	A massively, multi-player, online, role-playing game (MMORPG) produced by Blizzard Entertainment. According to the company's description, "World of Warcraft is an online game where players assume the roles of heroic fantasy characters and explore a virtual world full of mystery, magic, and endless adventure." Blizzard reported 10.3 million active subscribers as at September 2011 (Blizzard Entertainment, World of Warcraft home page, 2012).

1. Introduction

Social networks, three-dimensional (3D) immersive games, and metaverse virtual worlds are significantly changing the social lives of millions of North Americans in a manner similar to the way the Internet changed users' lives in the late twentieth-century (Smart, Cascio, & Paffendorf, 2008). Virtual social spaces provide platforms for individuals to participate in pro-social activities such as the exchange of ideas, information, and emotion; to provide social support; to create and share artistic media, such as movies and songs; as well as collaborate for business, education, and pleasure (Bainbridge, 2010a). There is, however, a dark side to social media. These spaces contain anti-social and violent aspects of human behaviour, including stalking, harassment, bullying, griefing rape, and assault. Given the number of reported cases of online acts of violent victimization (e.g., Chisholm, 2006 and Reyns, Henson, & Fisher, 2011) it is likely that our courts will adjudicate these matters in the near future.

When society and law encounter unanticipated new technologies that radically change the habits and behaviours of people, the reliance on analogical reasoning plays a profoundly important role (Blavin, 2002). This is because, in Canada, we look to past court decisions for the application of reasoning, precedent, and legislation to inform current legal questions (Verdun-Jones, 2007). Court decisions, resulting in real damages assigned to real humans, based on the actions of avatars, forces all of us to grapple with the notion that there is a code of conduct which varies between legal and illegal, acceptable and unacceptable, even in virtual worlds. In Canada, crime consists of two major elements: conduct that is prohibited because it is "evil or injurious or undesirable [in its] effect upon the public" (Justice Rand, *Margarine Reference* case, (1949)); and a penalty that may be imposed when the prohibition is violated (*Canadian Criminal Code*). Over the past 20 years, our courts have struggled to conceptualize the meaning of acts that occur on the Internet, to apply existing criminal and civil legislation, and to create new legislation to regulate behaviors related to issues such as virtual property ownership (Blavin, 2002), cross-jurisdictional movement of information

(Goldsmith & Wu, 2006), and the creation and distribution of illegal imagery such as child pornography (Joyce, 2008). It is therefore expected that they will similarly struggle to conceptualize and legislate acts of virtual violence.

While there are a number of scholarly articles which separately discuss online bullying, stalking, harassment, and even rape there is no known (to this author) compilation of the information provided, nor has there been an attempt to organize the information in a coherent manner that will provide a foundation from which to apply existing legislation, suggest new laws, and apply current criminological and psychological theories to these acts of virtual violence. Given the expected increase in future usage of virtual social spaces and the manner in which they will increasingly link to our physical lives (e.g., Kaneva), blurring the boundaries between what is "real" and what is "virtual", this thesis provides a much needed summary, exploration, and discussion of a topic which is certain to become more significant in future.

1.1. Structure of Thesis

The purpose of this thesis is to explore virtual violent victimization as real crime with negative consequence for those who are victimized in the online social spaces of metaverses, immersive games, and social networks. Chapter one provides the methodologies used to collect and analyze the information and the history of networked communication and its current manifestation in the 21st century, as an indispensible communication tool and community for millions of North Americans. Chapter two examines the meaning of social cyber-places through metaphor and cognitive perception, the meaning of the constructed self we place there through the relationships these selves form with others, and the meaning and significance these relationships hold for the creator. Chapter three examines trust through its functions and principles in physical space, how this transfers to online social spaces, and violations and impediments to trust that occur there. Chapter four reviews virtual violent victimization, specifically rape, harassment, stalking, intimidation, and violent assault, and applies current Canadian and American legislation to example cases. Chapter five applies current criminological theories to the violent acts explored in chapter four, including the psychological theory of disinhibitory effects, social control theory, and routine activity

theory followed by a discussion offering recommendations for legislative changes and the introduction of new legislation followed by conclusions.

1.2. Methodology

Despite the nascent quality of online social spaces, especially 3D immersive games and metaverses and the research on them, there are several reasons to conduct this study. First, there is a growing body of peer-reviewed research available; second, this thesis provides a highlight and examination of current findings; and third, it identifies the phenomenon, its current meaning, inconsistencies and contradictions in how it is perceived by scholarly writers, and applies existing legislation in a manner which may help to inform and provide direction for future research. As such, this is an opportunity to assess the emergence of media-related phenomenon through existing legislation and criminological and psychological theory.

Collecting the scholarly articles with which to conduct the literature review was a challenge given the lack of research specifically related to cyber-violence as well as the lack of consistent terminology and assigned meaning. Several search platforms, accessed via Simon Fraser University's online library, were used to retrieve peer-reviewed papers including Academic Search Premiere, Business Source Complete, Criminal Justice Abstracts with Full Text, EbscoHost, GoogleScholar, HeinOnline, IEEE Online, LexisNexis, JStor, Legal Affairs Online, ProQuest, Sage Social Sciences, ScienceDirect, SpringerLink, and Wiley Online. Government reports were accessed from Canadian and American government websites such as the departments of justice. Criminal cases in Canada were searched through CriminalSource using the words "Internet", "cyber-space", "social networks", "metaverses", "virtual worlds" and "immersive/computer/online games" in combination with the relevant Canadian *Criminal Code* sections for rape, harassment, and assault. American cases were searched through LexisNexis. Numerous scholarly texts and e-texts were read on the philosophy of the Internet, the meaning of virtual communities, behavior on the Internet, the constructed self, and legislation aimed at controlling criminal conduct and civil misconduct online.

The history of the Internet was searched via the keywords, "Internet history" and "Internet timeline". The topic of trust was searched via the keywords, "trust", "virtual

trust", "Internet trust", "e-trust", and "cyber-trust". Violence was searched via the keywords, "Internet intimidation", "Internet violence", "Internet rape", "Internet bullying", "Internet stalking", "Internet harassment", "cyber-violence", "cyber-rape", "cyber-bullying", "cyber-intimidation", "cyber-stalking", "cyber-harassment", "cyber-violence", "avatar violence," "avatar rape", "avatar bullying", "avatar stalking", "avatar harassment", "virtual violence", "virtual rape", "virtual bullying", "virtual stalking", "virtual harassment" and "tiny violence". The specific cyberspaces were searched via the keywords, "metaverse", "immersive world", "virtual world", "massively multiplayer online role-playing game (MMORPG)", "massively multiplayer online game (MMOG)", "multi-user dungeon/domain" (MUD)", and "social network".

Searching widely, hundreds of articles and texts were read in addition to explorations of the websites Second Life, Facebook, Kaneva, and numerous hours viewing YouTube videos and documentaries. Material related to topics of interest was noted, interpreted, collated, organized, and summarized resulting in the work here.

The following section examines the advent of Internet communications and how it has come to be an indispensible extension of our physical lives in the twenty-first century.

1.3. History of Networked Communications

Despite knowing that cyberspace was a computer-mediated communications web, Rheingold (2000), an early critic and Internet philosopher, highlighted its community-like aspects: "Not only do I inhabit my virtual communities; to the degree that I carry around their conversations in my head and begin to mix it up with them in real life, my virtual communities also inhabit my life. I've been colonized; my sense of family at the most fundamental level has been virtualized" (Rheingold, 2000 p. xxv). Arguments raged over whether the Internet was its own place, subject to values, rules, and laws that would naturally emerge or whether it was nothing more than an extension of physical space (Barlow, 1996; Johnson & Post, 1996). Over time we have come to understand that it is both its own place *and* an extension and expansion of our physical world. The following section provides a brief history of this social medium.

Three individuals, working independently and unknown to one other conceived a global network of computers. Leonard Kleinrock, Paul Baran, and Donald Davies focused on a revolutionary theory of communications that would avoid total destruction in the case of a nuclear attack (Hafner & Lyon, 1996). ARPANet, the predecessor of the Internet, through a system of linked interface message processors (IMPs – computers that interconnected the network, broke messages into packets of data, sent and received the packets, checked for errors, and routed the data packets) was launched in 1969 with 4 nodes: UCLA, Stanford Research Institute, University of California Santa Barbara, and the University of Utah (Hafner & Lyon, 1996, p. 10). The concept of a shared "world brain", which would allow information to be transmitted instantly, globally, and in a common language, had long been envisioned by men of creativity and science (e.g. H.G. Wells' essays in *World Brain* as reviewed in Burrows, 1999). The actual system, which has become the Internet, was the result of "a synergistic surge of technology, engineered by…researchers and developers amidst a defining period of challenge, creativity, invention, and impact" (Kleinrock, 2010, p 26).

In the late 1950s, Kleinrock's graduate thesis examined the interaction of behavior between computers, users, data, and nodes (Kleinrock, 2010). Simultaneously, Baran (RAND Corporation), was working on a similar network for military application (1964), and Davies, (National Physical Laboratory, United Kingdom), was working on packet networks for public use (1966) (Kleinrock, 2002; Kleinrock, 2010; Zakon, 2010). Packet-switching, the foundation of message flow on the Internet, is a system whereby information is broken down into small, separate packets, each taking the most expedient route to its destination, hop scotching through a network of intermediate pathways and then reassembling, in the proper sequence, at the destination (Copeland, 2000). A system using packet-switching can transfer large quantities of information via communication networks and avoid limitations that existed in the telephone system of the 1950s: centralized sources, making them vulnerable to attack; degradation of signal quality as links increased, making them limited for user capacity; and slow, dedicated switching, disallowing multiple users and underutilizing resources (Kleinrock, 2002; Kleinrock, 2010).

During the same time period, the cold war with Russia was intensifying and there was high-level military concern over a nuclear war. The limitations of the telephone system would be critical if America were to sustain a nuclear attack (Hafner & Lyon,

1996, p. 50 – 65; Kleinrock, 2010). This new communications system had to be highly functional and efficient, with a single priority – to transfer information reliably from source to destination even if parts were blocked, damaged or destroyed (Goldsmith & Wu, 2006; Hafner & Lyon, 1996, p. 79).

Under the direction of the Advanced Research Project Agency (ARPA), the research of Kleinrock, Davies, and Baran was brought together during a series of discussions focused on designs for a new communications network referred to as the ARPANet (Hafner & Lyon, 1996; Zakon, 2010). As a result of these meetings and with the financial support of ARPA, a commitment to go forward and build the ARPANet was made (Kleinrock, 2010).

The ARPANet grew rapidly between its inception and the mid 1970's. Subsequent changes led to the adoption of a standard set of protocols and language, (the Internet Protocol/IP), as well as providing a unique number identifying each individual computer attached (IP address) (Goldsmith & Wu, 2006). Email became a common method of communications between users (Hafner & Lyon, 1996; Zakon, 2010) and the term *Internet* was used to describe the system (Gribbon, 2011). Further technological changes occurred in the 1980s including: the introduction of Internet protocol suite routers to replace IMPs, the graphical user interface, the hypertext transfer protocol, and dial-up access for public use (Gribbon, 2011). In the 1990s, the National Science Foundation Network was decommissioned, opening up the Internet to commercial users (Gribbon, 2011). Companies such Amazon went online, Hotmail was launched, the Google search engine appeared, and in 2004, Facebook, the first social networking space, was created (Gribbon, 2011). The modern Internet, with its plethora of social networks, is thus a direct descendent of the original ARPANet, but a vastly different space with its 3D virtual worlds and increasing focus on entertainment and social connection (Smart et al., 2008).

2. Perception of Place and Self in Cyberspace

The 30 years between the creation of the Internet and its widespread use focused on military and academic applications and the development and construction of a physical structure that could support a world wide web (Kleinrock, 2010; Zakos, 2010). Little thought was put into the social implications of such a media and, thus, the use of the Internet began with a sense of wide-eyed naiveté focused on building communities in this new, virtual place.

2.1. Metaphorical Perception of Place

Rheingold (2000) referred to cyberspace as a "place" from the outset; he spoke of virtual communities with their fast-growing populations as locations he could physically visit: "I was *in* the Parenting conference on the WELL...I was *in* MicroMUSE, a role-playing fantasy game...I was *in* TWICS, a bicultural community" (Rheingold, 2000, pp. xv-xxv, emphasis added). Rheingold claimed that communities naturally emerge in cyberspace and were like the *agora* or central marketplace of ancient Athens where citizens could go to discuss and exchange ideas (Rheingold, 2000, p. 50). He exhorted others to think in terms of architecture to hasten their familiarity with this new place, "An architectural model of the WELL (Whole Earth 'Lectronic Link) can help you create a mental model of these spaces within spaces. If you think of the WELL as a building, you can walk down the halls and look at the signs on the doors to different rooms" (Rheingold, 2000, p. 51). Other critics and philosophers tacitly seemed to accept this naturally emergent society view of the Internet. Johnson and Post (1996) stated that these very qualities in cyberspace – the emergence of communities and villages similar to those that formed in physical space – would inform the norms, including folkways and mores, but not the laws (Johnson & Post, 1996). Cyberspace was not the same as our physical world, consisting of only the mind, and therefore could not be governed by the laws of earth.

The term *cyberspace* came from the name given to a global computer interface, similar to the Internet, by William Gibson in his 1984 cyber punk novel, *Neuromancer.* Cyberspace was "the consensual hallucination…experienced daily by billions of legitimate operators, in every nation...in the nonspace of the mind, clusters and constellations of data" (Gibson, 1984, p. 5/51). This definition worked well for the designers and early users because it reflected both their desire for human-computer symbiosis (Kleinrock, 2010) and their experience of connected data transfer in this new medium (Kollock & Smith, 1999).

As a "consensual hallucination", the Internet was perceived as full of communities and activities where individuals or groups could interact with one another exchanging ideas, information, emotions, property, money, social support, and even coordinate protests (such as the protests against the Stop Online Piracy Act (SOPA) in the United States and the Copyright Modernization Act (Bill C-11) in Canada, as well as the Occupy Wall Street movement) (Cohen, 2007; Zekos, 2005). It was a site to share and transfer so much of what humans perceived as real and valuable (Hunter, 2003; Lemley, 2003). Unfortunately, it quickly became a place where humans could also transfer their hatred, bigotry, and violence (Franks, 2011; Kennedy, 2009).

The metaphor of cyber places works well for human perception and cognition given that metaphor is crucial to language and so central to human thinking that we would be unable to speak or make ourselves understood to others without its use (Richards, 1936). Cyberspace, initially a text-based, language-filled medium, lent itself well to metaphorical description. Metaphor is central to human cognition which is always a function of social action, thus, given that cognitive activities were being increasingly conducted via networked communications, the continued exchange resulted in a "shared construction of reality at the interface between individual and collective, cognition and interaction, mental activity and social activity" (Saito, 1996 as cited in Riva & Galimberti, 1998, p. 144). Using metaphor allowed individuals to highlight the similarity between cyberspace and physical space, creating a strong link between the physical and the virtual (Cohen, 2007).

Metaphor was also widely used in early court decisions regarding events that occurred solely in cyberspace, significantly influencing how it began to be regulated:

"Thinking of cyberspace as a place has led judges, legislators, and legal scholars to apply physical assumptions about property in this new, abstract space" (Hunter, 2003,

p. 443). Using the "cyberspace as place" metaphor permitted the application of traditional laws, for court decisions in cases like *eBay v. Bidder's Edge* (2000), *Register.com v. Verio* (2009), and *Intel Corp. v. Hamidi* (1999/2001/2003) (Lemley, 2003). Courts not only applied the cyberspace as place metaphor, but also concluded that cyberspace *was* a place as indicated by their use of long-established real-world principles (Lemley, 2003).

Using the cyberspace as place metaphor and applying traditional property laws in early court decisions gave individuals the right to private ownership of virtual places which, in turn, granted them the right to defend their border and exclude individuals or groups from entering those places (Lemley, 2003). The application of borders in cyberspace directly counters the ideals that many early Internet philosophers held for the free movement of information in a commons-like space (Johnson & Post, 1996). Court decisions that support private ownership for online places have the potential of being used as precedent in cases of virtual violent victimization if the virtual self is perceived to be the same as virtual property. It is possible that courts may decide the same exclusionary rights should be extended to online creations of the self in the same manner that they extended them to online places. This could result in the formation of a type of restraining order for use in cyberspace similar to restraining orders used in physical spaces. Restraining orders are legal injunctions that order individuals or groups to do or refrain from doing something. If a restraining order is violated, the individual(s) named in the order can then be held legally liable and subject to civil and/or criminal penalties (Ministry of the Attorney General, Ontario, 2009). The development of this type of legislation would provide strong legal recourse for victims of violent online attack against those who would victimize them.

2.2. Cognitive Perception

Numerous studies in computer-mediated communications, with and without avatar presence, have determined that individuals are highly influenced by what they experience in cyberspace (Blascovich & Bailenson, 2011). Magnetic resonance imaging studies show the same part of the brain is active when being ostracized in online games as when experiencing physical pain (Blascovich & Bailenson, 2011). Avatars also socially influence individuals. Following their lead in games, humans make attributions

of sentience to the avatar, regardless of whether they know it is computer generated and controlled or human controlled (Blascovich & Bailenson, 2011). This evidence establishes that, at least during the moments the person is interacting with the avatar, it is perceived in a similar manner to the way we perceive human beings in real space.

Other experimental studies have "revealed significant differences in user perceptions of the degree of social presence/media richness in email and video-conference, compared with other means of communication like the telephone and written text" (Riva & Galimberti, 1998, p. 149). We imbue communications in cyberspace with a tangible quality that exceeds even telephone conversations where we are certain that we are speaking, in real time, with another person based on the timing and rhythm of the conversation and levels of dynamic interchange. Given asynchronous communication, and the possibility of auto-response texts and emails, a human in real time is not something we can easily confirm in some of our communications in cyberspace. The personal computer allows for the cognitive perception that what is present on the screen is real and currently active in the life of the person viewing it; this increases the sense of being in the same place and time as what is being viewed (Riva & Galimberti, 1998). Accordingly, "If embodied, experienced spatiality is hardwired, 'cyberspace' too is embodied, experienced space; it cannot help but be" (Cohen, 2007, p. 229). Clearly, cognitive science provides ample evidence that, "we do think of cyberspace as a place" (Hunter, 2003, p. 443).

The historical decisions by courts to view cyberspace metaphorically and cognitively equivalent to physical space, in determining meaning and application of property law, will no doubt have repercussions for the application of criminal law, related to violent victimization, when these cases begin to move through our courts. Further, allowing for a shared community definition of cyberspace indicates that the application of norms and standards, related to communities, may be legally considered when courts are asked to adjudicate in these matters. This allows for online violent acts to hold significance similar to their historical significance in physical space and should lead courts to apply current legislation in attempt to address wrongs.

The following sections examine the specific nature of online social spaces with particular focus on the qualities of place and community.

2.3. The Metaverse

Virtual worlds are Internet-connected, shared, persistent, open-ended, 3D spaces (Boellstorff, 2008; Smart et al., 2008). The metaverse, a special type of virtual world, embodies the fusion of a virtually enhanced physical reality with a physically persistent virtual space (Smart et al. 2008). Metaverses are virtual communities in which global participants interact continuously in social, economic, and cultural explorations, sharing ideas and concepts through the establishment of relationships and community activities (Carthage, 2009; Davidson, 2008; Smart et al., 2008). Metaverses, while linked to the physical world through the action of the participant, are places in their own right (Boellstorff, 2008).

The metaverse concept is credited to Neal Stephenson, based on his description of a virtual world in his novel, *Snow Crash* (1992). Stephenson (1992) described a dystopian society, inhabited by 120 million avatars, participating in social, economic, and personal entertainment (Boellstorff, 2008). Metaverses today, rather than the dystopian image provided by Stephenson (1992), are considered more utopian and act as online, immersive, collaborative, information, and social spaces that support the presence of multiple individuals (Lombardi & Lombardi, 2010). Real-life people construct 3D animated representations in the form of agents or avatars and place them in these virtual communities (Smart et al., 2008). These avatars may more or less resemble the participant's physical-world self in appearance and personality as individuals choose to either use the metaverse for escapism and carve out new identities, or to provide support mechanisms for their physical world self (Turkle, 2005). Metaverses combine verisimilitude and limited fantasy in the forms of self-invention and reinvention (Turkle, 1994). Yet, regardless of the fantasy/magic elements of metaverses, these worlds have come to be seen as a significant mode of technology-mediated communication and source of important social interaction (Boellstorff, 2008).

Using client-server architecture, each participant's computer is in continual conversation with the metaverse's server (Lombardi & Lombardi, 2010). As the participant inputs commands for movement or action via keyboard or mouse, the avatar responds, alerting the servers, which in turn, interpret intentions, establish a state for the simulation, and replicate information about the state of that simulation multiple times across all machines participating in that simulation (Lombardi & Lombardi, 2010).

Current metaverses include Active Worlds[1] (two-plus million members), There[2] (two million members), Kaneva[3] (five million members) and Second Life[4] (23 million registered avatars).[5] Second Life, There, and Active Worlds have been solely populated and filled with virtual objects by the users who, in utilizing the provided software tools, construct a wide assortment of avatars, buildings, personal accouterments, and play spaces (Davidson, 2008*).* Kaneva is unique, blurring the lines between social networks and metaverses by encouraging members to create avatars based on their own physical appearance (Robinson, 2012, Kaneva home page, 2012).

The opportunity for individuals to work collaboratively, creating and modifying not only the space they occupy but also the objects within that space, represents a leap forward in social interaction (Lombardi & Lombardi, 2010). Interaction with others' avatars and artefacts produces the effect of a shared mental space making tangible the space in which individuals meet, communicate, share information, and play with one another (Barbatsis, Fegan, & Hansen, 2006). All this interactivity has resulted in vast commercial activity whereby participants make available the created objects to share, sell or trade within these worlds (Lombardi & Lombardi, 2010).

Established companies are flocking to metaverses. IBM is now firmly situated within Second Life and sees the metaverse as a valuable location for business, education, knowledge enablement, collaboration, and fun (Carthage, 2009). The New York Stock Exchange (NYSE) has built an interactive 3D trading floor, called 3DTF, as a real-time decision support tool for its operators (Hunter, 2003). Given that metaverses are "increasingly…mediated by large commercial entities similar to those that mediate

[1] *Active Worlds* taken from: http://www.activeworlds.com/info/index.asp;

[2] *There* taken from http://www.prod.there.com/info/company;

[3] *Kaneva* taken from and http://en.wikipedia.org/wiki/Kaneva

[4] *Second Life* taken from http://community.secondlife.com/t5/Everything-Else/How-many-members-are-there/qaq-p/885369. *Second Life* claims that number of avatars, however most are inactive with somewhere between 1 and 2 million active during any month and approximately 50,000 active at any specific time.

[5] Population statistics taken from information gathered from the corporations that own the metaverses (except *Kaneva, which* does not provide this information. Information for *Kaneva* was taken from Wikipedia).

interactions in real space" the bond between our offline and online lives is strengthened (Cohen, 2007, p. 218). The ability to enter the virtual establishment of Adidas or American Apparel, try on clothes, order, and pay with either metaverse or physical world dollars, then receive the product in the physical world blends the two worlds, blurring boundaries between what is real and what is virtual (Davidson, 2008).

As predicted by William J. Mitchell in *City of Bits: Space, Place, and the Infobahn*:

> cyberspace places will present themselves in increasingly multi-sensory and engaging ways. They will look, sound, and feel more realistic, they will enable richer self-representations of their users, they will respond to user actions in real time and in complex ways, and they will be increasingly elaborate and artfully designed. We will not just look *at* them; we will feel present *in* them (1996, p. 114-115, emphasis in original)

3D spaces present in worlds such as Second Life have become much more realistic compared to the earlier renditions (Smart et al., 2008). According to media richness theory, as media environments become richer, personal focus parameters increase making the space the individual is immersed in more personally meaningful (Bailenson & Segovia, 2010).

Clients of metaverses are encouraged to view these worlds as real with communities, neighbourhoods, and locations described in map-based, spatial terms. In the orientation video for newcomers to Second Life, Linden Lab (2012) claims a cartographical quality to their metaverse, "a huge map gives users a sense of just how big Second Life is." Yet, Second Life takes up no space as it is comprised of nothing but data. This does not, however, stop property development from being a highly lucrative business with one developer, Anshe Chung, earning more than one million U.S. dollars for property development and sales in 2006 (Hof, 2006) and the virtual city of Amsterdam selling for U.S. $50,000 in 2007 (Kane, 2009). The exchange of property and money in metaverses heightens the effect that, while the metaverse may be a different place, it is an adjunct to physical living where transactions of real meaning occur.

Given our tendency to experience cyberspace as a real and meaningful space in its own right, the addition of media-rich metaverses has had the effect of blurring

boundaries, which further intensifies the effect of reality. This results in even greater meaning for those who participate in them. The shared, persistent imagery combined with enhanced physical reality that leads to social and commercial interactions renders the metaverse a social, economic and cultural exploration of meaning and effect.

2.4. The Immersive Role Playing Game

There are many similarities between metaverses and online, massively multiplayer, immersive, role-playing games: persistent worlds, avatars, naturalistic settings, property that can be created, bought and sold, spatial orientation, cartographical metaphor for distance, routes, and direction, as well as commerce, education, and social interaction (Kane, 2009; Yee, 2006; Yee, 2010). Though both were designed to facilitate and enhance social interaction, games differ significantly from metaverses as they are predominantly task-oriented and quest-based. Games are also set in fantastical worlds where individuals form guilds to achieve the tasks and quests that lead to the amassing of wealth, power, and potentially allow players to win against other players in the game (Yee, 2006; Yee, 2010). In metaverses there may be collaborative tasks, such as the construction of buildings or objects; however there are few, if any, quests and no sense of competition with clear winners and losers (though normal competition for business, customers, etc. is as much a part of the metaverse as it is in the physical world).

The fantastical aspects of game space, combined with guild-based quests and tasks, while still holding meaning for those playing, does underscore the play aspect of these places. This is significantly different from metaverses that act as extensions and expansions of our day-to-day life. The differences between these two online social spaces is critical for any potential legislation and must be recognized to ensure we preserve play spaces as free from the normal standards of behaviour and legislation. This is because games are often highly violent, supporting the type of behaviours that in the physical world or metaverses would be considered not only anti-social but possibly criminal.

Immersive games are physically supported in a manner similar to metaverses with multiple servers creating single worlds and each server responsible for a specific sub-section of the terrain with player commands causing avatars to move and interact

(Gratch & Kelly, 2009). Games are similar to metaverses in that the worlds are persistent and the players participate on the Internet, accessing them via personal computer, game consoles, and mobile devices (Krikke, 2003). The ability to enter games and metaverses via mobile devices embeds these online social places into physical world lives allowing players to simultaneously live online and offline (ComScore, 2012). This blending of worlds is expected to increase and over the next decade it is predicted we will begin to move seamlessly between our realms, unable to discern which we are situated within (Smart et al., 2008).

The worlds in which role-playing games are situated have been thoughtfully designed for a number of purposes including interest, excitement, levels of immersive feeling, reality of experience, as well as challenge (Yee, 2010). Just as in the physical world where education, skills and abilities allow for increased wealth, in games players develop skills which result in the ability to amass valuable property and increase their power and wealth (Kane, 2009; Yee, 2006). Games are also designed to induce social interaction; however, unlike the physical world where social interaction is subject to an almost infinite number of variables, levels and types of social interaction are deliberately written into the code (Korsgaard, Picot, Wigand, Welpe, & Assmann, 2010; Yee, 2010). Coding is considered the architecture of the game and "…is a kind of law: it determines what people can and cannot do" (Lessig, 1999, 58-59).

Early assertions were that code would control the behaviour of individuals online; however, it has been shown that humans are particularly inventive and often determine how to outsmart coded-in rules, violating community standards and fair rules of game-play (e.g., Adrian, 2010; Dibbell, 1993). On the other hand, empirical research, examining in-game friendship, has demonstrated that the nature of these code-based worlds does encourage close bonds in the form of friendship. 75% of players, who report they have become good friends with someone in a game, describe these relationships as more intimate and intense than they experience in the physical world (Yee, 2010). Strong friendships form, in part due to the naturally social nature of humans (Vallor, 2011) but within game space this sociability is enhanced due to the need for cooperation in the pursuit of common goals (Axelsson & Regan, 2002). Just as the playing of games and metaverse living has embedded itself into our physical lives and spaces, online friendships, when they cross over from the game to the physical world do the same (Korsgaard et al., 2010; Axelsson & Regan, 2002). Researchers who predict that online

and offline worlds will soon seamlessly blend, find strong support for their prediction when essential social relationships, such as friendship, blend seamlessly between these two worlds.

In addition to design features that encourage and enhance pro-social interaction, online games have specific qualities of terrain design as well as processes the player goes through to achieve entrance into the space. These rituals have the effect of increasing feelings of having crossed over into a realm that is real. According to Mitchell (1996) in *Contiguous/Connected*:

> Spatial cities, of course, are not only condensations of activity to maximize accessibility and promote face-to-face interaction, but are also elaborate structures for organizing and controlling access. They are subdivided into districts, neighborhoods, and turfs, legally partitioned by property lines and jurisdictional boundaries, and segmented into nested enclosures by fences and walls. For the inhabitants, crossing a threshold and entering a defined place – as an owner, guest, visitor, tourist, trespasser, intruder, or invader – is a symbolically, socially, and legally freighted act.

The symbolic crossing-over into a type of parallel world that is like, yet unlike, our physical world is deeply embedded into the cultural history of Western literature and philosophy. Most children have been exposed to ideas of crossing over to parallel worlds through stories such as *Alice in Wonderland*[6] by Lewis Carroll, *The Lion, The Witch and the Wardrobe*[7] by C. S. Lewis, the poetry of William Butler Yeats, including "The Lost Child"[8], the *Old Testament* stories in the *Bible* and epic retelling of the fall from

[6] In *Alice in Wonderland,* the child, Alice, after falling down a rabbit hole finds herself in a strange world that is similar to her "real" world. To return to her real world, she must achieve the goal of re-orienting herself and managing the fantastical adventures and creatures she meets without the complete loss of her mind or her way.

[7] In *The Lion, The Witch, and the Wardrobe*, four children are sent to a country house during the London bombings in WW II. There they find a large wardrobe placed in an empty room. Entering the wardrobe they find themselves in the fantastical world of Narnia.

[8] In *The Lost Child*, a child is enticed to a fantastical fairy world through the proffering of real world treats such as berries by the fairies who guide him over.

grace in works such as *Paradise Lost* by John Milton[9]. These spaces have also been the subject of much philosophical discussion (see, for example, Foucault's discussion of the heterotopia, places of otherness, situated on the borders of regular space operating under non-hegemonic conditions). For games, the very familiarity of the concept of crossing over imbues these spaces with a reality that adds to the sensation that events that occur within them are real. The design features of games taps into the shared crossing over mythos and the process whereby the players enter the game to play together creates a foundation upon which a sense of community and shared immersive real space is created.

Immersive, massive, multiplayer, role-playing games are even more popular than metaverses, with an estimated 100 million avatars (each generally representing a unique player) participating in them at any given moment (Kane, 2009). Between 20 and 30% of those who play are more involved and spend more time socially in the online world than they do in their offline world (Kane, 2009). World of Warcraft, one of the most popular online games, had 11 million subscribers worldwide in 2010 (Barnett, Coulson, & Foreman, 2010). Immersive games, like metaverses, may also be the site of education and business as well as academic conferences, such as "Convergence of the Real and the Virtual" held in World of Warcraft in 2009 (Bainbridge, 2010a). As an individual's life-roles blend and cross over between worlds (e.g., student at a physical university with classes held inside a game) the perception that there is really any difference between realms becomes much less defined (Bainbridge, 2010b).

Just as commerce has emerged in metaverses, so too has it emerged in games. Some players prefer to purchase items rather than spend the hundreds of hours of gameplay necessary to acquire them. This has led to the creation of a huge secondary market (estimated at 1.5 billion U.S. in 2007) in the physical world where virtual artifacts are sold privately and through online auctions (Kane, 2009). This has not only resulted in a large and lucrative market of transactions (the highest recorded price paid for a

[9] In *Genesis* and the retelling in *Paradise Lost*, Adam and Eve, the first two people on earth are tempted to eat an apple from the Tree of Knowledge and as a result fall from the grace of their world of perfection and idyll to a world that is similar but where they must work to survive.

virtual item, a space station, in 2007 was U.S. $100,000), but has also led to crime in the real world as a result of virtual business dealings going awry (TechCrunch, 2007, as cited in Kane, 2009).

Virtual property deals have generated conflicts, with a number of these now making their way through courts. In Shanghai, China (2005), one player borrowed an artifact from a fellow player and rather than return the item, as promised, he sold it on an online auction site. When the lender demanded money in lieu of the property and was refused, he stabbed the man to death (Finlayson, 2005). The case was resolved with a guilty plea for intentional injury; however, the mitigating circumstances of theft of virtual property could not be admitted as evidence due to the fact that China did not, at that time, have virtual property laws (Finlayson, 2005).

In 2006, the U.S. courts were asked to make a decision over a virtual property deal gone bad (*Bragg v. Linden Research, Inc*. (2006)) and also, in 2006, they were asked to determine the legality of *farming* – a practice of hiring third-world labourers to play online games with the purpose of amassing virtual goods that could be sold for real-world money (see *Hernandez v. Internet Gaming Entertainment and IGE US LLC* (2007)). The fact that courts are making decisions regarding the creation, sale, purchase, and trade of virtual property, as well as adjudicating in matters related to theft of virtual property, demonstrates the very real financial and personal losses some individuals have sustained and gives greater weight to the significance of online gaming sites. As stated by Cohen in her examination of law and real place online, "cyberspace is peopled by real users who experience cyberspace and real space as different but connected, with acts taken in one having consequences in the other" (Cohen, 2007, p. 212). Definitely, when a player murders another player over an artifact used to achieve the next level in a game, the consequences of game-play have certainly spilled out into the physical world.

Metaverses and games act as extensions and expansions of our physical lives. Within them we form and maintain relationships, conduct commerce, and even acquire an education. Through a shared, ritualistic crossing over, our physical and virtual selves become situated simultaneously in both, deeply fusing these worlds. Friendships that form within games move out into the physical world; virtual property, produced within games, similarly moves into the physical world to be bought, sold, shared, and even stolen. Given the large number of hours spent within games to earn these virtual items,

their theft or loss may cause strong, violent emotions with equally strong, violent acts. As such, these online social spaces are legally and socially freighted with significance.

Courts, all over the world, have begun to watch online social spaces closely with the goal of defining the meaning and significance of virtual property. Given the very real outcomes, such as murder, that have also occurred, it is expected that they will also be asked to make assessments regarding virtual acts, especially those that result in violent outcomes. While China and other countries, do not yet have separate virtual property laws, many have begun to apply physical world property laws to the plethora of cases the courts have been asked to adjudicate (Adrian, 2010; Lastowka & Hunter, 2004-2005; Ledgerwood, 2009; Lim; 2010). Given their willingness to hear cases based on virtual property, it is only reasonable to conclude, they will soon show a similar willingness to adjudicate virtual behavior. To do so, courts will need to determine whether avatars are property that can be bought, sold, stolen, and potentially damaged or destroyed and thus protected by criminal property law, or whether they are some type of quasi-human and thus, entitled to a higher level of protection offered by criminal personal law.

2.5. The Social Network

Online social networks differ considerably from metaverses and online games as they are not parallel worlds but websites designed to reflect people and events in the physical world (Pentecost, 2011). Most sites encourage members to create an individual profile they personalize through expressions of the self, related activities, interest, hobbies, educational affiliations, or any other information the user would like to share (Facebook, 2012). Used for connecting and staying in contact with friends, family, business associates, co-workers, and even celebrities, users "friend" other people with whom they would like to have a relationship (Kay, 2007).

Social networks facilitate reciprocal exchanges that are socially gratifying including a forum for self-expression, the proffering and acceptance of friend requests, the ability to "like" something on a friend's page, the ability to share photos and videos, as well as a plethora of third party applications (Vallor, 2011). Networks encourage users to build complete virtual representations of themselves through a variety of activities including the posting of location and event statuses, sharing of thoughts, beliefs, and opinions, recording life events, and the uploading of personal photos (Kay,

2007). Social media sites, such as Facebook, Twitter, and LinkedIn are extremely popular: 70%of those who use the Internet log onto these sites one hour per day, seven days per week (Pew, 2008). For many, social media sites become virtual "identifiable communities" linked by "emotion" and "mutual interest" that are as strong, or stronger, than the physical communities they belong to (Pentecost, 2011).

While metaverses and games reach millions in North America, the influence of social network sites have eclipsed both and are the most popular online activity accounting for 19% of all time spent online (ComScore, 2012). Social networks cross all demographic boundaries and are as popular with those over the age of 55 as those who are younger (Brynko, 2011). For the digital generation (ages 15 to 24), social networking is the norm and is expected to become the most important communications channel over the next few decades (Brynko, 2011).

Social networks can be accessed via a number of different platforms including mobile devices, tablet computers, and personal computers. Mobile devices allow users to connect at will, facilitating real-time interaction, allowing social networks to seamlessly blend into people's lives (ComScore, 2012). 40% smart phone owners log on daily to check status updates, post their own thoughts, and use location-based check-in services (ComScore, 2012). This demonstrates the desire for North Americans to be connected wherever they are and whenever they desire, thus "what we are seeing is the dawn of a truly connected era, where social networking platforms integrate more seamlessly with our lives through mobile technology" (ComScore, 2012, p. 24).

Social networks can be used for both strong, interpersonal bonds (close, personal relationships) and weak ties (acquaintance-type relationships) (Granovetter, 1973 as cited in Gilbert & Karahalios, 2009). Weak ties have been empirically shown to facilitate the dissemination of information much more widely than strong ties. This ensures information posted reaches close personal friends as well as acquaintances, co-workers, and others (Gilbert & Karahalios, 2009). Online social networks are similar to metaverses and immersive games, having the ability to support and strengthen friendships, including the principles of reciprocity, empathy, self-knowledge, and shared life (Vallor, 2011). Many use social networks to stay in touch with acquaintances as well as for maintaining strong ties from the physical world (Ellison, Steinfield, & Lampe, 2007). Large-scale surveys report that online users are more likely to have large networks of strong relationships (Pew, 2006) than those who do not use them (Brynko,

2011) with 81% of users stating they are willing to ask their online friends for help, information, decision-making, finding a new residence or job, home renovations, and political advice during elections (Boase et al., 2006). In this manner, online social networks not only act as an extension to our physical lives but also expand the number of social relationships far beyond that which could occur in physical space.

Online social networks have been shown to have particular utility for those who are too shy to form and maintain social ties in physical space (Ellison et al., 2007). This type of computer-mediated communication has also been shown to lower barriers and increase levels of honest self-disclosure (Bargh, McKenna, & Fitzsimons, 2002; Tidwell & Walther, 2002). In laboratory experiments, students were paired and asked to converse for short periods of time face-to-face or via Internet chat room, demonstrating that via computer they were more likely to develop higher levels of affection for their partner and, as a result, offered increasingly intimate and honest personal self-disclosures including location and contact information for themselves in geographic space (Bargh et al., 2002; Tidwell & Walther, 2002). Self-disclosure and feelings of affection in combination with high levels of trust render social network users particularly vulnerable to exploitation in these online communities. As well, online social networks provide those inclined to stalk and harass access to information related to potential victims' lives in geographic space.

Social media has become indispensible for many living in North America. Individuals access it daily, in multiple locations, to share personal aspects of their lives, thoughts, opinions, and beliefs. Social networks allow for representations of the physical and authentic self and, thus, affect not only online and offline friendships that build social capital (Helliwell & Putnam, 2004) but also impact mental health (Bargh & McKenna, 2004). The increase in connections that occur as a result of online social access, facilitate the formation and maintenance of online friends, giving individuals access to a wider base of knowledge and information; however these networks also make them vulnerable to a wider group of people including those who would potentially stalk and harass them (Mann, 2008).

2.6. The Constructed Self

Individuals in North America who use the Internet are no longer fated by their birth, biology, or social circumstance because the creation of virtual space has allowed them to be anything and anyone their imagination allows (Turkle, 1999). Deliberate ambiguity, false signals, and imaginative design permit those in cyberspace to confuse the assessment of gender, age, sex, socio-economic status, education, race, culture, and all other aspects of the self in a manner that even 30 years ago was barely conceivable. This quality has both positive and negative repercussions, allowing individuals to become an idealized self or to don a disguise with the goal of obscuring true identity in the case of deviant or criminal behaviour.

Most Internet users create online personas for their technology-mediated communication (Bainbridge, 2010a) with some deliberately creating sophisticated visual icons known as avatars, while others create more minimalist avatars which are the by-product of the compilation of photos, personal thoughts, and responses to others in social networking sites (Bainbridge, 2010a; Franks, 2011). The avatar is a media-rich representation, increasing the amount of information we are able to extract from online social interactions while using it (Riva & Galimberti, 1997). Regardless of type, the avatar represents meaningful choice on the part of its creator when determining their virtual identity (Bailenson & Segovia, 2010; Huh & Williams).

The word “avatar,” which is of Sanskrit origin, denotes the incarnation or physical embodiment of the divine and, for the purpose of online personal representation, has been utilized since Neil Stephenson’s novel *Snow Crash* (1992). It is clear, however, that the avatar holds a more utilitarian position in our lives, “at its core [the avatar] is an interactive, social representation of a user” (Meadows, 2008, p. 23 as cited in Gunkel, 2010). Despite its utilitarian position it does hold significance and meaning for those using it (Bailenson & Segovia, 2010, Wolfendale, 2008) and many refer to their avatar using the personal pronoun, “I” (Wolfendale, 2008). High levels of emotional attachment, one of the most basic expressions of being human (e.g., Freud’s discussion on first attachments (1910)), are also often demonstrated towards avatars, including one’s own (Mennecke, Triplett, Hassall, Conde, & Heer, 2011).

The avatar is remarkable because users have the ability to manipulate its appearance, attributes, and characteristics resulting in a media-rich representation

(Lombardi & Lombardi, 2010). Users can create an avatar in their own managed image, as seen on social networking sites, (Gunkel, 2010; Yee, 2008) or in imaginative and fanciful ways, allowing the individual to experiment with new identities (Gunkel, 2010; Yee, 2010).

The ability to manipulate avatar characteristics has been celebrated as a way to liberate one's self from physical determination in geophysical space, creating a kind of postmodern cultural image of identity disengaged from gender, ethnicity and other constructions which may embody problems (Turkle, 1999; Yee, 2008). It has also been critiqued for trading on stereotypes of race, ethnicity, and gender, as a kind of "identity tourism" that can be donned and shed without real-life consequences (Nakamura, 2002). Donned as a disguise, it provides opportunity to perpetrate deviant and criminal behavior and given that depersonalization through disguise has been empirically shown to increase the likelihood of hostile and aggressive behavior (Mann, 2008; Zimbardo, 2007), there is reason to be concerned about the effects of using avatars socially.

For example, in his famous, Stanford Prison experiment in the 1970's, Paul Zimbardo, a psychologist studying deindividuation, randomly assigned college students to play the role of prisoners or guards to see how they would behave. Giving students assigned to the role of guard, mirrored sunglasses and uniforms, it took little time before the wearing of a disguise reduced their inner constraints and led to highly anti-social behaviours including physical aggression and sadistic torment (Zimbardo, 2007). Other empirical studies on deindividuation in high school classrooms, led to students using obscene language, the breaking of conventional norms governing conversation, self-expression in an extreme manner such as criticizing others and the performance of embarrassing behaviours (Lindskold & Finch, 1982; Mathes & Guest, 1976; Singer, Brush, & Lublin, 1965 as cited in Forsyth, 2006). As evidenced by these studies, the donning of a disguise can encourage hostile and anti-social behaviours.

Early Internet philosophers such as Sherry Turkle (1999), believed the gap between virtual and actual self-representation would be large because of the freedom offered by the anonymity of the Internet (Turkle, 1995). Even so, recent studies have shown that in immersive games only 20% females and 17% of males make any type of significant change from their physical selves when creating virtual self-representation (Huh & Williams, 2010). As in the case of avatar representation, current research has also shown that personality is fairly consistent with individuals demonstrating similar

social behaviours and emotions when embodied as avatars compared to their physical selves (Boellstorff, 2008).

There are several theories as to why humans create such similar virtual representations of the self and respond so strongly to avatars including the theory of self-concept. Self-concept theory posits that our understanding of the existence and properties of a separate self and its characteristics will both contribute to our self-definition as well as regulate our behaviour (Rosenberg, 1979 as cited in (Mennecke et al., 2011). Therefore, avatars, as a significant representation of the self, will serve to help define and regulate our physical selves.

The attachment individuals demonstrate for their own avatars also extends to the avatars of others, imbuing online interaction with an importance akin to physical social interaction (Mennecke,et al., 2011). Embodied social presence theory posits that when social actors experience a higher level of embodied interaction they more effectively encode, convey, and decode individual and collective communicative acts (Lombard & Ditton, 1997 in Mennecke et al., 2011). The avatar, as an embodied representation of the social actor is the nexus of this communication, thus the communicative act, in a virtual environment, has symbolic meaning through shared space and tools (Lombard and Ditton, 1997 in Mennecke et al., 2011).

Given the attachment we show to our own avatar representations as well as those with whom we socially interact, it makes sense when avatars are taken over against their will or violently attacked, the person behind the avatar will experience distress. Bailenson & Segovia (2010) found that individuals whose avatars were “mind-controlled” by other players experienced high levels of helplessness and distress not only during the episode but following, when they were asked to reflect back on the experience. They also found that participants in virtual reality studies who found doppelgänger avatars, they weren’t controlling, expressed confusion and described feelings of loss (Bailenson & Segovia, 2010). During these same studies, magnetic resonance imaging (MRI) demonstrated that self-referential information is processed using unique structures in the brain resulting in an increase in significance of information acquired and more deeply embedding the related memories (Bailenson & Segovia, 2010). This makes events that a doppelgänger avatar experiences more likely to hold greater personal significance for the individual witnessing their look-alike manipulated by others. This significance increases the likelihood that these experiences will be retained

for longer time periods, embedding them as long-term memories (Bailenson & Segovia, 2010).

The avatar, as our personal representative is highly effective for the purpose of social interaction and communication for a number of reasons: it is media-rich, capable of sending and receiving social cues, holds relevance and importance for the individual who creates him or her, and while immersive games, metaverses, and social networks (to a lessor degree) allow for disguise and the selection of avatars that do not match the physical individual behind them, rarely do people choose to alter themselves in that manner. Given that social interactions online mimic those of offline spaces and that individuals are clearly aware of the social presence of others, the avatar becomes personally and socially significant much in the same way as our physical bodies in physical space.

2.7. The Constructed Self in Metaverses and Immersive Games

The above discussion covered a great deal of the information specific to 3D avatars. There is, however, some information that exclusively relates to avatars in metaverses and games. The inclusion of graphical elements, such as is seen with avatars, increases the potential range of emotions and resulting interactions and experiences that the avatar and person is capable of sending and receiving (Blascovich & Bailenson, 2011). Given that avatars are embodied constructions of the controller's self, it is reasonable to assume that it is not the graphical representation that is actually experiencing the emotions and interactions, but the individual behind the avatar (Bailenson & Segovia, 2010).

In many ways, the metaverse parallels our experience of physical space. When we place a personal avatar within a metaverse, that avatar may be used as a tool for exploring possible futures and examining the implications of those possibilities (Turkle, 1999). This exploration occurs through the augmentation and extension of physical space, the simulation of possibility within that augmented space, individual identity formation, and the acquisition of information about, and control of, the world around the avatar (Smart et al., 2008). Given that this type of experience holds deep significance and, as demonstrated by experiments, informs the individual behind the avatar altering

cognitions in physical space (Blascovich & Bailenson, 2011), these experiences are perceptually real and important for the individual experiencing them.

For those participating in metaverses and immersive games, the space and experience may be perceived as even more real than terrestrial existence (see *Infinite Reality: Avatars, Eternal Life, New Worlds, and the Dawn of the Virtual Revolution,* Blascovich & Bailenson, 2011 and *Online Worlds: Convergence of the Real and the Virtual,* Bainbridge (Ed.), 2010). Part of the reason that online personal representations are considered so real is that avatars are created and act as agents for the human behind them and use language to communicate (Wolfendale, 2007). Language is essential for the communication of humans and, as such, tends to provide cyberspaces with a level of significance and reality equal to the physical world because words are considered expressive of a person's intentions and actions in both physical space and cyberspace (Wolfendale, 2007).

The tendency of the game or metaverse to expand and augment real space blurs boundaries between them. This seamless movement of experience between the two realms translates into a similarly seamless movement in cognition (Blascovich & Bailenson, 2011). In virtual reality experiments with children, researchers immersed subjects in a "swimming with whales in a virtual Sea World" experience. Questioned a week following the incident more than 50% of the children were convinced the memories were real and that they had, indeed, gone swimming with the whales – not *observed* themselves swimming with the whales (Blascovich & Bailenson, 2011). Experiments such as these demonstrate, as we experience increasing degrees of blended worlds that are media-rich, it is reasonable to assume that experiences sustained in either realm will deposit memories that, in review, will be indistinguishable one from the other.

As can be seen by the experiments and cognitive and emotional reactions to creating personal representations for placement in a game or metaverse, the act is symbolic, socially and personally meaningful, and capable of resulting in experiences any socially significant space and interaction can create. This offers insight into how individuals experience emotionally intense experiences. It is not unusual today to hear that a friend or relative has fallen in love with someone they met in cyberspace and have yet to meet in physical space lending support for the social and emotional significance of avatar social interaction. While this may result in closer bonding between individuals it may also result in serious emotional harm should an avatar be unexpectedly violently

attacked. Given that the avatar is a clear extension of the individual behind him or her any violence it sustains will be perceived as such and cognitively embedded via memory becoming indistinguishable from events sustained in the physical world.

2.8. The Constructed Self in Social Networks

Profiles are created when an individual joins and provides answers to preset questions related to demographics such as age, sex, geographic location, and "the about me" section which asks for personal interests and beliefs (boyd & Ellison, 2008). Adults on social networks are usually familiar with one another in the physical world prior to becoming friends on the social network (Gunkel, 2010). This disallows large deceptions as to race, gender, or other clearly identifying qualities (Gunkel, 2010). Individuals do, however, indulge in image management by choosing the most flattering images and poses for their profile photo, demonstrating a desire to be thought of as attractive by others (Wang, Moon, Kwon, Evans, & Stefanone, 2010).

While computer-mediated communication has come a long way since its inception, online representations are still not as rich as offline (Wang et al., 2010). The social identification model of deindividuation effects by Lea and Spears (1991/1995) posits that a lack of identifiability serves to accentuate the effect of salient social identity and strengthens the dominant normative response associated with it. This means that individuals will increasingly use stereotypes and exaggerated representations of others to fill in information that is missing online.

In empirical studies, using fake profiles on a social networking site, adults were observed augmenting their self-presentation through hyper-personal interactions including spending significant time to compose and edit messages utilizing more cognitive resources and offering higher levels of intimacy (Walther, 2007). When messages were sent asynchronously, participants spent more time and cognitive resources composing and editing them compared to interactions that were synchronous (Walther, 2007). This, in many ways, mimics social interaction in physical space but in an exaggerated manner.

Personal self-disclosure occurs in profiles on social networks via written exchanges on walls or daily news feed postings and can be used as a measure of friend intimacy and to measure the progressions of relationships online (Walther, 2007). One

byproduct of these interpersonal exchanges is that it provides, often publically, an increasingly complete and intimate image of the physical person behind the social network profile (Walther, 2007). This online public disclosure of one's most intimate information is both the facilitator of relationships but also makes the individual increasingly vulnerable to exploitation such as harassment and stalking which can occur in either realm – the social network online, or in geographic space, offline (Mann, 2008; McLaughlin & Vitak, 2012).

2.9. Conclusion

Our online social interactions in metaverses, games, and social networks place us firmly within these otherworldly, but very real spaces as well as embedding them into our physical lives. The communities we perceive to exist influence the way we think about them as well as how we behave and interact with others (Parks, 2011). Experiences in online social realms cause change in our physical selves and communities through the multiplicity of places and experiences we sustain (Cohen, 2007, p. 235). Despite a lack of agreement over whether online experiences are real or more real than their offline counterparts, the high numbers of North Americans logging on daily to participate in role-playing games, metaverses, and social networks, demonstrates it is obvious that these online worlds compete directly with the physical world for our time and attention (Bainbridge, 2010b).

Blurred boundaries between the physical and the virtual, expanding weak-tie social networks in conjunction with perceived meaningful social interaction is changing the way we think and behave in online spaces. This leads people to divulge increasing personal information to increasingly unknown groups of others whose trustworthiness cannot be known with any certainty.. Media richness, 3D spaces, and personal profiles, supported by visual imagery, are all geared to appeal to the human's evolutionary and developmental abilities (Lombardi & Lombardi, 2010) which results in a sense of natural evolution for the transference of meaningful social relationships into these online spaces. Persistence of space simply enhances the effect, given that these worlds exist before we enter them and remain after we leave, providing a permanence and continuity equal to, if not more so, than the permanence of our physical worlds.

Personal self-disclosure, perceptions of identifiable social groups, and the desire to work cooperatively to create and maintain online spaces and friendships are all reflective of human behavior in the physical world. Relationships can and do occur, but are amplified by the unique qualities coded into online social spaces. The value of artifacts we create online has also intensified our feelings of reality and permanence for online social spaces as well as increased feelings of need to protect that property. The involvement of North American courts, addressing issues such as value, appropriate use, and disposal of such assets, provides support for the contention that we need no longer assume the virtual has no place, value, or significance in the physical world.

In addition to constructed online social places that we have begun to view as extensions of our physical world, within these online spaces we also construct and place representations of ourselves to act as our agents. These agents hold a great deal of importance for those who construct them, yet at the same time, provide opportunity for disguise and deceit. Virtual violent acts such as cyber-rape, cyber-harassment, cyber-stalking, and cyber-assault are all facilitated in cyber places populated with avatars due to the ease of disguise and the availability of access to these human representations. Given that individuals care so deeply about their virtual selves, these acts will hold great significance for those who would sustain them.

The personal representations we create and place online are closely tied to the physical human behind them. Social connections, regardless of where they occur, are critically important in the lives of humans. Online social spaces provide for augmented and expanded emotional and intellectual interaction. Yet, this very ability, to facilitate social interaction, also facilitates the dispersal of information, resulting in higher levels of vulnerability for the online and offline person because they provide increasingly complete personal profiles online which offer predators the information necessary to locate victims online and also in real time and geographic space.

Disturbingly, in addition to expanded social interaction, the basest of human nature has also emerged in these online social spaces. Theft of virtual property, resulting in murder, has reminded us that, just as in physical space, there will always be those who will violate trust and those who will wreak revenge for that type of violation. Given that the self-images we place online are viewed as meaningful and valuable as both personal representations and virtual property, it is likely that over time we will

become more vigilant about their safety and guardianship and should they be violently attacked, will most definitely be violently revenged.

Trust is highly salient to feelings of violation when an individual is assaulted or harmed. Higher levels of trust that emerge in social networks make individuals particularly susceptible to this kind of violation. As a result of the importance of not only the places we go online but the constructed selves that we place there, trust is an important part of the social interactions we conduct and violations have both personal and, sometimes, legal implications. The next chapter examines the concept of trust in physical and online spaces and its salience for accountability, litigation, and legislation.

3. Trust

Trust acts as a form of security in our social world (Bierhoff & Vornefeld, 2004). Based on stipulated conditions, both clearly stated and simply understood, trust is necessary if a society is to function and thrive (Rotter, 1967; Weinstock, 1999). Online, trust has also been considered a necessary condition for cyber-societies to function and thrive (Nissenbaum, 2001); however, just as it occurs in physical space, misplaced virtual trust allows for us to become victims of hostile and violent acts (Grodzinsky, Miller & Wolf, 2011).

3.1. Functions of Trust

Trust is the "faith or confidence in the loyalty, veracity, reliability, strength, etc. of a person or thing" (Barber, Ed., 2004). Understanding the dynamics of trust is central to understanding modern society, as trust is evident at all levels from close, personal relationships to more distant, contractual interactions (Markova, Gillespie & Gillespie, 2008; Nissembaum, 2001). Trust in others can be both rational and irrational therefore all trust involves some level of risk (Grodzinsky et al., 2011; Simpson, 2011; Weinstock, 1999). External controls, such as the publication and punishment of misdeeds, are effective in ensuring that community-members do not violate others' trust (Hardin, 1996). It is not unusual for individuals and groups to look to past dealings with other individuals, groups, or institutions to make decisions regarding in whom, and in what, it is safe to trust (Hardin, 1993; Hardin, 1996; Nissenbaum, 2001; Taddeao & Floridi, 2011). Trust-affirming actions within a community will help trust to grow resulting in stability and control (Hardin, 1993; Putnam, Leonardi, & Nanetti, 1993). More formal institutions are often utilized to enforce the power of social constraints, such as conventions, norms and laws; however, these are not enforced in loosely connected or highly diverse societies in the same manner as they are in highly collective societies (Hardin, 1996; Weinstock, 1999). Trust induces and increases levels of cooperation, success, enrichment,

boldness, adventure, creativity, and, ironically, the possibility of criminal success (Nissembaum, 2001

3.2. Principles of Trust

Social scientists agree that trust generates positive influence in the lives of humans, is instrumental and implicated in many valued aspects of individual and social life, and requires a relationship, regardless of intensity and duration, between a trustor (person/agent trusting) and a trustee (person/agent in whom the trustor places that trust) (Bierhoff & Vornefeld, 2004; Grodzinsky et al., 2011; Hardin, 1993/1996; Taddeo & Floridi, 2011; Weinstock, 1999). Several academic writers also agree that there are basic principles upon which trust forms and flourishes including history and reputation, personal characteristics, mutuality and reciprocity, role fulfillment, and contextual cues (Bandura & Walters, 1963; Cosmides & Tooby, 1992; Nissenbaum, 2001; Rotter, 1964 as cited in Rotter, 1967).

There is a high level of agreement as to the basic principles, in the physical world, upon which humans predicate their trust. If human nature is to be considered consistent, and the principles of trust in the physical world considered salient for the online world, then trust online should fail on all the principles due to anonymity. If trust cannot be formed and maintained online, it would logically follow, no communities would form and stabilize, and online activity, of all types, would fail to flourish in attempts by individuals and groups to minimize risk. Yet distinct communities, as bounded in social networks, immersive games, and metaverses, have flourished with greater numbers of individuals joining in these activities and greater amounts of time being spent online, as the Internet has aged. Given that trust is a crucial mechanism, central to the lives of humans in all societies and all communities, trust must have transferred to online sites in a manner that permits trust to form and be maintained. The following sections will explore how trust forms and is maintained in these online spaces followed by an examination of violations of trust and criminological and psychological theories which may explain those violations.

3.3. Trust in Cyberspace

E-trust, or trust that forms solely in cyberspaces, occurs without direct and physical contact. When there is no direct and physical contact, morals and social pressures may be differently perceived (Taddeo, 2009). If theories of social e-trust are to spring from historical theories of social trust and explain the formation and maintenance of trust in social networks, immersive games, and metaverses, then these new theories must somehow account for the lack of direct and physical contact or re-imagine trust as bounded in the person and their constructed online presence.

In 2001 Nissembaum claimed that, in relation to cyberspace, the subject of trust was beset by deep and difficult questions regarding authority and governance especially at a time when the Internet was increasingly being used for relationships, community life, information, and commercial interactions. This has proven to be true. Increasing numbers of individuals go online for a myriad of utilitarian and social reasons and, at the same time, new legislation has been enacted in North America to deal with the problem of online victimization (e.g., in Canada, *Canada Criminal Code,* s. 342.2, "unauthorized use of a computer"; s. 430, "mischief in relation to data"; the *Personal Information and Electronic Documents Act;* in the United States, *Identity Theft and Assumption Deterrence Act of 1998*, *Identity Theft Penalty Enhancement Act*, and the *Communications Decency Act of 1996*). Nissembaum (2001) further claimed, as the Internet became a more certain part of our lives, trust in cyberspace would emulate trust in physical space as individuals and groups sought to improve the quality of personal experience, communal life, civil life, and stability of government and these, in turn, would allow the online world to thrive (Nissembaum, 2001).

If it is assumed that Nissembaum (2001) was correct in stating that only when trust manifested would cyberspace flourish socially, then, given the increase in individuals flocking to online social spaces, we can presume that e-trust has formed and is present in cyberspace.

3.4. Trust in Metaverses

There are a wide variety of parallel world websites available with distinct norms emerging within the context of each (Chen, 2005; Martey & Stromer-Galley, 2007; Suler,

2004; Williams, Ducheneaut, Xiong, Zhang, Yee, & Nichell, 2006). As I stated earlier, metaverses are parallel worlds that resemble the physical world with all its activities such as work and play (Smart et al., 2008). The following examination of metaverses will be conducted through the social interaction of players and the context of play space to determine whether trust can emerge and be maintained in a manner similar to the physical world.

3.4.1. History and Reputation

The process one goes through to create and name an avatar might imply the taking on of a disguise or a persona, similar to the way it has been historically thought of: as a mask donned for social interaction but not necessarily representative of the real person (Boellstorff, 2008). When metaverses were first created this was the common opinion of many researchers (e.g., Schaap, 2002 as cited in Boellstorff, 2008); however, recent research demonstrates that individuals who spend anything beyond minimal time in a metaverse tend to drop the role-play quite quickly and revert to a much closer version of their real selves (Boelstorff, 2008; Dibbell, 1993). Thus, avatar behavior, as reflective of the values and beliefs of the person behind the avatar, tends to be stable, especially if considerable time is spent in virtual worlds (Boellstorff, 2008; Dibbell, 1993).

As metaverses and other virtual worlds are increasingly used for education, business, and nonprofit work, the trend of mandatory anonymity (as is currently required by EULAs in many virtual worlds) appears to be diminishing with more sites allowing the participant to link their virtual-world self to their physical-world self (e.g., Kaneva) (Boellstorff, 2008). This, of course, will enhance history and reputation as principal factors of trust. Given that trust is based partially on the ability to ascertain various criteria including personal history and reputation of an individual, the stabilization that metaverses are experiencing would indicate that these can be used to judge and display trustworthiness.

3.4.2. Inference Based on Personal Characteristics

Ongoing relationships, avatars sustain, lead to close relationships and indicate the assessment of personal characteristics. Ethnographic researchers found that avatars, working collaboratively, demonstrate heightened situational and social

awareness while sharing ideas and concepts (Martey & Stromer-Galley, 2007). Through collaborative work avatars establish relationships while assessing personal characteristics by observing behaviours such as politeness and courtesy (Martey & Stromer-Galley, 2007). Sharing community activities increases the likelihood of individuals giving and receiving trust (Yee, Bailenson, Urbanek, Chang, & Mergot, 2007).

Nonverbal communication is recognized as a key component of interpersonal interaction (Argyle, 1988 and Hall, 1959 as cited in Yee et al., 2007) and offers a way to assess characteristics such as the desire for the good opinion of others that is demonstrated by following social norms (Yee et al., 2007). In 2007, researchers collected and analyzed 420 hours of information in Second Life related to interpersonal distance and eye gaze (Yee et al., 2007). Comparing physical world social norms to those displayed by avatars, researchers determined that they were similar. Avatars take turns in speech and follow interpersonal distance norms, such that pairs of female avatars stood closer together than male or mixed gender pairs, and female avatars gazed into each other's eyes more than males or mixed pairs, leading researchers to conclude that social norms, which dictate conventions in the physical world, are replicated in metaverses (Yee et al., 2007).

3.4.3. Mutuality and Reciprocity

Mutuality and reciprocity, in the form of virtual reciprocal altruism, is common in metaverses with the tendency for residents to offer free advice, support, and objects to other avatars (Boellstorff, 2008; Martey & Stromer-Galley, 2007). Being polite is considered highly important in some worlds (Martey & Stromer-Galley, 2007). In an ethnographic study of the Sims Online, Martey and Stromer-Galley (2007) found that hosts of homes were expected to provide food and accommodation for guests, greet them upon arrival, and ensure the rules of the house were enforced. Guests were expected to respond to greetings, be tidy, sometimes help with cleaning and cooking, be grateful when fed, and avoid insulting other guests. Guests and hosts came to know one another over time and would greet each other with fondness and familiarity if their previous interactions had been positive (Martey & Stromer-Galley, 2007). Clearly, mutuality and reciprocity are present in some metaverses inducing and maintaining trust.

3.4.4. Role fulfillment

In games like Sims Online and Second Life, many individuals choose to play out physical world conceptions of family members, friends, lovers, or other such roles (Boellstorff, 2008; Martey & Stromer-Galley, 2007). Often these roles take on accepted offline norms and the behaviours attached to them (Peña & Hancock, 2006; Yee et al., 2007) including attendant cooperation (Tidwell & Walther, 2002), intimacy (Walther, 2007), and self-disclosure (Walther, Van Der Heide, Kim, Westerman, & Tong, 2008).

In Second Life, many players have established commercial enterprises that are not only economically viable (e.g., Anshe Chung) but also employ other avatars (Tseng, 2012). The roles of employer and employee, with attendant wages and rules of work, help to establish the fulfillment of roles with the same online expectations (e.g., payment for services rendered) that occur offline. This helps to establish strong norms around those roles and expectations.

3.4.5. Contextual Factors

Norms exist as a result of context in metaverses with individuals learning simple behaviours such as standing up to signal impending teleportation as well as learning how to land outside homes and other private areas to ensure they do not go where not invited (Boellstorff, 2008; Martey & Stromer-Galley, 2007). These cultural norms, for politeness and social interaction, are highly reflective of the offline world (Boellstorf, 2008; Martey & Stromer-Galley, 2007). As in the physical world, when interactions are not positive, others generally used mild admonishment and encouragement rather than more forceful methods (Martey & Stromer-Galley, 2007). Martey and Stromer-Galley (2007) found that hosts would quietly speak with misbehaving avatars or deal with them privately rather than forcefully ejecting them from their homes (though they have the right and ability to do so).

The presence of clickwrap agreements, a form of EULA that a player must click “I agree” to be permitted to proceed into the game or world, further ensures that there are agreed-upon standards. These standards offer the company hosting the site potential recourse should players misbehave (Tseng, 2012). EULAs usually include provisions for intellectual property, virtual property, privacy, account transfer, account termination, dispute resolution, liability, warranty, as well as behavioural guidelines (Tseng, 2012).

Given that many avatars are creating stable personalities, reflective of their offline selves, and with these avatars, form relationships based on offline models of friendship, replicating standard social norms of politeness, interpersonal distance, collaboration and cooperation, reciprocal altruism, and personal self-disclosure, demonstrates the similarity of the virtual to the physical world. Interpersonal behaviours such as cooperation, collaboration, and reciprocal altruism have all developed in online worlds with attendant intimate self-disclosure and therefore it must be considered that trust can and does form and maintain in metaverses. The trust that forms in metaverses induces avatars, and the individuals behind them, to offer personal self-disclosure as well as rely on predictability for future social interactions. This helps to provide stability for the online communities but also provides nefarious individuals the opportunity to take advantage of avatar trust, in a manner similar to the offline world.

3.5. Trust in Immersive Games

3.5.1. History and reputation

Players in immersive games often play more than 20 hours per week and those who belong to guilds meet regularly (several hours per day, several days per week) to accomplish in-game feats (Tseng, 2012). In a recent study, comparing games to other forms of online play, it was determined that the immersive game "does not lend itself to the same sorts of persona abandonment because of the amount of time and effort needed to cultivate one's avatar or onscreen character" (Chen, 2005, p. 4). Indeed, history and reputation for immersive gaming is not only essential but established quickly.

In most gaming worlds, guilds or clans, of varying sizes, develop regularly (Chen, 2005; Williams et al., 2006; Smith 2010). In games such as World of Warcraft, researchers found that small guilds (10 persons or less) often had pre-existing friendships offline or moved long-running guilds into the game from other games (Williams et al., 2006). For those who are not first friends in offline space, the prevailing norms of a guild will offer indications as to the types of people who belong to it and will attract specific players, with specific traits and behaviours, who wish to be with others like them (Chen, 2005). Groups are highly identifiable by size, type, goals, and playing behavior with these qualities being particularly salient regarding cooperative play,

collaboration, and the equal distribution of rewards (Williams et al., 2006). With the transference of offline friend-groups to online play, as well as the investment necessary for successful play, it becomes fairly easy to assess trustworthiness of other avatars which provides a basis for the formation and maintenance of trust.

3.5.2. Inference Based on Personal Characteristics

Game-players, as in real life, have varying abilities to fit in and play well with others (Chen, 2005). Usually players will remain quietly in the background and learn implicit norms by observing and following the lead of other players (Williams et al., 2006). Some players do not wait and observe, rather jumping in and making social errors which may irritate other players; however in studies of social dilemmas in computer games, this has been empirically shown to be induced by pre-existing personality traits rather than the game context (Chen, 2005).

Personality characteristics matter a great deal to guilds, given that guild members must trust one another to follow agreed upon strategies for success, as well as to share equally in rewards (Yee, 2010). Surveys show that small guilds, which are built on shared ethics and bonds, tend to recruit new members only after carefully scrutinizing the potential player for the desired characteristics (Chen, 2005; Williams et al., 2006; Yee, 2010).

As in the physical world, people of all abilities and personalities are present in immersive games. Given that personalities are stable across realms and that it is an advantage for a new player to demonstrate qualities such as loyalty, honesty, and prudence, characteristics are presented in such a way that they can be examined for trustworthiness.

3.5.3. Mutuality and Reciprocity

Games such as Gauntlet and StarWars Galaxies are based on classic trust dilemmas known as the “prisoner’s dilemma” (e.g., Axelrod, 1980). Players who work cooperatively and collaboratively are much more successful than players who do not (Williams et al., 2006; Yee, 2010). Despite mutual reward for collaborative game-play, if a single player cheats then he or she stands to attain the greatest reward (Yee, 2010). The dilemma comes from the possibility that everyone might cheat and then all will lose

(Smith, 2010; Williams et al., 2006). Players operate under the shadow of the future, with ongoing cooperation necessary for success (Smith, 2010). Given that 80% of players work in guilds where reciprocal altruism is common, trust builds and is maintained (Williams et al., 2006).

3.5.4. Role fulfillment

In many games there is something known as the magic circle. This is a boundary that divides the virtual from the real; inside the circle are rules governing codes of play and conduct and outside defaults to real-world rules and laws (Tseng, 2012). This helps to specify roles and behaviours in the game including ones that are not permitted as well as resulting punishment for them (Castronova, 2004-2005; Tseng, 2012).

Guilds have clear expectations and, as previously discussed, all members contribute and cooperate and trust one another such that "the cooperative choice is to put one's *trust* in other members of the group to do the same" (Williams et al., 2006 emphasis in original). Given that "guilds are likened to extended families, social circles, and sports teams" (Chen 2005, p. 3), the fulfillment of roles is crucial to trust.

"Grief" or "white-eyed" players deliberately disrupt other player's game experience and derive enjoyment from it: "Grief players are considered the deviants in gaming societies; they break the laws (codes and rules of conduct) of their game worlds, violate the norms and etiquettes of their communities" (Lin & Sun, 2005, p. 2). The very existence of grief players, who break rules and codes of play, provides support for the existence of roles and their attendant rules of conduct.

3.5.5. Contextual Factors

Norms emerge from the rules and goals coded into multiplayer online games, heavily influencing behaviors (Lin & Sun, 2005). These determine what will and will not be tolerated by players as well as the rules of the game itself (Chen, 2005; Lin & Sun, 2005). The presence of clickwrap agreements ensures that there are consistent standards all players must agree to. As in the case of social networks and metaverses, these agreements offer the company, providing the site, a myriad of potential recourses should players misbehave (Tseng, 2012)

In games like World of Warcraft, there are norms and rules that everyone, who wishes to successfully play the game, must learn (Chen, 2005). For example, if a guild comes upon a group of monsters, it is considered fair that all the monsters are killed before any player begins looting. To "ninja loot," or loot while other players are still battling the monsters, is considered bad manners and can result in either public punishment or ejection from the guild (Chen, 2005). Norms are clearly understood by all players with violations tolerated to different degrees depending on whether the player is considered a newbie, and thus ignorant of the rules, or one who is deliberately misbehaving (Lin & Sun, 2005).

Larger guilds that form from smaller guilds require stronger rules to ensure all players work to a common end (Williams et al., 2006). In a mixed method study, guild leaders were observed rebuking or ejecting players who violated the rules (Williams et al., 2006). Rogue members cannot claim ignorance of the rules as "rules, probationary periods, and attendance policies [were] common" amongst all guilds (Williams et al., 2006, p 347). In large guilds, mission statements existed in all and were codified about 50% the time (Williams et al., 2006).

The presence of guilds with established and codified rules is probably the strongest argument for the formation and maintenance of trust in online games. Intense game-play, long hours, investment in stable avatar identities, as well as classic trust dilemmas all pushes players towards collaborative and trust filled game-play. Personal reputations draw guilds to recruit players and guilds that develop reputations for trustworthy play, attract better players resulting in greater success. The contextual factors in games promote formation and maintainance of trust.

3.6. Trust in Social Networks

Online social networks are based on the concept of staying in touch with offline friends and making new ones through connections in the network (Rosenberg & Egbert, 2011). Trust is one of the foundations for friendship (Donath & boyd, 2004; Wang et al., 2010) and given that a significant number of online friendships emerge from offline relationships, it is reasonable to assume that online trust in social networks will be based partially on historical and reputational factors (Traud, Mucha, & Porter, 2012; Wang et al., 2010). If this is true, then evidence for trust in online social networks should be

evident from behavior displayed there and systematically responsive to the same factors as trust in the physical world.

3.6.1. History and Reputation

Unless there is a deliberate effort to deceive (e.g., posting a false profile), individuals who create online profiles in social networks, will typically use their real name and photograph (Donath & boyd, 2004), linking them conclusively to their offline self. Studies using structural equation modeling, with a Facebook snowball sample, demonstrated a strong link between personality characteristics and online behaviours (Rosenberg & Egbert, 2011) in a manner similar to the way behavior and personality is linked offline. This provides strong evidence for consistency of behavior in the two realms, giving support for trust to have transferred from offline to online (Donath & boyd, 2004). Indeed, many individuals who accept friend requests claim they already knew the individual in physical space (McLaughlin & Vitak, 2011). In a study of fourth year college students, the majority claimed that they were uncomfortable accepting or offering invitations of online friendship to anyone that they hadn't personally met (McLaughlin & Vitak, 2011). Given that shared history and knowledge of reputation is one of the factors that allows for the formation and maintenance of trust, then certainty of identity, prior relationship, and knowledge of reputation must support trust in social networks.

For those who meet solely online, there are a number of ways to assess history and reputation. Reading historic postings on the individual's wall or news feed allows one to assess their interaction with others and thus assess their personal characteristics (Donath & boyd, 2004; Walther et al., 2008). In some social networks, such as LinkedIn, reputation can be assessed be reading testimonials placed on the individual's home page (Donath & boyd, 2004). Given the transparency of reputation and history in online social networks as well as their permanence and ease of accessibility, trust should emerge more rapidly in these online communities than in the physical world..

Many individuals have become aware that their reputation offline can be seriously harmed by reputation online and vice versa (Smith & Kidder, 2010). In Vancouver, Canada, news reports following the hockey riot in 2011 described individuals experiencing severe repercussions, such as job loss, related to their offline behavior when evidence of rioting was posted in online social networks (*Canadian Employment Law Today, 06.24.2011*; Fullhouse, 2011). Some individuals, having been involved in

the riot, found their photos posted on the Facebook page, "Vancouver Riot Pics: Post Your Photos" (Fullhouse, 2011), blending information from the two realms. This allowed information related to reputation and personal characteristics to easily flow between the two. As the offline and online world of social networks merge, each informs the other regarding trust and trustworthiness. Given the tendency of computer-mediated communication to magnify the meaning of messages (Walther, 2007), reputation and history online, in the formation and maintenance of trust, should be even more salient than offline.

3.6.2. Inferences Based on Personal Characteristics

Presentation and image management are important in computer-mediated communications (Walther, 2007). Given the public nature of profiles combined with the qualities of networked online communication (networks linked to networks, exponentially dispersing information), personal characteristics may be widely dispersed (Donath & boyd, 2004; Rosenberg & Egbert, 2011). Studies have demonstrated that most individuals are not only aware, but also concerned as to how they are perceived online, with qualities such as loyalty and a desire for the good opinion of other listed consistently as reasons for moderating behavior (Donath & boyd, 2004; Martey & Stromer-Gallery, 2007; Rosenberg & Egbert, 2011). The public nature of online social networks, linked with stability of personality, and a desire to be thought well of, are similar to the principles of trust offline. Indeed, the fact that your reputation and character is available to be seen by such a wide group of people (average in studies range from 150 to 500 online social network friends compared to 30 friends and 150 acquaintances in physical space) indicates that those wanting to be thought well of and who are using online social networks would be highly concerned about behaviours construed as untrustworthy in this realm (Smith & Kidder, 2010; Wang et al., 2010).

Estimates of character may also be taken from online friends of the individual one is assessing. Many social networks allow viewers to not only see the postings on their friend's wall/news feed, but also those on the friends of the friend (Donath & boyd, 2004; Smith & Kidder, 2010). Given the tight link between online and offline personality characteristics, the crossover from offline to online of friendships, and that trustworthy individuals tend to associate with those who are also trustworthy, assessing the personal

characteristics of friends online all facilitate character assessment and increase the likelihood of trust forming and being maintained online.

3.6.3. Mutuality and Reciprocity

The norms of politeness, mutuality, and reciprocity, established in physical world groups, guides interactions amongst members in online social networks as well (Baym, 1998 cited in McLaughlin & Vitak, 2011). Findings from Facebook server-level data, demonstrate that people learn the norms of content sharing by observing the habits of their online friends (Burke et al., 2009 as cited in McLaughlin & Vitak, 2011). Focus groups stated that they were highly considerate of their online friends and all were aware that reputation was to be taken seriously on social network sites with violations of privacy or social rules, such as inappropriately tagging an unflattering photo or publishing an obnoxious post, would be responded to by untagging, deleting the post, hiding the friend, or, in extreme cases, de-friending them (McLaughlin & Vitak, 2011).

3.6.4. Role Fulfillment

Given that users will refer to other users' profiles and postings to determine what is appropriate in social networks demonstrates that there are certain expected roles that play out in these online spaces (McLaughlin & Vitak, 2011). Accepted behaviours on social networks are generally implicit, yet easily learned by observing friends' behaviours and examining past histories, when new to the network (McLaughlin & Vitak, 2011). While there are no formalized roles, it is clear that *friend* is the implicit role everyone takes in social networking sites. Trust is an inherent aspect of friendship and therefore, the role of friend on social networks should not only induce trust but should maintain it.

3.6.5. Contextual Factors

Netiquette, the established set of social norms (customs, standards, rules, values, fashions etc. (Sherif, 1936 as cited in Meyers & Spencer, 2006)) all help to guide users' behavior in online social networks (McLaughlin & Vitak, 2011). As well, these sites have terms of service agreements (ToS) that spell out appropriate use and unacceptable content guidelines that all must agree to (Tseng, 2010). Violations of formal terms and conditions may result in sanctions, from admonishment to the

suspension of an account (Burnett & Boninici, 2003 as cited in McLaughlin & Vitak, 2011).

The context of the social network itself mediates most behavior because there is a wider audience than one normally must deal with, it is perpetual and accessible by friends, as well as friends of friends, that friends will offer punishment and reward if postings or behaviours violate the norms or are exceptional in some way, and a demonstrated similarity of behavior online to offline (Martey & Stromer-Galley, 2007; Smith & Kidder, 2010). Many college students claimed that if they saw something inappropriate on a friend's wall/news feed they would notify them personally and privately to give them the opportunity to remove it (McLaughlin & Vitak, 2011). This behavior demonstrates not only vigilance in monitoring one's own space, but also in monitoring the spaces of others, demonstrating respect, mutuality, as well as overt acknowledgement that there are expected levels of politeness and decorum in these online social spaces. Given that numerous researchers have found college admissions offices (Hechinger, 2008 as cited in in McLaughlin & Vitak, 2011) as well as employers (Palank, 2006; Zeidner, 2007 as cited in Smith & Kidder) check social network sites to help in assessing suitability of applicants, demonstrates that the online social spaces are used an extension of offline, not only for the purpose of making and maintaining friendships, but to assess character and potentially trustworthiness.

The role of online social networks is an extension and expansion of offline social networks. The crossing over of friends from offline to online, the stability of personality characteristics in both realms, mutual and reciprocal behaviours, including monitoring for violations of established overt and implicit norms, all demonstrate that online social networks function in a manner similar to those in offline space and therefore should support both the formation and the growth of trust for those using them.

Online social spaces do support the formation and maintenance of trust; however, these very same factors allow for violations of trust that are all the more harmful because of the breach of trust they involve. While the principles of trust are clearly exhibited in online social spaces and helpful in making a determination as to who is and who is not trustworthy, those who wish to deceive can mimic reputation, personal characteristics, mutuality, reciprocity, role fulfillment, and contextual factors.

The combination of online social places, that are perceived as real, together with meaningful personal representations that form and maintain trust, in these spaces,

combines to make online social spaces as significant and meaningful as physical life social spaces. The unique qualities of the Internet, including permanence of communication, dispersal of information, anonymity, affordability, and accessibility, also combine to make the Internet a particularly attractive social space with access to a greater number of people and experiences than can be sustained in physical life. Unfortunately, these same qualities allow those with less than honourable intentions to obscure identity and perpetrate behaviours that, if perpetrated in physical space, would be considered deviant, if not criminal.

The following chapter explores a number of cases in which the unique characteristics of the Internet, including anonymity, accessibility, affordability, the perceived reality of place and person, in combination with online trust, all led to violent victimizations resulting in real harm to real people.

4. Virtual Violent Victimization

With the increase in individuals using online social media, games and immersive worlds, and the development of trust in these sites, the opportunities for deviant behaviour increases along with the potential for serious harm to victims. Currently, North American society and courts have yet to consistently react to acts of online violence. Some have defined acts that occur in cyberspace as "unreal" and therefore, not meaningful or criminal while others have defined these acts as highly significant and argue for a strong legislative response (Balkin, 2004; Castronova, 2004-2005; Franks, 2011; Lastowka & Hunter 2004; Lastowka & Hunter 2004-2005; Smyth 2009-2010; Tseng, 2011). While virtual property has begun to be accepted as holding real value (Kennedy, 2010; Lim, 2010), the prevalent attitude towards the violent victimization of an avatar or socially represented persona in cyberspace is to devalue the extent of the loss experienced by the creator (Wolfendale, 2007). Yet, when individuals report their experiences online as real or more real than those experienced in the physical world, it becomes clear that unwelcome acts of virtual violence do have the ability to cause (or bring about) harm with lasting consequences (Dibbell, 1993; Reid, 1999). Therefore, it is understandable that individuals, when violently attacked in these spaces, may feel violated in a manner similar to violent attacks in physical space.

The following section examines online events in which the behaviours, as seen by the victims and others, were considered not only morally wrong but also, if they had been perpetrated in offline space, would be judged criminal. Various cases, in which virtual assaults take place, are examined and using the *Canadian Criminal Code* analyzed for the potential application of existing Canadian law. While some of these cases occurred in jurisdictions other than Canada and, as a result, other legislation would apply, for the purposes of this thesis, the *Canadian Criminal Code* was chosen as a way to be consistent in the analysis of the cases to explore and apply physical space law to the virtual realm.

Beginning with the first known case of cyber rape (Dibbell, 1993), an assortment of other cases, demonstrating a variety of virtual violent acts will be examined. Some of these cases have been prosecuted or are in the process of being prosecuted while others are not. The examination of these cases will be followed by an explanation for these behaviours through the application of current criminological theories. Recommendations for the use of existing legislation and a suggestion for a single new piece of legislation, to clearly demarcate the Internet as an extension and expansion of our physical lives as separate from the fantasy world of gameplay, will be offered.

4.1. Rape

Julian Dibbell, in1993, reported the first widely publicized case of virtual rape in the text-based community of LambdaMOO. LambdaMOO was constructed as a large, rustic chateau, communally imagined by its 1,500 participants. The event, referred to by community members as a rape, occurred in the living room – a large, inviting room that was packed with community members who were visiting and chatting at the time of the offence. According to Dibbell, "a cruel mind could hardly imagine a better place in which to stage a violation of LambdaMOO's communal spirit" (Dibbell, 1993, p. 472).

Mr. Bungle, a character created by a New York university student, appeared in LambdaMOO as a "fat, oleaginous, Bisquick-faced clown" (Dibbell, 1993, p. 472). By use of a subprogram he was able to attribute actions to other characters they did not write (p. 475). Bungle first impersonated, "legba, a Haitian trickster spirit of indeterminate gender" (p. 473), a character created by a woman in Seattle. Bungle wrote her character as sexually servicing his character (p. 473). The real legba responded by heaping "vicious imprecations" (p. 473) on him though she could not stop him from continuing to write commentary as though it was coming from her character. Soon other individuals ejected him from the "room." This should have prevented Bungle from continuing, as LambdaMOO's program was coded in a manner that requires a character to be present in a room to see the written output of other characters (p. 474) but, despite no longer appearing to be in the same room, Bungle was able to continue his attack.

Bungle then impersonated a second character, Starsinger, a "non-descript female character", created by a woman in Pennsylvania, and forced her into unwanted

liaisons with other characters in the room (Dibbell, 1993, p. 473). Under Bungle's control, the actions of the two characters, he had taken control of, became increasingly violent. He made legba eat his/her own pubic hair and forced Starsinger to "jab a steak knife up her ass causing immense joy" (p. 475) all the while laughing "evilly" from the adjacent room (p. 473). Eventually, someone summoned a "wizard" ("master programmers of the MOO") (p. 478) who disabled Bungle's ability to use the malicious code and the violation ceased (p. 473).

The resulting discussions by the community members of LambdaMOO not only concluded that the actions of Mr. Bungle were, indeed rape, but also, by these very public actions, had violated the community standards as much as the individuals targeted (Dibbell, 1993, p. 472). legba, who had deliberately constructed a genderless character, was devastated by the attack (p. 475). The evening following the online assault she wrote:

> I also think that Mr. Bungle was being a vicious, vile fuckhead, and I…want his sorry ass scattered from #17 to the Cinder Pile. I'm not calling for policies, trials, or better jails. I'm not sure what I'm calling for. Virtual castration, if I could manage it. Mostly, [this type of thing] doesn't happen here. Mostly, perhaps I thought it wouldn't happen to me. Mostly, I trust people to conduct themselves with some veneer of civility (p. 475).

Months later, the woman who had written the character of legba, divulged that as she was writing those words "posttraumatic tears were streaming down her face" (p. 475). This violation was most likely bound up in several factors including the anti-social behavior of Mr. Bungle, the public violation of her character, the humiliation of having the attack witnessed, the violation of community standards, and the importance and meaning of language, especially in a text-based community, giving permanence to the record allowing anyone to go back and peruse it, ensuring continued violations.

While the "rape" in LambdaMOO was the first reported, there have been numerous instances of online sexual violence reported since (Barry, 2009; Chisholm, 2006; Huff, Johnson, & Miller, 2003). Adolescent and college-aged females are commonly targets of online violence (Arnold, 1998; Chisholm, 2006) as are those who join online communities for the purpose of support (Reid, 1999). One of the most

disturbing cases of virtual rape occurred in an online support community, for survivors of childhood sexual assault, called JennyMUSH (Reid, 1999).

JennyMUSH had been designed and was administrated by a psychology graduate student whose field of interest was survivors of sexual assault and abuse (Reid, 1999). The university she attended officially supported the JennyMUSH project ensuring a degree of security of existence for those in the online community. Survivors of sexual abuse, especially those who sustained the abuse in childhood, at the hands of their fathers, often find it difficult to trust and need stability in their communities of support (Kreidler, 2005). The JennyMUSH community was one of delicate balance, striving to provide support for the participants while at the same time addressing issues of posttraumatic stress disorder, depression, anxiety, low self-esteem, sexual dysfunction, self-abusive behaviours, substance abuse, eating disorders, and high suicide attempt rates (14 – 19 times higher than women in the general population), all of which are commonly found in adult survivors of childhood sexual abuse (Gorey, Richter, & Schnider, 2001). JennyMUSH was experimental as an online support community and supervised carefully by the student, the university administrators, and the student's supervisors to ensure it provided the necessary support for its members (Reid, 1999). Despite the careful supervision of the site, a single person, using technical and social means, was able to commit a virtual rape of all its members (Reid, 1999).

Two weeks after being admitted to the community and assigned a character, a member of the support group used the MUD's commands to transform him or herself "into the virtual manifestation of the other user's fears" (Reid, 1999, p. 115). The user changed his or her name to "Daddy" and then using the shout command, sent messages community-wide. In these messages he or she described sexual assaults in "graphic and violent" language (Reid, 1999, p. 115). When the assault began, neither the administrators nor university supervisors were online. This may have been deliberately planned, as the administrator and supervisors maintained regularly scheduled online hours to ensure that survivors had support when expected. For over an hour, obscene messages were sent to all community members. Some members logged off while others transported themselves to the same locale as the abuser and urged him or her to cease the violation (Reid, 1999). When begging failed, some members resorted to threats but failed to stop the assault due to a general lack of knowledge and understanding of how to mute the offending member (Reid, 1999).

At the end of the hour, one wizard logged on and found a dozen of the community members in a single room, eleven of whom were being "obscenely taunted" by the twelfth (Reid, 1999, p. 115). The wizard took control of the user's virtual manifestation, gagged him or her and changed his or her description to read, "this is the lowest scum, the most pathetic dismal object which a human being can become" (Reid, 1999, p. 116). At this point, those present took retribution resulting in "virtual carnage" (Reid, 1999, p. 116). Together, they described violent punishments they would like to enact on him or her, emoting hatred, rage, and frustration (Reid, 1999).

As a result of the attack, the community radically changed from one of mutual support and sharing to a much more constricted and restrictive environment. New users had to be vouched for by existing members, instructions on how to gag others was part of the required reading before being allowed to enter, the shout command was disabled, making it much more cumbersome to contact all members, and all members had to provide the supervisor with their personal telephone number and legal name (Reid, 1999).

The short- and long-term effects of this assault are not known as emotional and psychological effects on the community members were possibly not recorded, but certainly not published. The administrator stated, "We spent so much time trying to make JennyMUSH a place where people could feel free to speak out – we provided anonymity and very few restrictions. Sadly, we didn't foresee the negative aspects such encouragement could have….freedom to…became freedom from" (Reid, 1999, p. 117). As a result, the society and support group became a rigid and restrictive one with a strict hierarchy of rules and privileges.

The members of LambdaMoo and JennyMUSH determined rape had occurred not based on the application of a criminal definition of rape, but on a social construction of rape, as these communities understood it. Although the legal definition of rape varies from jurisdiction to jurisdiction, in Canada it is referred to as "sexual assault" and is defined under the assault section of the *Criminal Code*, ss. 265. (1) (a) (b) (c) and s. 265. (2). Assault occurs when one individual "intentionally applies", or "threatens to apply, force" to another person "without their consent" or openly "carries a weapon" and accosts or impedes another person (see Appendix A). This section includes "sexual assault, aggravated sexual assault, sexual assault with a weapon, and threats to a third party or causing bodily harm." Canada's sexual assault law is radically different from the

rape law drafted by the United Nations, which defines rape as "a physical invasion of a sexual nature, committed on a person under circumstances which are coercive. Sexual violence, including rape, is not limited to physical invasion of the human body and may include acts which do not involve penetration or even physical contact" (United Nations, 1998). Rape, as defined through rape crisis centres, also tends to vary quite widely from the *Criminal Code.* Vancouver Rape Crisis Centre (2012) defines rape as "forced or nonconsensual sexual contact including unwanted vaginal, anal or oral penetration, groping/touching your body and forced kissing." The widely differing definitions of rape demonstrate the radically different interpretations that can be applied to this crime and may help to explain why the individuals in both LambdaMOO and JennyMUSH might refer to their different experiences by the same name.

There are a number of problems in attempting to apply Canada's existing sexual assault legislation to cyber rape. Even though the events that occurred in LambdaMOO and JennyMUSH are clearly assaults of a sexual nature, resulting in serious emotional harm to the victims, under current legislation in Canada (s. 265 of the *Criminal Code*), they do not qualify as a sexual assault. The crime of sexual assault requires two human beings, a perpetrator and a victim, and direct physical force of a sexual nature. If there is no direct physical force applied then the threat of force may qualify as an assault, but only if the victim perceives that the perpetrator has the means by which to carry out the assault.

The definition of sexual assault in Canada's *Criminal Code*, (s. 265. (2)), does not allow for text-based characters, written by human beings (avatars), to qualify as "persons" in the eyes of the law. This is so even if the avatar is based on a close parallel to the real, physical, human being. The reason for this is because, in Canada, a text-based representation is not a person. Personhood is limited to those who are human beings (as determined from definitions in the *Canadian Criminal Code* of "homicide", s. 222, and "when a child becomes a human being", s. 223). The crime of cyber rape is, however, one of a serious nature. It violates, in a violent manner, the sexual integrity of its victims, and may result in real emotional and psychic harm to real humans, as demonstrated by the reactions of the victims in LambdaMOO and JennyMUSH. These attacks do, nevertheless, meet most of the remaining criteria of criminal assault, including threat, application of force, and lack of consent (*Canadian Criminal Code* s. 265). Therefore, if Canada were to apply its existing sexual assault legislation to acts of

cyber rape, new legislation or a new test would have to be created to account for personal representations, in the form of avatars that hold quasi-human status.

Based on the definition of *quasi*, an avatar that would take on the status of quasi-human being would be an entity, similar to, or resembling a human being, one that is nearly human or, in part, human. There are certainly a range of arguments that could be made in favour of granting personal representations in the form of avatars the status of being quasi-human, including the cognitive and perceptual manner in which they are viewed by their creators, the significance they hold for their creators, the tendency to reference them with the personal pronoun, "I" the tendency of creators and those who interact with them to assign them sentience, as well as others. However, these arguments are beyond the scope of this thesis and will require thoughtful and reasoned argument by Canada's legislators.

The second hurdle to overcome in applying current assault legislation to cyber rape is found in s. 265 (1)(b), the belief that the individual perpetrating the assault has "the present ability to effect his purpose." In common law and Canada's criminal law, assault may occur when there has been no actual physical assault but solely the threat of applying force of a sexual nature. According to Canada's *Criminal Code* s. 265(1)(b), the threat by "act or gesture" is sufficient for a charge of sexual assault as long as the potential victim believes, "on reasonable grounds that he [the perpetrator] has, present ability to effect his purpose." Therefore, crimes of sexual assault, occurring in cyberspace, could be dealt with through criminal charges or civil lawsuits, using existing legislation. Application of existing legislation (s. 265) would require avatars to be considered quasi-human beings, the content of the message containing threat of sexual assault, and the victim experiencing genuine fear of the perpetrator's ability to follow through and commit the crime. The stumbling point for the legislation would then be the interpretation of the clause, "present ability to effect his purpose." This clause requires, at the moment of receiving the threat, for the victim to make an assessment of the physical location of the person making the threat and to further assess whether this individual does, indeed, have the ability to effect their purpose of assault. This may be an unsurpassable hurdle for our victims and courts to overcome in pursuit of using current sexual assault legislation to prosecute crimes of cyber rape.

In Canada's assault legislation there is no requirement for a minimum level of physical harm to be sustained, nor any level of physical harm at all required. Courts,

over the last few decades, have shown a willingness to take into account the emotional and psychic harm of victims of violent assault whether or not they sustained physical injury (Urbas, G., personal communication, July 15, 2012). In *R. v. Hau*, (1996), the judge, J. Edwards, determined that the complainant (victim) need not suffer or fear they would suffer physical harm. It was considered sufficient that the complainant genuinely experienced fear and, as a result, sustained psychological or emotional harm. This case, however, dealt with harassment (s. 264 *Criminal Code*) and not with assault or sexual assault (s. 265 *Criminal Code*).

In addition to the requirement for the victim to be a human being, and to genuinely believe that the perpetrator has the means by which to commit the threatened assaultive act, in Canada and the United States, there are two essential requirements for any crime to have occurred: *actus reus* and *mens rea*. *Actus reus* is the act of doing something, and *mens rea* is the guilty intent (Adrian, 2010; Griffiths, 2007). The crime of sexual assault requires both; however, the crime of harassment does not require *actus reus*, it simply requires *mens rea* (e.g., *R. v. Hau* (1996)). Further, the intent, on the part of the perpetrator need not be that the victim feels genuine threat, but simply, that they have been reckless in their behaviour such that it results in the victim feeling genuinely threatened, "The accused must know that his attentions are unwelcome and be reckless as to the effect that he is having on the complainant. Thus, the complainant need only fear psychological or emotional harm from the harassment (J.A. J. Edwards, *R. v. Hau*, (1996))

The behavior of "Mr. Bungle" and "Daddy" may only qualify as a sexual assault or rape if one uses a social construction of rape or, alternately, views cyber rape as a blend of sexual harassment and sexual assault, or views cyber rape as a type of community violation. Applying a social construction of rape, in the manner that has been done by the United Nations and the Vancouver Rape Crisis Centre, reduces the requirements for rape to a violation of an individual's sexual integrity. The constructions of what is and is not a crime develop or evolve naturally within communities and cultures based on codes, mores, and folkways (Griffiths, 2007). The social construction of rape depends on the cultural context in which it occurs and the interpretation of the acts involved (MacKinnon, 2006). Feminist theories of rape include damage that is physical, emotional, psychological, or material in nature, and thus, the violation can be of the body or the mind, or even, trust, provided a definition that allows for virtual rape or sexual assault

(Kelly, 1988 as cited in MacKinnon, 2006). Therefore, in the case of “Mr. Bungle” and “Daddy”, it was not only “legba” and “Starsinger” and the unnamed eleven individuals in JennyMUSH who were violently attacked, but also the very real women behind them. This provides one explanation for the posttraumatic stress effects that “legba” reported and the “virtual carnage” the JennyMush members unleashed in their virtual revenge.

Those in LambdaMOO believed in its veracity as a real community (Dibbell, 1993, p. 472). The descriptions of the rooms and those in it provided a “lucid illusion of presence” (Dibbell, 1993, p. 474), increasing the sense of reality. Therefore, actions that occurred within this community would have real significance and, as a result, real psychological effects for those who either sustained or witnessed them. This was supported by the fact that when it was suggested that Mr. Bungle be toaded there was strong support from some of the community (p. 478). The resulting arguments that raged on the social forums of LambdaMOO fell into two categories that Dibbell (1993) labeled: parliamentarians, who argued for the establishment of rules, judiciary, and prisons and/or the return of a ruling wizard class in the MOO and technolibertarians, who argued that the presence of Bungle-types, who abused their freedom of speech, were an unfortunate hazard of the system and could be controlled through code such using the “@gag” command that prevents you from seeing what someone else texts (p. 479-80). During a subsequent meeting of community members, the application of physical world remedies, such as applying California state laws regarding obscene phone calls or having Bungle’s university administrators punish him for sexual harassment were considered and rejected. Not because they didn’t think his actions were serious, but rather, they believed a crime in a MOO should be dealt with in the MOO. The community reached no consensus and a single wizard, acting alone, toaded Mr. Bungle, removing him permanently from the MOO (p. 484-5).

In the case of JennyMUSH, it is unknown if any legal remedies were considered. Certainly changes were made to the system to ensure individuals such as “Daddy” would not be able to join the community and members were trained to gag offensive messages (Reid, 1999). The reaction of the administrators, providing a gag command, does not stop the offensive behavior but simply prevents other members from receiving the message. Dibbell and others refer to those advocating the use of gag commands for virtual rape as the “gag-it-and-get-over-it” school of thought (Dibbell, 1993; Lynn, 2007). As stated, this approach fails to take into account the damage perpetrated prior to the

gag command taking effect. Language holds real meaning for those experiencing it. Online text-based communities are meaningful because the power of speech acts as embodying both illocutionary force (intentional acts) and perlocutionary force (social effects and significance) which make language-based interactions online similar in nature to those in the physical world (Powers, 2003). This imbues theses acts with legitimate moral expectations and significant meaning (Powers, 2003).

It is between freedom of speech and freedom of security of person that tension emerges in virtual communities over events such as virtual rape. In Canada and the United States, the individual's right to freedom of speech is enshrined (see s. 2 (b) of the *Canadian Charter of Rights and Freedoms* and the First Amendment of the *United States Bill of Rights*). Further, every citizen also enjoys the right to freedom from unwanted assault (see s. 7 in the *Canadian Charter of Rights and Freedoms* and the Fourth Amendment of the *United States Bill of Rights*). Freedom of speech means being permitted to state one's opinion, truth, or beliefs; however, having to listen to or read rape-text denies the liberty and security of the self, as well as the right to freedom from harassment, and places responsibility for virtual rape on the victim. These two rights clash in situations such as LambdaMOO and JennyMUSH.

Part of the appeal of virtual worlds is the feeling of freedom they offer users which allows them to interact with others as well as shape their environment. Restrictions on avatar freedom and power may undermine the allure of the virtual environment (Hunter & Lastowka, 2003). For individuals who, in the physical world experience a lack of freedom, the online environment can be an attractive world of adventure, intimacy, and experimentation (Chisholm, 2006).

Those who do not understand the attachment to the avatar or other online representations of the self and the immersion that occurs in virtual worlds and games take the position that players or community members should avoid the possibility of victimization by opting out if they don't like how the game-play goes or the messages they are receiving. Unfortunately, this nullifies the legitimacy of their victimization (Kenney, 2010). We would never tell someone who had been physically assaulted that they should just opt out of whatever activity they'd been immersed in when the assault took place.

While Rape Crisis centres are setting up virtual offices in metaverses like Second Life, in the attempt to help victims of virtual sexual assault deal with their emotional and

psychological reactions, the biggest concern for those working with sex abuse victims is that these online behaviours are grooming both victims and perpetrators for physical world crime (Barry, 2009). A counselor with Rape Crisis Scotland stated, "The fact is what they are doing in this fantasy world is normalizing behavior such as child abuse and rape and validating it…anyone who works with sex offenders recognizes this" (Barry, 2009). In Second Life, there are cafes dedicated to rape, rooms in which you can either hold down the victim or perpetrate the rape, a human torture room, human slave trafficking mansion, and a school where pupils can be sexually abused (Howie, 2009). Activities such as these are legal for those of consenting age. The problem is that, despite a separate teen grid, given Linden Lab's reduced security (users no longer have to provide a credit card to register an account), teens can easily create adult characters and show up on the main grid. Unless they explicitly tell someone their age and are reported to Linden Labs the likelihood of being removed is exceptionally low.

A further problem is found in the use of the metaverse. For those using it as an extension and augmentation of their day-to-day physical life, rape cafes and torture rooms do not belong; however, for those using the metaverse more akin to an online game, these spaces may represent fantastical play spaces where physical world rules and laws do not apply. This is one of the problems that can be clearly dealt with through the adoption of a law of interration (Castronova, 2004-2005) and the drawing of a magic circle to determine which spaces online are fantastical play spaces and which are extensions of physical world life (see section 4.2 and 5.3 of this thesis for a full explanation and application of a law of interration).

If virtual rape results in serious emotional and psychological damage for the victim and breaks down online communities, and online sexually abusive behaviours potentially groom individuals to commit offline sexual offenses or to become victims, and children and adolescents are at risk of virtual sexual assault and code-based responses will not prevent victimization but, rather, place the responsibility in the hands of the victim to protect themselves, then the act of virtual rape must be considered as a serious violation of the person as well as community standards and legal remedies must be made available.

There have been no prosecutions in Canada under s. 265. (2) of the *Criminal Code* (as searched in Criminal Source) for sexual assault perpetrated on the Internet. In addition to the prior listed reasons: failure of being human, uncertainty in relation to

perpetrator being able to effect action, and application of a social construction of rape compared to criminal definition, there may also simply be no appetite to prosecute under a section of the *Criminal Code* that was written to deal with serious, physical assault for an act that appears radically dissimilar to a physical sexual assault (DeKeseredy, Ellis, & Alvi, 2005). For many, sexual assault may not properly represent the act of a written or visual, virtual, sexual violation during which no bodies touch and the likelihood of physical harm seems remote. While it is recognized the both cognitively and perceptually, words can be very hurtful, nevertheless they cannot be considered crimes of the body.

Crime is both defined through legislation and our understanding of the physical world. Changes in technology, such as we've seen with the Internet, cause changes in people's behavior that, in turn, cause changes in community norms and rules. Changes such as these may render some laws unenforceable or rarely enforced due to changes in lifestyles of the citizenry. Other laws may require modification to be able to adequately deal with emerging or new behaviours caused by the technological changes. North America is at this stage. The Internet has caused radical shifts in the behaviours of those in Canada and the United States. 20 years ago, the thought of having to determine the value of quasi-humans as relates to criminal law and the similarities and differences between a physical world rape and a virtual rape were unthought-of, while today we wrestle with this and more.

Behaviours, such as were perpetrated in LambdaMOO and JennyMUSH, will be significantly difficult to prosecute under current Canadian legislation unless changes are made to more closely match the definition provided by the United Nations International Law (1998) which includes "a physical invasion of a sexual nature" not limited to "physical contact". It is not my recommendation that Canada change its legislation regarding sexual assault for several reasons. First, Canada has revisited its sexual assault legislation several times (see R.S.C. 1985, c. 19 (3rd Supp.), s. 10; 1994, c. 44, s. 19) in its attempts to provide a law that adequately captures the sexually violent and assaultive behaviours it deems criminal; second, our law is built upon both legislation and precedent, both of which would have to be discarded should we radically change our laws; and third, our law reflects the standards of our country as a community. Further, the United Nations rape law was specifically drafted in response to sexual assault as connected to acts of genocide and provides such a wide definition that it is

certain to give rise to a plethora of lawsuits in an effort to categorize and define the act which this author considers unnecessary given the adequate nature of our current sexual assault laws. Given that Canada has successfully used its existing legislation and precedent to prosecute acts of physical world sexual assault, I suggest that it remains as is.

While those in LambdaMOO claimed that they wished for the punishment to be dealt with within the virtual world, others, such as those in JennyMUSH may wish to have their experience recognized by the outside world and the legal system. There is no doubt that the acts perpetrated were serious violations of community standards, a violation of the sexual integrity of the victims, and that the individuals in each case were emotionally harmed. Yet, even those in LambdaMOO, who were victimized, recognized that virtual rape is both like and unlike physical world rape. In their case, no consensus as to how to deal with the offender could be reached and a wizard determined the punishment on his own. Relying solely on a single individual, who may or may not understand the gravity of the event, is also not the ideal solution.. Individuals who are harmed in this manner must be able to rely on a fair, impartial legal system in which the laws are written clearly and applied consistently and equally to all (Griffiths, 2007).

Given that rape is a violent act and one that violates the victim as well as causes long-term humiliation, depression, anxiety, fear, and stress (Biegel, 1985), other victims may feel that they would like their victimization to be recognized by the judicial system in the physical world and wish to report it. In that case, online acts of sexual violence such as experienced in LambdaMOO and JennyMUSH may be recognized as threatening but not containing the inherent qualities of physical rape and as such, better suited for prosecution under Canada's harassment laws, s. 264. (1) (see Appendix B) of the *Criminal Code.* Section 264. (1)) which allows for written communications that threaten or sexually threaten others, causing them to fear for their safety or the safety of others. This is discussed in detail in below.

4.2. Harassment and Stalking

Harassment, as defined in the *Criminal Code* falls under s. 264. (1) and (2), and states that, "no person shall, without lawful authority harass or recklessly behave in a manner that harasses another by, engaging in conduct such as repeatedly following,

communicating, watching, or other threatening conduct that causes the other person to reasonably fear for their safety or the safety of anyone known to them".

Stalking is also prosecuted under the same *Criminal Code* section in Canada and can be defined as a constellation of behaviours involving willful, malicious, repeated and persistent attempts to impose on another person unwanted communication and/or contact causing a degree of fear or trepidation (Mullen et al., 1999, Goode, 1995 and Gothard, 1995 as cited in *Criminology Research Council,* 2000). Like rape, this is not an agreed-upon definition, nor is it used consistently by the varying law enforcement agencies within the United States or in other countries such as Canada (United States Department of Justice*,* 2009).

Cyber-stalking is now recognized by a number of jurisdictions, including Canada and the majority of the American states, with definitions taken from traditional definitions of stalking (Department of Justice, Canada, 2011). Canada has yet to modify the *Criminal Code*, s. 264, to ensure that electronic communications are included in the law of harassment, but over the past decade the courts have shown a willingness to accept Internet communications as one of the ways in which a person may harass another (e.g., *R. v. Moss*, (2011); *R v. Labrentz* (2010); and *R. v. Basha* (2002)). In American jurisdictions, where they have changed the laws to include the Internet as a form of communication used for the purpose of harassment, minor changes in existing legislation to include the word, "Internet" or "electronic communications" were sufficient without having to further define the behaviours (e.g., *Attorney General Janet Reno's Report to the Vice President in* 1999, United States Department of Justice, 1999). In Canada, there is a proposed amendment to s. 264 of the *Criminal Code*, Bill C-273, *An Act to Amend the Criminal Code, Cyberbullying.* The proposed change states, "For greater certainty, paragraphs (2)(b) and (d) apply in respect of conduct that is communicated by means of a computer or a group of interconnected or related computers, including the Internet, or any similar means of communication." The proposed change to existing legislation is not unusual for Canada as Canada's laws can be amended and changed in three ways: legislative change, which formally codifies new laws; changes to existing laws, achieved through amending existing laws; and precedent, which changes laws through new interpretations and applications of existing legislation and past precedents (Griffiths, 2007). In this way, Canada's justice system is

able to flexibly respond to changes in society norms and standards and reflect these changes in the application of the law.

Section 264 of Canada's *Criminal Code* also includes "Uttering threats". These include threats of "death or bodily harm", as well as the threat to destroy "real or personal property" and "kill or harm" animals (*Criminal Code,* s. 264.1 (1)(a), (b), (c)). Threats may occur singly or consist of "repeated conduct that is carried out over a period of time and that causes victims to reasonably fear for their safety but does not necessarily result in physical injury. It may be a precursor to subsequent violent acts" (Department of Justice Canada, 2011). An alternate section of the *Criminal Code* that may be used, depending on the content of the messages, is s. 423. (1) "Intimidation". Intimidation is an indictable offence liable to a similar prison term (five years) as harassment and uttering threats, and includes the use of "violence or threat of violence" against an individual such that they are "intimidated " by the threat of "violence or other injury" to themselves or someone they know or damage to their property. In the case of intimidation, the prosecutor (the crown's representative) would have to prove, beyond a reasonable doubt, the victim genuinely feared this violence or threat of violence and believed that it could be carried out.

There are a large number of reported cases in North America of online stalking and harassment that have yet to be prosecuted but which have been reported in popular media and news sources as well as several that have been successfully prosecuted. The following section will examine two cases of online harassment for the purpose of demonstrating the breadth that online harassment and stalking may encompass followed by several examples from Canadian case law that will be examined for the application of s. 264 of the *Criminal Code* to incidents of cyber harassment and cyber stalking. The LambdaMOO and JennyMUSH cases will be re-examined using s. 264 of the *Criminal Code*.

In 2007, a young woman, with a paid commercial presence on YouTube (a YouTube Partner), Stickam, LinkedIn, and MySpace experienced harassment via reply postings to her YouTube videos. Applemilk1988, whose real name is Emily Connor, came to the attention of 4chan, and th /b/ forum for the content and style of her videos (Encyclopedia Dramatica, 2012). 4chan and /b/ are notorious for their influence on Internet culture and media coverage of their offline activities under the guise of Anonymous (see denial of service attacks against Mastercard, PayPal, and presence at

protests such as Occupy Wall Street) (Bakioglu, 2004; Bernstein, Monroy-Hernandez, Harry, Andre, Panovich, & Vargas, 2010).

Subsequent to those on /b/ noticing Applemilk1988, a notice was posted on the /b/ message board to commence attack on Connor (Encyclopedia Dramatica, 2012). The Patriotic Nigras, one of the anonymous, loosely formed sub-groups that exist within 4chan, commenced an organized harassment of Connor on all online social networks and forums in which she had a presence (Dibbell, 2008; Encyclopedia Dramatica, 2012). The harassment began on a single site, YouTube, and over a period of several weeks her account was bombarded with messages (i.e. flamed). The Patriotic Nigras first commenced a distributed denial of service attack by creating so much traffic on her YouTube channel that it began to interfere with other channels due to the amount of bandwidth they were using. The goal of a denial of service attack is to create sufficient traffic to a single site that it slows down the server, preventing legitimate users from accessing the site. The Patriotic Nigras were successful in this first attack, rendering Connor's channel unusable by regular viewers as her videos were loading so slowly that the images were rendered unwatchable.

Several weeks later, the Patriotic Nigras launched their second attack. Using highly offensive imagery of a sexual nature and comments that threatened not only her but her family and friends, including racial slurs and sexually abusive language, the Patriotic Nigras (the group that takes credit for the harassment) posted so much offensive content that YouTube, in defense of their appropriate use policy, was forced to close her account (see, suspended account for Applemilk1988, at http://www.youtube.com/ user/applemilk1988).

Connor posted a response on */b/* that, in turn, incited a further call for harassment on the same message board (Encyclopedia Dramatica, 2012). Members were asked to attack Connor's Internet webpages "AT FULL FORCE", a request that asks all available members on the forum to focus on a single target (Dibbell, 2009; The Free Dictionary, 2012). Connor's MySpace, LinkedIn, and Stickam accounts were then hacked and altered images of her, unclothed and posed next to an assortment of offensive sexual imagery, including erect penises and used condoms, were posted on the sites as though by her. Her home address, personal phone number, social security number, blood type, personal passwords to her online accounts, and body measurements, along with her father's name, place of work and mother's address were

all published in the /b/ forum and on her personal webpages (Encyclopedia Dramatica, 2012). Connor closed all her accounts and disappeared from the Internet leaving behind a brief video explaining her withdrawal (this has also been subsequently removed). All searches for Emily Connor, Applemilk1988, or variations thereof, on Google either bring up her closed accounts or are linked to Encyclopedia Dramatica's wiki page on Connor. Connor, in the words of those who author Encyclopedia Dramatica, has "flamed out." .To flame out is the term used to describe a woman who has withdrawn from the Internet as a result of violence inflicted on her by a team effort.. According to Scott, Semmens and Willoughby (2010) flaming out "highlights the fact that the use of male violence to victimize women and children, to control women's behavior, or to exclude women from public spaces entirely, can be extended into the new public spaces of the Internet" (p. 549).

The closing of Connor's accounts caused her to suffer real monetary damage at the time of the attacks as well as her potential earnings as an identified performing personality. As a rising YouTube star, Connor's value as a performer was closely linked to the personality she presented in her videos. The popularity, and thus monetary value, of YouTube personalities is determined by number of views their videos sustain (Yahoo! Answers, 2012). As the number of views rises this draws the attention of performance agents who use YouTube as a way to view upcoming talent. Forcing Connor off YouTube, first through the denial of service attack and then through inappropriate content, effectively destroyed her marketable value. The likelihood of Conner being able to create a new online personality and market it successfully is low. Popularity, in online sites, is often bound up in the character of the online personality, the forces at play on the Internet at the same time, as well as social trends. Even if Connor created a new online personality there is no guarantee that it would experience the same popularity as her original one given all the factors that impact online marketability.

The economic loss experienced by those who are harassed online is not the only loss that may be sustained. Character, reputation, present and future employment, as well as interpersonal relationships can all be affected by the content and type of messages posted about an individual online. The following case, examining the message board, AutoAdmit, and resulting lawsuit, *DOE I and DOE II v. Anthony Ciolli et al., Defendants* (2008), resulted in these types of losses.

AutoAdmit is an open message board, similar to The Dirty.com,[10] and self-proclaimed as the "the most prestigious law school discussion board in the world" (see, AutoAdmit home page at http://www.autoadmit.com/). The message board became quite notorious after articles in *The Washington Post*, in 2007, and *Conde Nast Portfolio*, in 2009, detailed the abuse women were experiencing on the message board including lies, sexual and racial harassment, threats of violence, and general, vile commentary (Margolick, 2009). This was followed by a lawsuit in which the victims indirectly challenged the *Communications Decency Act of 1996* (Appendix E) by suing for harassment and defamation a number of online posters as well as the owner and operator of the message board (Margolick, 2009).

Brittan Heller, a student at Yale Law School, began to notice her name appearing in the threads on AutoAdmit not long after she was accepted into the school (Heller, 2007). Heller was accused of bribing her way into law school and having an affair with the Dean of Admissions to ensure her acceptance (Heller, 2007; Margolick, 2009). Anonymous posters on the message board claimed that she had herpes and called her derogatory names (Heller, 2007; Margolick, 2009). Soon, a number of other law students noticed their names appearing in regular posts including Heide Iravani. On the message board, Iravani was sexually harassed, racially demeaned, lied about in posts claiming she had gonorrhea and was addicted to heroin, and that she had sexually serviced the Law School Dean for a passing grade in his class (Heller, 2007; Margolick, 2009). Iravani was also mocked for her religion and her body measurements in a manner that caused her family a great deal of embarrassment, resulting in a rift between her and her father and grandmother (Margolick, 2009). Another student, an African-American who had been accepted to Vanderbilt Law, was so traumatized by the violent and racial slurs in posts aimed at her that she changed law schools (Margolick, 2009).

[10] *The Dirty.Com* – a website devoted to the anonymous posting of photos and attached disparaging remarks by the poster and then a response by the pseudo-named "Nik Richie." This website can be found in every major (and even some minor) cities in North America and has numerous linked sites on college and university campuses. According to self-promotion on the home page, it ranks as the 2,338 most popular site in the U.S. (*The Dirty*, 2012).

Numerous requests to the site owner/operators to remove the offensive posts met with silence, resistance, and then further abuse on the message board (Heller, 2007; Margolick, 2009). Resorting to something known as "Google bombing" posters flooded the message board with comments about Heller and Iravani, ensuring the threads on the AutoAdmit board would push down the rankings of any other information linked to their names on Google resulting in the inflammatory and defamatory comments emerging at the top of Google searches. This guaranteed that anyone using Google to search the students' names would get the posted AutoAdmit threads at the top of their search results (Margolick, 2009).

AutoAdmit also spawned an offshoot website, The Girls of the T14TALENT, a sexist website displaying photos of female law students, all of which have been taken and posted without consent. In the United States posting photographs of other individuals, taken in a place where they had a reasonable expectation of privacy, and for which you do not have express permission, is a violation of copyright laws (Heller, 2008). The photos were entered in an online beauty contest without the women's permission or knowledge (Heller, 2007; Margolick, 2009). Iravani's photo, on T14TALENT, was linked to her Facebook account allowing individuals to follow the links from AutoAdmit to The Girls of T14TALENT and then to her Facebook page and potentially in the other direction, widely dispersing the defamatory and vitriolic commentary on AutoAdmit and T14TALENT (Heller, 2007; Margolick, 2009). Commentary accompanying her photo described her in gym attire and remarked on her figure, which let her know that whoever had made the comment also frequented the same gym as she did (Margolick, 2009).

Numerous students, including Heller and Iravani, begged to have their photos taken down both because they were posted in violation of copyright laws, but mostly because of the accompanying sexist, demeaning commentary that was consistently emerging at the top of Google searches. Again, because of the manner in which the message board was structured, the inflammatory comments were gaining widest possible distribution on the Internet. Both women claimed that they were seriously concerned, not only for their present reputations, but for their future employment possibilities, knowing that many law firms check out applicants online using Google (Heller, 2007). Regardless of what or how the women asked the response of those who owned and managed the website was the same as Auto Admit – the women should learn to ask nicely and those who were posting had the right to say what they wished

based on the right of freedom of speech (Heller, 2007; Margolick, 2009). Students' emailed requests to have offending material removed often ended up posted in the threads and simply became fodder for more abuse (Margolick, 2009).

Eventually, Heller and Iravani joined forces and launched legal action. They could not sue Google or AutoAdmit for publishing the defamatory and untruthful comments because the *Communications Decency Act of 1996*, Section 230(c), protects hosting sites from lawsuits over defamatory content posted by users. This Act was written to ensure the free flow of information on the Internet by treating message boards and search engines as bulletin boards upon which anyone could post information and which could not be reasonably monitored by the owners/managers due to volume of traffic (Margolick, 2009). Instead, the two women spent considerable effort attempting to identify the various individuals who had defamed them online, all of whom were aspiring law students, including the administrator of AutoAdmit. Despite efforts to identify the individuals responsibly, when they eventually sued them in Federal Court for "defamation, invasion of privacy, and infliction of emotional distress" only the owner of the AutoAdmit message board was identified, all other defendants were listed as John Doe (Margolick, 2009, para. 7/ para. 32) (see *DOE I and DOE II v. Anthony Ciolli et al., Defendants* (2008)). Subsequently the two women have settled out of court for undisclosed sums with a number of those accused and the owner of AutoAdmit was required to embed codes that, in future, would prevent the message board from Google bombing (Margolick, 2009). Heller also hired the company, ReputationDefender to remove the offending posts from the Internet (Heller, 2007; Margolick, 2009).

Sections 264.(1), 264.(2), and 264.1(1) of the Canadian *Criminal Code* apply to the cases of Connor, Heller, and Iravani, if they were prosecuted in Canada. All of their harassers committed behaviours that qualify under the legal definition of harassment; that is to "knowingly engage in conduct that reasonably causes the target to fear for their safety or the safety of someone known to them." The taking of photos and posting them on the Internet, as experienced by Iravani, and the theft of Connor's photos and subsequent alteration and re-posting on her websites, demonstrates that the individual or individuals responsible had access to Iravani in physical space and had broken into or hacked Connor's computer. Iravani knew at least some of the individuals posting had followed her to the gym, based on their description of what she wore to work out, which made her sufficiently fear for her safety such that she was "unable to concentrate on her

school work, embarrassed to be seen in public" and subsequently sought therapy and was eventually hospitalized (Margolick, 2009, para. 24/para. 26).

Heller, Iravani, and Connor were repeatedly communicated with, both directly and indirectly through the online websites. The possibility that Heller and Iravani were watched repeatedly at their university or other places, they regularly frequented, violates s. 264 (2)(c) of the *Criminal Code*, and was reasonable to conclude given the detailed descriptions of their physical appearance and the photos posted on the T14TALENT website. As well, all three victims were publically threatened which violates s. 264 (2)(d) of the *Criminal Code*. In numerous posts all three were threatened with detailed sexual violence, violating s. 264.1 (1)(a) of the *Criminal Code.*

Both Iravani and Heller claimed that the experience of being harassed online, in this manner, was emotionally devastating and had significantly altered their lives for the worse (Margolick, 2009). Iravani ceased going to the gym, grew suspicious of men, felt "unsafe when alone" and withdrew from classes (Margolick, 2009, para. 34). Heller tried to move on but felt that she was being scrutinized unfairly and often unsure of what others thought of her (Heller, 2007). It is unknown what the emotional effect on Connor's life was as there have been no media reports regarding her case. Nevertheless, Connor did close all her social and professional networking sites and no longer has a presence on the Internet, indicating the effect of the harassment and stalking was significant not only personally but also monetarily.

Online harassment and stalking may be the worst form of harassment due to the interconnecting networks of acquaintances and friends that people often have online (Reyns et al., 2011). In this way the violent victimization moves through the boundaries between the two worlds and becomes situated in both. Given the Internet's ability to magnify and disperse information, online harassment has the ability to reach into the far corners of an individual's life. In the case of public harassment, such as was done on he AutoAdmit board, the defamatory information spread through the university, the faculty and administration, to potential future employers, and through friend networks and extended families of the victims. No aspect of their lives was untouched by this harassment.

The perpetuity of information posted online also adds dimensions to the victimization that expand it in a significant manner. Unless those targeted permanently change their names, the information posted online will follow them until they can

somehow either force companies that provide Internet search engines, like Google, to change the manner in which they page rank; force message boards to remove defamatory and harassing comments; or hire companies like Reputation Defender to remove the offending posts. The perpetuity of these messages becomes a way to victimize the individual over and over.

Section 264 of the *Criminal Code* has been successfully used to prosecute those who cyber-harass and cyber-stalk in Canada (see *R. v. Moss* (2011); *R. v. Labrentz* (2010); and *R. v. Basha* (2002) in which s. 264. (1) was successfully used to prosecute). In the United States, there is a variety of state legislation as well as the federal laws including U.S.C. Section 18 § 2261A, federal cyber-stalking legislation (see Appendix C) and U.S.C. § 223(a) (1) (C), obscene or harassing phone call legislation, both of which have been used successfully to prosecute cases (e.g., *United States of America v. Erik Bowker*, in which U.S.C. Section 18 § 2261A was applied, and *State of Wisconsin v. Peck*, 2008, in which U.S.C. § 223(a) (1) (C) was applied).

A landmark case in American cyber-stalking involved the murder of Amy Boyer in 1999. The killer used the Internet, as well as physical space, to stalk and murder his victim (Roberts-Roach, nd). In October of 1999, 20-year old Amy Boyer was shot 11 times as she left her job at a dentist office. Boyer's stalker obtained her Social Security number via the Internet as well as her place of work, home address, and numerous other pieces of personal information using an online document search company, Docusearch. Boyer's stalker had posted that he had "lusted for the death of Amy" openly on a website where he had detailed, step-by-step the process he was going to go through to kill her (Boulard, 2001). The stalker, Liam Youens, shot himself immediately after killing Boyer, thus no lawsuit was ever filed against him for her murder; however, Boyer's parents, in *Remsburg v. Docusearch, Inc* (2002), sued the Internet company, and brought cyber-stalking to the forefront of media and legal attention.

The New Hampshire Supreme Court "aggressively interpreted the foreseeability element" of the negligence doctrine and held that the company was liable for its customer's criminal acts, stating that Docusearch had a "duty to exercise reasonable care in disclosing a third person's personal information to a client" and, thus, the stalking and identity theft were "sufficiently forseeable". (Chief Judge Barbadoro, United States District Court for the District of New Hampshire, 2002, Civil No. 00-211-B DNH 90; 2002).

The first American prosecution for cyber-stalking was against Gary Dellapenta, a 50-year old, former security guard (*State v. Dellapenta* (1999), Los Angeles Superior Court). He had solicited the rape of a 28-year old victim by impersonating her on message forums and chat rooms where he posted her home address, personal phone number, and a series of messages stating that she fantasized of being raped (History.com*,* January 19, 1999). At least six times she had men appearing at her home, often in the middle of the night, demanding to be let in so that they could rape her and fulfill her fantasies (United States Department of Justice, 1999). California Penal Code s. 646.9 was used to successfully prosecute the man (Wired, 10.25.99).

Canada has also been successful in applying current legislation to those who perpetrate stalking online. Despite the fact that s. 264 of the *Criminal Code* only covers print, television, telephone, and radio (see Bill C-273, passed June 6, 2012, now being studied by the Justice Committee, to include Internet and all electronic forms of communication (Ip, 2012)) it has been used to prosecute cases of cyber-stalking. On May 2011, the first case of cyber-stalking was concluded when a 39-year old truck driver was found guilty of stalking a 16-year old actress and sentenced to 18 months jail time, three years probation and sex offender treatment (see *R v. Cholin*, (2010)). This was also a case in which the stalking behaviour flowed back and forth between cyberspace and physical space. Cholin began contact with his victim when she was 12-years old by attempting to visit her at the CBC television set (he was escorted off the premises twice under guard). He also sent her hundreds of emails, contacted her and her friends through the social networking site, Nexopia, messaged other cast members via email, and sent her gifts, including marijuana. Justice Stone had no difficulty in applying the law of harassment to the online and electronic communications, referring to them as "direct communication" which he found to be excessive in number.

In making his judgment Justice Stone referred to *R. v. Wenc,* (2009), a case in which there were also numerous emails used to harass an individual, and *R v.* Leasak, (2007), a case in which there was no Internet communications. Justice Stone considered the two cases equal examples of harassment and suitable to be used as precedent for the Cholin case. Numerous other cases of cyber-stalking in Canada have also been prosecuted under s. 264 of the *Criminal Code* (e.g., *R v. Moss*, (2011); *R v. Labrentz*, (2010); and *R. v. Kitchen* (2012)).

Those who commit stalking and harassing behaviours in cyberspace may gain intimate personal knowledge of the other person through online communication without his or her consent or after being told to cease (United States Department of Justice, 1999). Stalkers lurk in chat rooms, news groups, bulletin boards, games and metaverses. They may send e-mails, instant texts, and inappropriate electronic greeting cards to the victim and their family, friends, teachers/professors, employers, co-workers, customers, or other individuals who belong to the same social or religious groups as the victim. They have, at times, created and posted personal advertisements in the victim's name (e.g., Craigslist), created or utilized existing websites, such as social networks, to post threatening and/or harassing messages that may include pictures which depict the victim pornographically or photos which have been altered to include threatening imagery such as blood, nooses, gags, etc., or maintain electronic surveillance (Department of Justice Canada, 2011; Mullen, Pathé, Purcell, & Stuart, 1999; United States Department of Justice, 2009).

While stalkers, in online games and metaverses, tend to follow victims from location to location, when perpetrated across multiple platforms – including seeking access to and publishing personal information that identifies the victim in geographic space, the activities intrude upon, dominate, and ultimately control the behavior of the victim (Suler & Phillips, 1998). In general, cyber-stalking is done to create fear in, and obtain a reaction from, the victim (United States Department of Justice, 2009) including forcing them to remove their presence from all social spaces on the Internet (Dibell, 2008; Encyclopedia Dramatica, 2011; Roberts, 2008; Suler & Phillips, 1998).

In Canada, according to information provided by the *Family Violence Initiative*, (Department of Justice Canada, 2011), cyber-stalking is defined as online harassment and usually refers to direct communication of some sort. In reviewing concluded criminal case files, this has been predominantly via e-mail, but does also includes texting, instant messaging, direct messaging through the text or e-mail functions on the victim's social network pages or any other form of person-to-person, electronic, computer-mediated communication. Internet harassment, in which the offender publishes, in an online space, the victim's personal information such as home address or private phone numbers, directly impacts levels of fear because victims no longer feel secure in the physical world knowing that their stalker (and others) have access to their physical location (Reyns et al., 2011). For most victims of stalking and other forms of criminal

harassment, fear is one of the most predominant emotions they experience (Reyns et al., 2011; United States Department of Justice, 2009). One Canadian victim reported to the judge in her victim impact statement the following:

> I don't feel safe anywhere. I don't know if I ever will. My life went black, it changed me forever. There's nowhere safe. My home. My work. Everything has been affected. I lost all interest in things. I cry a lot, my self-esteem and self confidence is zero. (D. White in *R. v. Basha* (2002)).

Prosecution for cyber-stalking or cyber-harassment, in Canada, is predicated on genuine fear for the victim's own safety or the safety of anyone known to them. *Canadian Criminal Code* s. 264 (1) states, "No person shall…engage in conduct…that causes that other persons reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them." Many victims refer to the fear as being both intense and prolonged (Department of Justice, Canada, 2011). Empirical studies on the long-term psychological and emotional distress experienced from stalking, demonstrate that the symptoms can be severe enough to qualify as posttraumatic stress disorder as defined in the *Diagnostic and Statistical Manual for Psychological Disorders* (APA, 2000) (Westrup, Fremouw, Thompson, & Lewis, 1999).

For most victims it is the unrelenting fear of the unknown that seems to take the greatest toll (McCall, 2003). This fear is based in two factors – first, due to online anonymity, it is unknown who is doing the stalking and, second, it is unknown what they potentially might do to their victim (Department of Justice, Canada, 2011; United States Department of Justice, 2009; United States Department of Justice, 1999).

In a study of cyber-stalking involving college-age students it was determined that, while most of the students expressed the belief that the individual stalking them must be known to them in some capacity, most did not know who it was (Reyns et al., 2011). Victims expressed deep-seated fears that it could be anyone in their life – the individual in the cubicle next to them at work, their neighbor across the hallway, or an ex-friend or lover (Reyns et al., 2011; United Stated Department of Justice, 1999). This type of uncertainty led to fears that there were few, if any, individuals in their life they could trust and caused many to alter their physical world behaviors, such as going out less with friends and family, being fearful when travelling to and from classes or work, and being fearful whenever someone came to the door of their residence, especially if their name,

address, and phone number had been published during the stalking incidents (Reyns et al., 2011; Westrup et al., 1999; United States Department of Justice, 2009). According to the U.S. Department of Justice (2009) approximately five percent of all cyber-stalking cases cross over into the real world with just half of those ending in violent assault or murder. Thus victims of stalking do have reason to fear their stalker.

When the stalker is a lone individual, both police and victim have a higher likelihood of narrowing down the potential perpetrator depending on levels of computer use sophistication (D'Ovidio & Doyle, 2003). Those who take steps to ensure anonymity via the use of IP blockers or other such identity-blocking software, will be much more difficult to locate (D'Ovidio & Doyle, 2003). In empirical studies, conducted by the FBI, less than four percent of stalkers used such sophisticated tools (D'Ovidio & Doyle, 2003). Additionally, for those who cross-over from cyber-stalking to physical stalking, the likelihood of identification rises, making it easier to not only determine identity, leading to the seizure and analysis of their computer, but also to lay charges based on the physical world actions regardless of online behavior (e.g., *R. v. Kitchen* (2012); *R v. Vandoodwaard* (2009)). When a group, with 150,000 to seven million members, such as 4chan and the Patriotic Nigras are victimizing an individual, managing to find and acquire the evidence necessary for a successful prosecution becomes a logistical nightmare including attempts to identify the individuals responsible, matching identities to statements/photos posted, and then proving genuine fear – which may be more difficult for others to comprehend when the group doing the harassment is so large (Margolick, 2009). Inability to match identities to actions severely reduces the likelihood of prosecution and increases the power of those operating behind the cloak of anonymity (D'Ovidio & Doyle, 2003; Baum, Catalano, Rand, & Rose, 2009; Valenti, 2007). These are some of the reasons that law officers and courts have had such a difficult time in prosecuting any of the members of Anonymous, even for attacks aimed at powerful targets such as The British Home Office, Sony, Apple, and Bank of America (FBI Cyber Division as cited in Infosec Island, 2012).

4chan is a large, anonymous, and ephemeral online community of over seven million users (Bernstein, Monroy-Hernandez, Harry, Andre, Panovich, & Vargas, 2010). /b/ is its most popular discussion board with a random series of threads on a variety of topics all of which are deleted when they reach 15 pages of continuous posts or are pushed to the bottom of the first page from lack of activity (Bernstein et al., 2010). In this

way there is often no history of postings to search and, given the default of "anonymous" for all postings, (except for the few individuals who choose to post under other non-registered user names), identifying the individual or individuals who make the posts appears impossible.

In the case of Heller and Iravani (discussed above), it was determined that a large number of users had posted their comments from common-use university computers or from Internet cafes, libraries, and other locations (Heller, 2007; Margolick, 2009). In this case, while the IP of the computer could be ascertained, there was no way to link any one, specific individual to a specific defamatory message. It was only through a careful investigation, related to the physical locations the women were described in, that a small number of the perpetrators were identified (Heller, 2007; Margolick, 2009). Others came forward and confessed (Heller, 2007; Margolick, 2009). Others were identified because they were the registered owner/operators of the message board (Heller, 2007; Margolick, 2009). The resulting case, *DOE I and DOE II v. Anthony Ciolli et al., Defendants* (2008) heard by the Federal Court, in the District of Connecticut, named one specific individual and twenty eight anonymous individuals responsible for the harassment. All but one has settled out of court for undisclosed sums (Margolick, 2009). The remaining individual, Ciolli, the administrator of the AutoAdmit message board, is counter-suing them in the Court of Common Pleas of Philadelphia County, Pennsylvania (*Ciolli v. Iravani, Heller, Lemley, Keker & Vannest LLP, Dave, Rosen, Rose & Associates, P. C., Chanin, ReputationDefender, Inc, and T14Talent,* 2008).

Group harassment seems to be closely linked to flaming, the expression of anger and hatred characterized by the gratuitous and uninhibited text and imagery, that has been present since the inception of the Internet and considered insignificant by groups that commonly indulge in it (Dibbell, 2008; Holt & Bosler, 2008; Kiesler et al. 1984 as cited in Reid, 1999). Group harassment reflects the tradition of flaming but when aimed at those who misunderstand the tradition or whose reputations become severely compromised it is seen as a crime rather than a cultural norm (Bansal, Sharma, Kumar, Aggarwal, Goyal, Choudhary, Chawla, Jain, & Bhasin, 2011). Flaming emerged in computer-mediated communications over time and is culturally specific (Bansal et al., 2011). Indirect flaming, the type that originally existed between groups, was the publicizing of a disagreement or hostility posted in language that could only be

understood by the factions involved; for example, on message boards devoted to specific topics, game discussions or other related discussions (Bansal et al., 2011).

Direct or intentional flaming is aimed at a specific person or group and, if the mode of communication is anonymous, the users tend to flame at high levels of hostility, being unrestrictive in their behavior, making inflammatory remarks while indulging in vicious attacks and derisive commentary (Bansal et al., 2011). It has been suggested that this occurs as a result of cultural misunderstanding and those committing direct and intentional flaming may believe they are participating in indirect flaming and misunderstand how seriously they have crossed the line from banter into criminal harassment (Pimentel & Elenkov, 2010). There is evidence that this may have occurred in the Heller and Iravani case as evidenced by one of the posts several months into the harassment, "People, this is sick…have you forgotten there's a real human being behind this? A flesh-and-blood girl, and apparently a somewhat emotionally fragile one? This isn't funny anymore. It's becoming evil." ("Josef Stalin", AudoAdmit, as cited in Margolick, 2009). Unfortunately, Stalin's comments were dismissed and the harassment continued, targeting other women (Margolick, 209). This demonstrates the cultural nuances that influence whether a behavior may be considered criminal or a cultural norm. Younger users indulge in indirect flaming and see it as a normal part of game-play and other online communication (Suler & Phillips, 1998). Others, who are also younger or less in control of their emotions and rage, seem to have more difficulty restraining their online posting, viewing others as less than human and more like targets (Suler & Phillips, 1998). Empirical studies show that, on average, online stalkers are male between the ages of 21 and 29 (Baum, Catalano, Rand & Rose, 2009) supporting the contention that young, adult males are much more likely to participate in the kinds of behavior that, at the extreme end, result in stalking or harassment (D'Ovidio & Doyle, 2003).

Early online stalking and harassment seemed to mimic traditional, physical world stalking with perpetrators developing an obsession for a single, online presence (Department of Justice, Canada, 2011; Ogilvie, 2000; United States Department of Justice, 2009). The more recent organized behaviours of groups like Anonymous, The Patriotic Nigras, and 4chan, indicates a new type of stalking that targets female bloggers, YouTube personalities, and other individuals who experience success on the Internet with the goal of "raping" them so that they withdraw from cyberspace (Citron,

2008; Dibbell, 2008). This may be bounded in their expressed need to show those who believe "the Internet is serious business" that it is not (Dibbell, 2008).

Cultural changes over time, with the Internet now being used more for business and day-to-day social and commercial transactions belie the attitude that the Internet is not serious business. For the hundreds of millions of individuals who socially interact, make their living, and get an education in social networks, games, and metaverses, it is serious business. Indeed, the emerging conflicts that have begun to make their way into courtrooms over flaming, harassment, and online violent assaults, portrayed as either innocuous, cultural exchanges or game-play are a testament to this.

4.3. Violent Assault

Many violent assaults within metaverses and immersive games are aimed at depriving other players of their valuable property (Adrian, 2010; Bakioglu, 2009; Dibbell, 2008) or disrupting game-play (Bakioglu, 2009; Kennedy, 2009; Dibbell, 2008). As a result, it is not just an assault that is committed but also a type of robbery (Adrian, 2010). Robbery is the infliction of bodily injury or the use of force, or threat of force, during the commission of a theft (see s. 343 of Canada's *Criminal Code*, Appendix D and U.S. Model Penal Code (MPC) 1962 § 223.2(1), specifically section 8), and a crime in both the United States and Canada.

Assaults in immersive games and metaverses often occur as a result of organized griefing (Adrian, 2010; Bakioglu, 2009; Kennedy, 2009). These attacks are not aimed at any specific person (an exception would be the attack on avatar Anshe Chung, real estate developer in Second Life during her 2006 live CNET interview) but aimed at causing mayhem, humiliating other players, and disrupting game-play by crippling servers and causing them to crash, and depriving those immersed in the game or metaverse of their property and freedom from unwanted assault, detainment, and/or interference (Adrian, 2010; Dibbell, 2008).

In 2008, the organized group, the Patriotic Nigras launched a sequenced attack on multiple sections of the Second Life metaverse by logging on repeatedly under different names and accounts, moving from location to location over a period of about seven or eight hours, and eventually, simultaneously crashing multiple servers that ran

Second Life, shutting down the metaverse (Dibbell, 2008). During the attack they took control of other player's avatars and forced them to repeatedly scream taglines from movies as well as specifically targeting certain islands, leaving behind virtual graffiti (Dibbell, 2008). The goal behind this behavior, according to ^ban^, their leader, was to push Second Life users past the brink and make them permanently quit visiting the metaverse –"it's all about the "lulz" said ^ban^, divulging that the enjoyment in ruining other individual's online experiences seems to be founded in the fact that most of the The Patriotic Nigras, are, in the words of ^ban^, "psychotic" (Dibbell, 2008).

Griefing behavior is also seen in social networks and blogs, often aimed at women, racial minorities, homosexuals, and other identifiable minority groups and consists of repeated communications filled with hateful and vile messages (Adrian, 2010; Franks, 2011; Moor, Heuvelman, & Verleur, 2010). Groups such as the Patriotic Nigras, the EVE Online GoonSwarm Alliance, 4chan, Anonymous, and the /b/tards of /b/, colloquially known as the "id" of the Internet, take their culture of online trolling, raids, rape, and harassment and model it on advice and attitudes perpetrated by the mythic, male-dominated, 150,000 strong, members-only message forum of Rich Kyanka's Something Awful (Bakioglu, 2009; Dibbell, 2008).

In one attack, an avatar horrified students on the virtual campus of Ohio State University, in Second Life, when it walked through the front doors and opened fire with an assault rifle on other avatars (Dibbell, 2008). This was an exact replication of the actual Virginia Tech shooting (Bugeja, 2007). Other scenes of mass violence have included the burning twin towers of 9/11, including avatar bodies falling/jumping from the buildings, murdered prostitutes, a murdered and disemboweled woman on a bed with an supply of code-in options allowing visitors to further violate her body, bloody carnage reminiscent of overkill scenes from genocides, and any other atrocity these groups can come up with (Dibbell, 2008). While some of these scenes are staged by the groups and do not include the destruction of avatars or virtual property that belong to others, shootings, such as at Ohio State's virtual campus are a violent assault that clearly violate others' avatars.

Violent assault in fantastical games is considered expected behavior especially for games that award points for killing your enemy (Barnett, Coulson, & Foreman, 2010). Despite the fact that the point of games such as EVE and World of Warcraft are based on violent interaction and harsh, unforgiving worlds, some behavior is considered

unethical such as killing newbies as soon as they arrive in the game and conducting battle strategies that are “a less-than-sporting end run around a fair fight” (Dibbell, 2008, p. 3). These attacks, while they may violate moral standards and practices in the worlds in which they occur, are not crimes, regardless of how violent they become. They are all simply part of the game. For a violent assault, such that it meets the definition of Canada’s *Criminal Code* ss. 265 (assault), 267 (assault with a weapon or causing bodily harm), 268 (aggravated assault), 269 (unlawfully causing bodily harm), 229 (murder), 232 (murder reduced to manslaughter), and even 228 (killing by influence on the mind) all require the victim to be a human being (*Criminal Code*) and do not include events which occur as part of fantastical game-play.

There are no known criminal cases in Canada that have applied the crime of robbery, assault, or murder to acts that occurred within a metaverse, immersive game, social network, or on the Internet (as searched in Criminal Source). This may be because of the requirement of the essential concepts of *mens rea* and *actus reus* in Canada (Griffiths, 2007) and the United States (Adrian, 2010) for a crime to occur in addition to it happening to a human being. *Actus reus* and *mens rea* are hard to prove in virtual spaces (Adrian, 2010). Additionally, what is stolen, destroyed, or assaulted must have some value and, while legislators have begun to grapple with the concept of virtual artifacts holding value and having the capacity to be stolen, misappropriated, and/or destroyed in a manner that does not honour the rules of the game (Adrian, 2010; Bakioglu, 2009; and Kennedy, 2009) there has yet to be any legislation specifically related to virtual artifacts (Kennedy, 2009). Most cases that have proceeded through courts, related to the value of virtual artifacts, have done so through civil actions with many of them settled out of court (e.g., *Eros v. Leatherwood* (2008) and *Eros v. Simon* (2008) as cited in Kennedy, 2009).

In Canada, real property is sometimes valued almost as highly as human life and provides reason behind legislation making acts such as arson, damage to chattels, and theft, crimes (Griffiths, 2007). Assaults that damage or deprive others of their virtual property, such as avatars and other artifacts, may better be dealt with under laws that relate to chattels, given the value and qualities of these items (value, ability to possess, use, enjoy, transfer, and exclude others) (Adrian, 2010). (A full discussion of chattels is beyond the scope of this paper, please see: “Intellectual property or intangible chattel?” Adrian, (2006), “Beyond Griefing: Virtual crime” Adrian, 2010, “Life, liberty, and the

pursuit of swords and armour: Regulating the theft of virtual goods" Aria, (2008) or "Virtually Liable" Ledgerwood (2009) for discussions on the law and virtual goods).

Professor Castronova and Yen-Shyang Tseng have both examined the boundary between game-play and non-game-play, which they refer to as the "magic circle", in an effort to discern which activities and behaviours are acceptable and legal in each realm (Castronova, 2004-2005; Tseng, 2011). While the difference between most spaces within metaverses, that act as an extension of our day-to-day lives, and immersive games, which invoke fantasy and play, may be clear to some, for others this difference may not be so easily discerned (Castronova, 2004-2005). Both scholars argue that there is intrinsic value in fantasy and game-play which will be threatened if we fail to secure the magic circle, ensuring the right to play, as well as protecting non-play areas from behavior that violates the rights and freedoms of those using it as an extension of their daily lives (Castronova, 2004-2005; Tseng, 2011).

Games are hard to define (Castronova, 2004-2005) which may partially explain the behavior of griefers and others who disrupt metaverses and other areas that are an extension of daily living. The conflicting views can be seen in comments made by griefers in reference to their online havoc, "you may be playing EVE Online, but be warned: We are playing Something Awful" (Commander Sesfan Qu'lah, chief executive of the GoonFleet Corporation and leader of the GoonSwarm Alliance, in physical life, Isaiah Houston, a senior medieval history major at Penn State University as cited in Dibbell, 2008) as compared to those who use metaverses, such as Second Life, as an extension to their physical world life, including commercial activities such as is done by "Profoky, Neva", a real estate entrepreneur (in physical life, Catherine Fitzpatrick, a Russian translator and human rights activist) who refers to griefing behaviour as "terrorism"; "it's anti-civilization…it's wrong…it costs me hundreds of US dollars" (Fitzpatrick as cited in Dibbell, 2008).

Generalized and non-focused attacks, conducted by griefers, seem to affect victims in a different manner than do singularly focused attacks such as the AutoAdmit case and the online stalking in *R. v. Cholin* (2010). This may be because a generalized attack, in a public place, feels less personal and more like annoying words spoken publically, especially when there are others present. This is significantly different than a singularly focused attack on a specific person. Singularly focused messages, posted specifically about a specific individual, or communication that is directed specifically via

social network site or email, is much more personal and, thus, much more threatening (Fukuchi, 2011). This may be because, in a focused attack, the listener is a captive audience whose privacy interests have been invaded in an intolerable manner with the unwanted communications violating the sanctuary of their home, office, or other personal space, and their computer. American courts have recognized these qualities of personal communication as more personal and non-random (see *Rowan v. U.S. Post Office Dep't.* (1970)). A statement such as this does not, however, belittle the very real damages that an individual, such as Emily Connor, might sustain from an organized griefing attack or the very real emotional and psychological damage any other individual might sustain from such an attack. The levels of fear and victimization are personal and known to vary from individual to individual. This is a fact of violent victimization that our courts have begun to attend to via the use of victim impact statements. Given that individuals invest their time, energy, and money into online representations as well as professional and commercial enterprises, the behavior of griefing should be recognized as a real harm to real individuals and property when it occurs in areas that are an expansion and extension of our physical world. In this way both civil and criminal remedies may be applied.

To determine which civil, criminal, or community standard remedies should be used within games and metaverses, the magic circle must be clearly drawn delineating which areas are fantastical play space and which are an extension and augmentation of the physical world. Within game space, community standards can be applied, instead of criminal or civil law, through the use of End User License Agreements (EULA) and Terms of Service (ToS) that clearly spell out the rules of play. Game-play and all it entails, must remain within the magic circle and not bleed over into the physical world to ensure it enjoys the protection of the magic circle. This would then clarify behavior that appears to be harassment or other violent victimization but is part of game-play and that which qualifies as violent victimization. To keep expansions and extensions of our physical world separate from play spaces the recommendations of Professor Castronova are viable. Drafting a "Law of Interration" would support the EULA's legal status, allowing them to preserve play space (Castronova, 2004-2005). This would ensure closed worlds with impermeable borders: physical world laws remain outside the circle and the EULA and/or ToS dictate community standards and rules of play inside (Castronova, 2004-2005). Open worlds, such as Second Life, would generally maintain

porous borders and the application of physical world law would have to apply except for specific zones that are clearly identified as fantastical play areas (Castronova, 2004-2005). Avatars, depending on where they are placed, would be classed as either personal property and dealt with through legal action related to property or as representations of real humans and dealt with through our current laws of harassment and stalking (s. 264 *Criminal Code*). In both cases civil and criminal law would apply depending on the details of the individual cases. For example, clear cases of harassment demonstrated via sustained, repeated personal communication via email, social network, message boards or other specific and individual-focused attacks would be viewed as criminal harassment and prosecuted criminally. In this way individuals would knowingly agree to the rules of game-play or the metaverse when entering and be certain as to which type of realm they are within and thus know the laws or rules would apply.

Several theoretical concepts have been touched on during the prior discussion of cyber-rape, harassment, violent assault, and griefing. The following section applies several criminological theories to these behaviours with the goal of providing insight into the behavior. Following the discussion of criminological theories is a general discussion and recommendations for a modification to existing legislation with a suggestion for the introduction of a new law of .Interration as well as a brief discussion recommending the examination of the quasi-human status of avatars.

5. Criminological Theory, Discussion, Recommendations, and Conclusions

5.1. Criminological Theory

Theory, if properly developed and applied can help explain human experience and behavior (Akers & Sellers, 2009). While it is true that North Americans are now experiencing new ways of living and communicating via cyberspace, it is also clear that this has not changed human nature. In the new realm of cyberspace there is still deviance and crime. Short of changing human nature, there is probably no way to avoid the difficulties of crime online, at least if we want our virtual worlds to be as engaging as the physical world (Hunter & Lastowka, 2003). Thus, it is expected that crime will continue to exist in cyberspace and, as such, theoretical explanations may offer insight into this behavior.

Currently theorists and researchers have begun to apply existing criminological theory to online acts of crime (e.g., "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization" by Holt & Bossler, 2009; and "Policing diversity in the digital age: Maintaining order in virtual communities" by Wall & Williams, 2007). In examining online deviant and criminal behaviours, through current criminological theory, greater understanding of this behavior will occur. The following section applies psychological, social control, and routine activities theory to the behaviours described in this paper with the goal of offering insight into this behavior

5.1.1. Psychological Theory – The Disinhibitory Effect

Rude language, harsh criticisms, anger, hate, threats, harassment etc. are all the toxic outcome of the online disinhibition effect. Based on the anonymity, affordability, and accessibility of the Internet, specific beliefs and behaviours tend to emerge in some individuals in online space. Building from deindividuation theories, Suler (2004) has identified specific phenomenon that emerge in online social interactions which increase

the likelihood of committing deviant or criminal behaviours including dissociative anonymity, deindividuation, invisibility, asynchronicity, solipsistic introjection, dissociative imagination, context, and self-constellation across media.

Dissociative anonymity occurs when individuals believe that they have the right to separate their actions online from the person they are in the physical world. Anonymity allows them to feel less vulnerable, knowing that what they say or do online cannot be linked back to the "real them". Joe Traw, one of the online posters in the AutoAdmit case, publically apologized. He stated that he was "anguished" over what he had done and wondered why he hated himself so much to do what he did (Margolick, 2009). Subsequently, feeling that the self he was online was so disjointed from the self he was in physical space, he withdrew from university, shelved plans for law school, and enlisted in the military (Margolick, 2009). Bowker and Tuffin (2003) also found that deceivers, in computer-mediated communications, tend to distance themselves from the message and feel less guilt in online communications as compared to face-to-face communications. Anonymity obviously affects not only tone but also content of online messages.

Deindividuation occurs when individuals believe that they are indiscernible from the group they are in. Personal disguise heightens this effect leading to lowered inhibitions resulting in increasingly unrestrained and anti-normative behaviours (Moor et al., 2010). Studies in the effect of avatar disguise found that individuals who played games using avatars that wore cowls were more likely to use hostile language than those whose faces could be seen (Blasovich & Bailenson, 2010).

The impression that we move through the Internet, seemingly without being seen, encourages individuals to say and do things they would not do in their physical lives for fear of damaging their reputation and negatively affecting the good opinion others hold towards them (Nissembaum, 2001). Perceptions of invisibility also reduce physical cues that help to moderate our behavior, such as the expression on another person's face or their body language (Suler, 2004). Without this feedback individuals are free from the constraints that interpersonal communication normally provides. According to Bartol and Bartol (2005), the Internet provides the very means of stalking due to its lack of social constraint because all normal sensory data missing. This allows stalkers to build larger, stronger fantasies about the victim without any moderating effects that negative responses might induce (Bartol & Bartol, 2005). This effect has

been identified in recent criminal cases. In *R v. Cholin* (2010), the judge remarked that regardless of response from the victim, her friends and family, the perpetrator continued to believe that his victim was enjoying his attention In the Boyer (1999) case, Youens, the stalker, created an entire website filled with information about his victim, openly posted for anyone to see, including the details of how he planned to murder her. In studies of flaming on YouTube, researchers found that a lack of interpersonal cues tended to increase the likelihood and intensity of flaming attacks (Moor et al., 2010). Rutter (1987) (as cited in Spears & Lea, 1994), found that a lack of interpersonal communication increased depersonalization, lowered cohesiveness, and reduced social conformity, resulting in higher levels of hostile communications and less inhibited interchange.

The lack of real-time interaction, or asynchronicity in communications, allows individuals to focus more intensely on their own feelings (Suler, 2004). This effect is increased by a "hit and run" type of messaging where an individual can "drop bombs" on others and then run away before they have time to respond. Asynchronicity of computer-mediated communications facilitates hit and run messaging because, unlike face-to-face or even telephone conversations, where the communications partner is present and able to respond to statements in real time, in computer-mediated communications the other person may not be present or able to respond immediately. The effect of asynchronicity is heightened by dissociative anonymity and feelings of invisibility (Suler, 2004). Not having to answer to others' real-time responses diminishes feelings of responsibility and accountability.

When working on a computer, without the feedback of others, a form of solipsistic introjection may also occur. Introjection is the "unconscious incorporation of external ideas into one's mind" (Barber, 2004, p 791). This occurs when the individual communicating via computer, introjects the other person into his or her mind, imagining their vocal response, as though having an inner dialogue. In this way, the person writing projects, at a sub-vocalization level, the responses of the other person and perceives them to be real. Simultaneously dissociative imagination occurs. This has the effect of making the other person seem less real with less genuine emotion than the individual doing the writing. This phenomenon may have occurred in the AutoAdmit case. There appeared little in the way of understanding that the individuals they were posting about were real human beings until one of the individuals posting tried to point out that the

women they were writing about were real. Both Walther (2007) and Nakamura (2002) have demonstrated, in studies on computer-mediated communications, that stereotyping is common with exaggerated representations of others filled in when the information is missing or incomplete, as it often is online. This may have also been a factor in the *Cholin* (2010) case with the stalker believing he was going to "save" his victim from her friends and family, as though she was some type of caricature of a real human, in this case, a fair maiden needing rescue.

The context, in which the communications occur, including personal values and culture of the situation, also influences the tone and level of hostility of messages (Suler, 2004). Historically, online flaming and aggressive communications have been a fairly consistent part of some message boards and immersive games (Forsyth, 2006; Holt & Bosler, 2008). Individuals who fail to recognize that they have changed context may perpetuate behavior that is inappropriate for the context they are in. This appears to be part of the explanation for organized griefing. Failure to recognize that metaverses, such as Second Life, act as extensions of day-to-day living rather than being a game which is play space in a fantastical setting, may induce individuals to treat others within inappropriately, causing personal harm as well as financial and emotional loss.

Individuals may also act more disinhibited in certain online contexts – avatars, strongly linked to the physical self, will be controlled in a manner more in line with who the individual would like to be seen as compared to avatars in online atmospheres that allow for complete anonymity where there can be no impact on personal history and reputation (Yee & Bailenson, 2007). This is referred to as self-constellation across media. Numerous studies have demonstrated that the more disguised the individual feels the more disinhibited their behaviour will become (Blascovich & Bailenson, 2010; Zimbardo, 2007).

Psychological theories, such as Suler's (2004) disinhibition effect, can help to explain the behavior of organized and solo griefing as well as communications such as occurred in the AutoAdmit, LambdaMOO, JennyMUSH, and *Cholin* cases. Imagining the response of the victim is commonly reported in cases of stalking, both offline and online, and was commented on by Justice Stone in the *R. v. Cholin* (2010) trial. The stalker's belief that his victim had willingly entered into communications and wished to be kidnapped, were entirely of his own mind with no external confirmation, "the accused appeared to have had the deluded view that complainant would welcome being

kidnapped by him, and that her friends and family were simply screening him from her" (Justice Stone, *R v. Cholin* (2010)).

While psychological theories are particularly suited to online behaviours, considering all interaction online is purely of social relations and, thus, of the mind (Wall & Williams, 2007), other criminological theories, such as social control theories offer insight into these behaviours as well.

5.1.2. Social Control Theories

Social control theories also offer insight into the behaviours of those individuals who violate the trust of others online. Theorists such as Agnew (1993), Gottfredson and Hirschi (1990) and Reiss (1951) have all argued that humans only refrain from harming others due to the social constraints or controls of society (as cited in Akers & Sellers, 2009). The risk of violating the trust of those with whom we are socially attached and, as a result, experiencing punishment, renders us unwilling to commit harms against others. This risk is significantly diminished in online space due to anonymity. While researchers have demonstrated that approximately 80% of all game-players are consistent in their use of a single, stable avatar identity due to the rewards that come from establishing history, reputation, and trust in guilds, that still leaves 20% who may not be as concerned.

Control theorists contend that there are both external and internal controls (Akers & Sellers, 2009). External controls exist via social sanctions such as reward for conformity and punishment for deviance (Reiss, 1951 as cited in Akers & Sellers, 2009). In cyberspace, due to anonymity as well as the reluctance of many game providers to impose sanctions, punishment rarely occurs for deviant behavior (Adrian, 2010; Lin & Sun, 2005). Some researchers have found that only players who routinely grief in avatar-based environments are labeled as such and punished for their behavior (Lin & Sun, 2005). Despite a lack of consistent punishment, many players do respond strongly to sanctions and rewards provided by their guilds and online friends, which does provide support for the contention that there are external social controls in these environments (Williams et al., 2006; Yee & Bailenson, 2007).

Internal social controls are exerted by the individual and emerge as guilt or shame, preventing them from committing deviant behaviours (Reckless, 1951 as cited in Akers & Sellers, 2009). Though emerging after the fact, shame was clearly evident in

individuals such as Kirk Cheney and Joe Traw, who showed remorse and shame for harassing Heller and Iravani on the AutoAdmit message board. Cheney made efforts to personally apologize to both women and Traw publically apologized (Margolick, 2009). Given that none of the other stalkers in the AutoAdmit case admitted guilt or shame, it would appear that they were somehow convinced the object of their obsession desired the attention or they simply didn't care and as a result normal guilt and shame did not affect them in the same manner as it did for Cheney and Traw.

Large-scale research studies, on stalking in the United States, determined that the primary motives for stalking were control, intimidation, or frightening the victim (Tjaden & Thoennes, 1998 as cited in Bartol & Bartol, 2005). This is moderated by typology. Love obsession and erotomania stalkers are convinced that victims return their affection and simple-obsessive and vengeance stalkers are motivated by a desire to frighten and intimidate their victims (Bartol & Bartol, 2005). While internal and external controls can offer some insight into violent online behaviours, when it comes to stalkers, other theories are necessary to help fully explain differences in how these individuals respond to external and internal controls.

Other individuals and groups, such as the Patriotic Nigras and the Goonswarm Alliance do not seem to be bothered by external or internal controls. When asked about legal sanctions, they claim that the EULA keeps them safe from lawsuits and criminal charges and that they are just playing "something awful" (^ban^ as cited in Dibbell, 2008) or playing the other players (Lin & Sun, 2007) with the goal of ruining everyone else's fun. Indeed, the motto of the Patriotic Nigras is "ruining your Second Life since 2006" (Encyclopedia Dramatica, 2011).

Sykes and Matza (1957) proposed a theory they called, "techniques of neutralization" to explain attitudes of juvenile delinquency which can be applied to griefers. These techniques are rationalizations that justify deviant behavior and include denial of responsibility, denial of injury, denial of victim, condemnation of the condemners, and appeal to higher loyalties (Lilly, Cullen, & Ball, 2007). Griefers do not use all of these techniques of neutralization, such as denial of responsibility, as they often want the notoriety that comes with taking responsibility for their behavior (Dibbell, 2008). They do, however, claim denial of injury, denial of victim, and condemnation of the condemners, claiming that everything they do online is just a game and that people shouldn't take the Internet so seriously (Dibbell, 2008; Lin & Sun, 2007). In the case of

the LambdaMOO rape the response of the perpetrator was that it was only a game and that he was indulging in some harmless “mind control” (Dibbell, 1993). Statements such as this definitely deny injury, victimization, as well as responsibility for the behaviour. While some individuals, who harass others online, see themselves as rebelling against social norms, others simply do not accept them, “You pay to play with unintelligent artificial characters, I pay to play you” (griefer as cited in Lin & Sun, 2005).

Gottfredson and Hirschi’s (1990) general theory of crime, a control theory, is based on a single premise: low self-control. These theorists view deviance as a function of ineffective or incomplete socialization (particularly poor parenting) that results in low self-control (Gottfredson & Hirschi, 1990). Given that a large number of the individuals who grief are university students and otherwise well behaved in their lives, low self-control is not a particularly viable theory to explain online deviance.

Further research into social bonding and online communities will need to be conducted before a full application of social control theories can be applied to online deviant behavior. Despite our limited knowledge of online communities, there is evidence that the majority of those playing games and interacting in metaverses do care deeply about social norms, are capable of forming intense, emotional attachments (Walther & Tidwell, 2007), and wish to be accepted by their community. This provides a foundation from which to begin researching how, exactly, these social norms exert influence on those who might be otherwise be tempted to commit deviant and/or criminal behavior.

Psychological and social control theories rely heavily on the inner motivations and the outer containment of behaviours. Other theories, such as routine activities theory, are predicated on the intersection of perpetrator and victim in time and space. The following will examine the suitability of routine activity as an explanation for online harassment.

5.1.3. Routine Activity Theory

For victimization to occur, Cohen & Felson’s, (1979) routine activity theory relies on the intersection of a motivated offender, suitable target, and the absence of a capable guardian (Cohen & Felson 1979 as cited in Akers & Sellers, 2009). Routine activities theory must be re-imagined to accommodate asynchronicity, in computer-mediated communications, in regards to the intersection of offender, target, and lack of

guardianship. If re-imagined in this manner, the offender and victim do not have to converge in real-time because of the unique quality of permanence to online communications. In this way, the crime must be seen to occur when the victim becomes aware of his or her victimization (e.g., reading the message board or receiving the message in their social network or via text or email). Viewed in this manner, the Internet provides the conduit for the interaction and acts as a proxy for physical space (Reyns et al., 2011).

Studies of cyber-stalking show that victimization is high. In a sample of college students it was found that 46% of women and 32% of men had experienced it (Reyns, Henson, & Fisher, in press cited in Reyns et al., 2011). Using routine activities theory as the foundation for their research, Reyns et al. (2011) concluded that the number of photos posted in online social networks, the number of social networking accounts, permitting strangers to view personal information (posted on social networking sites), and the use of AOL Instant Messenger were significant, positive predictors of receiving unwanted online sexual advances – demonstrating that online victims do vary in suitability and attractiveness (Holt & Bossler, 2008).

The use of a profile tracker was also a positive predictor of victimization. Profile trackers are designed to monitor social network activity so that an individual can see if someone is repeatedly viewing their profile and then watch to see if troubling patterns of behaviour emerge (Holt & Bossler, 2008). Those using trackers may have already experienced stalking and thus may already be at higher risk of victimization (Reyns et al., 2011). This, again, demonstrates that certain individuals appear to be more suitable targets than others and that guardianship, in this manner, does not seem to work.

Deviant peers and the lack of capable guardians had the effect of increasing victimization with gender, physical beauty, and relationship status modifying composite target attractiveness (Holt & Bossler, 2008). Being female doubled the likelihood of victimization while prior victimization tripled the risk of sexual advances online and multiplied the likelihood of being physically stalked by 1.8 times (Holt & Bossler, 2008).

In studies of griefing, researchers found that white-eyed players view their activities as opportunistic (Lin & Sun, 2005). These players are motivated, the opportunity presents itself, and there are no effective guardians to protect the suitable victim (Lin & Sun, 2005). Opportunity, online, appears to be a factor of such things as asynchronous communication which allows for greater planning in deception. This

facilitates the use of ambiguity in favour of the deceiver (Galanxhi & Nah, 2005). Ultimately, "the Internet also provides…an almost endless supply of potential victims" (Reyns et al., 2011, p. 1149), almost unlimited opportunity, with little guardianship. Organized griefing groups appear to be always on the look-out for opportunity. These groups persistently troll the Internet for individuals and items of interest as evidenced by the large number of the Internet memes they are responsible for creating (element of culture or system of behavior transmitted from individual to individual non-genetically (Barber, 2004)).

5.1.4. Theoretical Summary

Given the short history of online social networks, metaverses, and games, online deviant behaviours have only just begun to be studied. Despite the newness of these online social places, the application of criminological theory can provide insight and explanation for some of the behaviours especially those that contravene social conventions and community standards. Some research has already been conducted into routine activities (e.g., "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization" by Holt & Bossler (2008); "Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory" by Marcum, Ricketts, & Higgins (2010); and "Being pursued online: Applying cyberlifestyle-routine activities theory to cyberstalking victimization" by Reyns et al., (2011)). More research into the disinhibition effect, social control, and routine activities is certain to be conducted as researchers strive to understand anti-social behavior in these new realms. There are also a number of other criminological theories that could be applied to online deviance and criminal behavior, including differential association, social learning, feminist theories, social disorganization, and life-span theories. All of which may offer further insight into the perpetration of violent online acts and virtual violent victimization.

5.2. Discussion, Recommendations, and Conclusion

Where cyber-harassment and cyber violence exists, there is neither freedom of speech nor freedom of person. The very act of stalking, assaulting, and harassing

another removes their freedoms by restricting their voice and movement both in cyberspace and physical space. Many of those victimized online withdraw from social cyber-places as well as social physical places while the unknown assailant goes free - this is neither fair nor right. Canada and the United States, as countries and communities, rely on the established norms as well as laws to ensure that the inalienable rights and freedoms of their citizens are assured. Therefore, online violent victimization must be adequately responded to both socially and legally.

It is clear that the Internet has radically altered the lives of North Americans. Online social spaces provide platforms for the exchange of emotion, art, ideas, information, and much more. The fact that some, who use this media, would do so to violate the rights of others to stalk, harass, and assault is unacceptable and our courts must respond in a reasoned and fair manner. While it is true that it takes time for legislative processes to catch up with technological change, the recognition that human behavior has remained much the same in cyberspace as it has always been in physical space offers the appropriate direction our courts should take. First, we need to clearly demarcate the boundary between online play spaces and those that are extensions and expansions of our offline spaces. Second, we need to begin the debate on the quasi-human quality of avatars when they represent our physical selves in online spaces that are not fantastical play spaces. Third, we need to ensure that existing legislation for harassment, with the proposed amendment of Bill C-273, is applied consistently to acts of online violence which, at this point until the nature and value of the avatar is better understood, must be applied to cyber rape in addition to harassment and stalking.

Understanding that cyberspace is simply an extension of physical space, with meaningful interaction, including the production of valuable artifacts, has successfully led judges, legislators, and legal scholars to apply existing legislation to virtual artifacts. Therefore, there is no reason why existing legislation cannot be applied to virtual victimization. In the same way that our courts have begun to assess the value of virtual goods our courts should be able to assess the meaning behind virtual, violent victimization of avatars. This includes threatening emails or text messages, the posting of threatening, harassing, and defaming messages in public, online social forums whether they are aimed at the physical person or the online representative of the person (in the form of an avatar, be it 3D, text, or some other format). It is clear that these acts are directed to the person behind the avatar and therefore meaningful to humans. If the

individual behind the avatar feels the threat as genuine and honestly fears for their safety or the safety of others close to them, then pursuing the individual by applying existing harassment laws should fulfill both the need for legal recourse as well as place greater restrictions on the freedom to perpetrate these threats. Pursuing legal recourse, whether criminal or civil offers general and specific deterrence and recognizes the damage that is done through these acts.

When it comes to harassment, increased legislation is not the solution. The solution is the appropriate application of current legislation with the proposed amendment to s. 264 of the *Criminal Code*. Bill C-273, the proposed change to this section of the *Criminal Code*, states, "For greater certainty, paragraphs (2)(*b*) and (*d*) apply in respect of conduct that is communicated by means of a computer or a group of interconnected or related computers, including the Internet, or any similar means of communication." Allowing reform, in this manner, will enhance existing legislation and allow it to be consistently applied to cyber-harassment and cyber-stalking cases and help rebalance the power in cyberspace by allowing freedom of speech for all while protecting the rights of those who have been victimized by others.

Legislative reform is a normal practice in Canada. In prior years, revisions to s. 264 of the *Criminal Code* have been made and, in one such case, *R. v. Hinchey* (1996), Madame Justice L'Heureux-Dubé stated the following:

> The notion of criminality, thus, is not a static one, but one which very much changes over time. As society changes, the conception of what types of conduct can properly be considered criminal also evolves. There are a myriad of different activities which at one point in time were considered legal, but which we now consider criminal. The offence of criminal harassment is one obvious example. For many years, it was not recognized as criminal to persistently follow someone and cause them to fear for their safety, so long as no contact was made. Now, that has distinctly changed with the addition of s. 264 of the *Code*, which makes this conduct a crime. (Madame Justice L'Heureux-Dubé, 1996)

Therefore, the proposed amendment to s. 264, Bill C-273, is not unusual and must be considered given the apparent permanence of electronic communications in the lives of North Americans.

The issue of freedom of expression, as enshrined in the *Canadian Charter of Rights and Freedoms*, versus harassment laws (s. 264 of the *Criminal Code*) has also

been judiciously examined and the law was found to infringe on the freedom of speech rights of Canadians, but to a reasonable degree. Arguments that s. 264 is overly vague and broad and, should thus be voided, under sections 2(b) (freedom of expression) and 7 (life, liberty, and security of person) of the *Canadian Charter of Rights and Freedoms* were found to have no merit (e.g., *R. v. Hau*, 1994 and *R v. Hau*, 1996) with the constitutionality of the section upheld. Justice Berger found that s. 2(b) of the *Charter* does not apply to ss. 264(2)(a) or (c) of the *Code*, denying a s. 7 argument that posited s. 264 "allows the morally innocent to be punished" (e.g., *R. v. Sillipp*, 1997). Justice Michaud supported this decision in the year 2000 and claimed that there was "no merit to a constitutional challenge of s. 264(2)(c) of the *Code."* In further challenges (see *R. v. Davis*, 1999), the court supported the *Sillipp* (1997) decision and conceded that the communication component of the provision did violate s. 2(b) of the *Charter,* but the "laudable objective of the criminal harassment legislation far outweighs the negative impact that it has on freedom of expression." All subsequent challenges have been thus denied based on these decisions (see *R. v. Krushel*, 2000, leave to appeal, 2002). Canadian courts have considered the conflict between freedom of expression and freedom from harassment and found that the two can co-exist as they stand.

In comparing the effect of cyber-rape, cyber-harassment, and cyber-assault, discernible differences seem small. In all cases the victim experiences distress and fear and in all cases the experience has the potential for repeatedly victimizing the individual by the very permanence of online communications. This can be seen as an aggravating factor and, as prior cases have shown, is already accounted for in Canada's harassment laws. Harassment is "repeatedly following" or "repeatedly communicating" (s. 264. (2) (a) and (b)) and/or "engaging in threatening conduct" (s. 264. (2)(d)). The permanence of the communications, and subsequent harassment violations, due to the nature of the Internet to magnify and disperse information, does not change the crime. It may only be considered to enhance it, assuring the court that a crime had, indeed occurred. Individuals who knowingly publish, in online spaces, messages intended to defame, harass and/or emotionally harm others must be held liable for their actions. Regardless of location, based on our understanding of the realness of cyber-places and the significance of the personal representations we place there, cyber-stalking and cyber-harassment are as real in cyberspace as they are in physical space. Physically stalking someone or repeatedly communicating or threatening via telephone, radio, television or

any other historic communications medium is only minimally different with the difference bounded only in the communications device, not in intention or effect.

The significance of sexual assault online must also be considered. As is evident in this thesis, the representations of the self that are created and placed in online space are meaningful and significant to their creator and take on the same role in cyberspace as our physical bodies do in physical space. While current harassment and stalking legislation can be used to prosecute these acts of online sexual violence as long as the behaviour is interpreted as threatening and there is evidence that the victim genuinely fears for their safety, in the future an amendment or clarification, recognizing the role of the avatar as quasi-human and explicitly including acts of online sexual violence may help courts to make appropriate decisions regarding the prosecution and punishment for violent sexual behaviour perpetrated against avatars. In this way it would recognize the unique nature of online sexual violation and the harm that it does. Punishment for these acts, if prosecuted under s. 264, is adequate as it currently stands, as the punishment for the crime of harassment is harsher (prison term not exceeding 10 years) than for assault (prison term not exceeding five years).

The confusion as to the significance of online harassment, for those who perpetrate these acts, appears to be partially bounded in the cultural history of the Internet and the false belief that these online spaces are somehow free of the rules and laws that bind human behavior – they are not. Historic arguments that insisted online spaces were meaningful in different ways than physical space and would govern themselves have been predominantly disproven by the fact that cyber places and the constructed persons we place there have real significance and meaning, metaphorically, cognitively, emotionally, and through the trust which forms and is maintained within them.

Current criminological theories offer some insight into the psychological processes and contextual factors that lead individuals to online acts of harassment. These theories may also help us ascertain what strategies might be employed to divert some individuals from perpetrating these crimes. For some individuals it must certainly be a lack of understanding regarding the power of their messages to harm in online realms. Education is one way in which we can help everyone who uses the Internet, as a form of communication and social interaction, to understand the meaning of the communicative acts that occur there. Through terms of service and EULAs that are

clear and concise as to community standards and rules that govern these places users may be educated to understand that there is no difference between communications that are bound in historic mediums and communications conducted via the Internet. These contracts must also clearly define the spaces that are fantastical play spaces found in immersive games as compared to spaces that act as extensions of our physical world lives.. Clear warnings, similar to those placed in the entrances to unfamiliar or unusual places, would help clarify the meaning of these places for those who are operating under the false belief that computer-mediated communications are free of the standard rules and laws that govern all other types of communication.

While it is true that the very nature of the Internet, with its packet-switching technology and multiple jurisdictions, will offer very real challenges to our legal system, it is not true that it is its own place, free of the laws and rules the guide our lives in physical space. The social spaces of the Internet are very much an extension and expansion of the social spaces of our physical world, filled with the meaningful symbolism of language and, therefore, must be subject to the same rules that bind social interactions of humans in the physical world. Understanding this illuminates the very real nature of virtual harm and violations of trust and demonstrates that these are very capable of producing real damage for those victimized.

Efforts to regulate Internet harassment may also have to be attended to through modification of existing laws, such as the *Communications Decency Act of 1996.* Currently, based on this law of the United States, companies and individuals who host sites upon which harassing messages are posted or sent, are absolved of liability. It is considered that those hosting sites cannot possibly monitor the activity on them to the degree that they would be held liable in the case of harassment. This act was passed to ensure the freedoms of speech were supported in cyberspace. While it is admirable and even necessary to ensure the right to free speech, this must be balanced against the right for others to be free of harassment. After all, we already have limits on our freedom of speech with “hate speech” (Canada *Criminal* Code ss. 318, 319, and 320) disallowed. One potential partial solution would be mandatory registration for users of all online sites with clear rules of acceptable use embedded into clickwrap licenses carrying warnings that violations will be dealt with under criminal law. While this won’t prevent all cases of harassment it would certainly help to educate those using these online social spaces so that they might understand that the same laws and community standards that govern

offline spaces, govern those online. The added benefit of clearly worded warnings in clickwrap licenses is that identification of the type of online social space could be clearly spelled out ensuring that individuals understand the difference between fantastical play spaces and those that are an expansion and extension of our physical lives.

The creation of a "law of interration", proposed by Professor Castronova (2004), will allow a strong boundary or magic circle to be drawn around the fantastical worlds found in immersive games and protect these spaces from physical world laws by defining the types of activities that are unlikely to give rise to criminal and tortuous liability. A law of interration is a specific act of government that "grants EULAs a legal status robust enough to allow them to preserve synthetic worlds as play spaces" (Castronova, 2004). These laws would create closed and open worlds. Closed worlds (games) would be provided a strong, impermeable border between the synthetic world and the real word with the EULAs determining the laws and rules, and open worlds would maintain porous borders where the real world laws would be in effect (Castronova, 2004). A law of interration would permit the developers and providers of games and metaverses to determine which type of online space they prefer to host and thus determine whether players and users are bound by the legislation of the country in which they reside or bound by the rules of play as explicated in the EULA. This would provide users and players with assurance that behaviours that might be construed as harassment or violent victimization in the physical world are not subject to prosecution because they are occurring within the magic circle and thus part of game-play.

The most critical thing in drafting a law of interration is to ensure that the types of worlds are clearly defined. Immersive games and metaverses, that act solely as extensions of our physical world, must not be viewed in the same manner as they are different and, as such, both should not be subject to the laws of physical space. Immersive games are fantastical places that often center on activities that, if conducted in the physical world, would lead to criminal charges. It is not logical to apply physical world law to these places. Games are fantasy as compared to metaverses. Metaverses act as an expansion and extension of our physical world, with businesses and universities and communities and living spaces that must be governed by existing legislation as they act very much in the same way our physical world does.

The companies that host the game or metaverse should be charged with determining what type of online space they are and this can be detailed in their EULA. EULAs can be reinforced through the coding used to create and facilitate the world.

Worlds that are determined to be games, or existing within the magic circle, must not act in any way like the physical world and therefore, may have no commerce. In fact, nothing that exists in the physical world, except the players, can be real and all the play space and everything within it must be fantasy. Here, players, according to the rules of the game embedded in the EULA, may act as they please without concern for the criminal laws of the country in which they reside. If artifacts from within the game are transported outside the game for trade, sale, or purchase, then they must be subject to the laws of the country.

Worlds that are an extension of our physical world – places where we learn, play, shop etc. should be considered extensions of the physical world and subject to the laws that exist wherever the individual resides. If you go inside Second Life and design a pair of Adidas shoes at the Adidas store and then have them delivered to your physical world address so that you can wear them, regardless of whether you pay in Linden Dollars, American Dollars, Canadian Dollars, Euros etc. the shoes are real and subject to the laws of commerce in the physical country in which you live. In the same way, the behaviours of individuals will be subject to the laws of the country in which they reside depending on whether they are immersed in a metaverse or immersed in a game.

The issue of jurisdiction for games, metaverses, and social networks, in cases of criminal harassment, must be in the country where the victim resides. As discussed, games will embed their rules and community standards into the EULA and online mediation will probably suffice for any violations. The United States court in *Bragg v. Linden Research, Inc*. (2006), determined that it was unfair for companies to hold mediations at a set location in the world given the likelihood of hardship for those not residing in the location the company chooses. Therefore, given that rules of play will be clearly spelled out in the EULA, online mediation with either court appointed or agreed upon mediators should suffice. This allows equal distance for all involved and places no undue hardship.

For those who are the victims of cyber-harassment and cyber-stalking, it is not unusual to find that it is a “local cybercrime” in that the victim and the perpetrator reside in the same jurisdiction (Brenner, 2008). As was seen in the AutoAdmit case, all the

perpetrators were in the same national jurisdiction as the victims. It is probable that this is a common occurrence given how interest develops in stalking cases and that the behaviours involved often move between the offline and online realms. Sheer harassment may be less likely to move between the two realms, in which case, the crime should be considered to have occurred where the victim resides.

Ultimately, those who use the Internet to communicate must understand that our rights of freedom of expression are not rights to harm others. Cyberspace offers an amazing opportunity to be free of the constraints that the physical world and our physical bodies impose but cyber-harassment and cyber violence violate those freedoms. Criminal harassment compromises everyone's right of enjoyment of the Internet and this compromise extends into the physical world damaging the possibility for social interactions that we might enjoy. Socially and legally we must consider the communicative acts that impose these restraints as criminal and address them through legal reform and major educational reform so that everyone who uses the Internet might experience the freedom that it has the power to confer.

References

Adbusters. (2011). Occupy Wallstreet. *Adbusters* "Occupy Wallstreet" page. Retrieved from http://www.adbusters.org/blogs/adbusters-blog/occupywallstreet.html

Adrian, A. (2006). Intellectual property or intangible chattel. *Journal of Intercultural Information & Management 1*(4), 331-343. doi: 10.1504/IJIIM.2009.025939

Adrian, A. (2010). Beyond griefing: Virtual crime. *Computer Law & Security Review 26*(2010), 640-648. doi: 10.1016/j.clsr.2010.09.003

Akers, R. L. & Sellers, C. S. (2009). Social Disorganization, anomie, and strain theories. In, *Criminological theories: Introduction, evaluation, and application* (5th ed.) (pp.177-210). New York, NY: Oxford University Press.

American Psychiatric Association. (2000). Posttraumatic stress disorder. In, *Diagnostic and Statistical Manual of Mental Disorders,* (4th ed.), text revision. Washington, DC: American Psychiatric Association.

Applemilk1988. (2012). In *Encyclopedia Dramatica*. Retrieved from http://encyclopediadramatica.se

Arias, A. V. (2008). Life, liberty, and the pursuit of swords and armor: Regulating the theft of virtual goods. *Emory Law Journal, 57*(5), 130-145. Retrieved from http://www.law.emory.edu//student-life/law-journals/emory-law-journal.html

Arnold, A. M. (1998). Rape in cyberspace: Not just a fantasy. *Off Our Backs, 28*(2), 12-13. Retrieved from http://www.jstor.org/stable/20835976

AutoAdmit (2012). The most prestigious law school discussion board in the world. *AutoAdmit.com.* Retrieved from http://www.xoxohth.com/

Axelrod, R. (1980). Effective choice in the prisoner's dilemma. *Journal of Conflict Resolution, 24*(1), 3-25. doi: 10.1177/002200278002400101

Axelsson, A. S. & Regan, R. (2002). How belonging to an online group affects social behavior – A case study of Asheron's Call. *Microsoft Technical Report,* (MSR-TR-2002-07). Retrieved from http://research.microsoft.com /apps/pubs/default.aspx?id=69910

Bailenson, J. N. & Segovia, K. Y. (2010). Virtual doppelgängers: Psychological effects of avatars who ignore their owners. In W.S. Bainbridge, (Ed.), *Online worlds: Convergence of the real and the virtual* (pp.175-186). London, UK: Springer-Verlag.

Bainbridge, W. S. (2010a). Introduction and New World View. In W.S. Bainbridge (Ed.) *Online worlds: Convergence of the real and the virtual* (pp. 1 – 21). London, UK: Springer-Verlag.

Bainbridge, W. S. (2010b). When virtual worlds expand. In W. S. Bainbridge, (Ed.) *Online worlds: Convergence of the real and the virtual* (pp. 237-252). London, UK: Springer-Verlag.

Bakioglu, B. (2009). Spectacular interventions in Second Life: Goon culture, griefing, and disruption in virtual spaces. *Journal of Virtual Worlds Research, 1*(3), 1-21. Retrieved from http://jvwresearch.org/

Balkin, J. M. (2004). Virtual liberty: Freedom to design and freedom to play in virtual worlds. *Virginia Law Review, 90*(8), 2043-2098. Retrieved from http://www.virginialawreview.org/

Bandura, A. & Walters, R. H. (1963). *Social learning and personality development.* [Citation Classics, ebooks]. Retrieved from http://garfield.library.upenn.edu/classics1981/A1981MB16700001.pdf

Bansal, A., Sharma, S. M., Kumar, K., Aggarwal, A., Goyal, S., Choudhary, K., Chawla, K., Jain, K., & Bhasin, M. (2011). Classification of flames in computer-mediated communications. *International Journal of Computer Applications, 14*(6), 2-28. Retrieved from http://www.ijcaonline.org/.

Barbatsis, G. Fegan, M. & Hansen, K. (2006). The performance of cyberspace: An exploration into computer-mediated reality. *Journal of Computer-Mediated Communication, 5*(1), 1-22. doi: 10.1111/j.1083-6101.1999.tb00332.x

Bargh, J. A., McKenna, K. Y. A., & Fitzsimons, G. M. (2002). Can you see the real me? Activation and expression of the "true self" on the Internet. *Journal of Social Issues, 58*(1), 33-48. doi: 10.1111/1540-4560.00247

Barlow, J. P. (1996). A declaration of the independence of cyberspace. *The Humanist, 56*(3), 18-21. Retrieved from http://www.thehumanist.org/humanist-content.html

Barnett, J., Coulson, M., & Foreman, N. (2010). Examining player anger in *World of Warcraft*. In W. S. Bainbridge (Ed.), *Online worlds: Convergence of the real and the virtual* (pp. 147-160). London, UK: Springer-Verlag.

Barry, M. (2009, January 20). Fury over cyber site rape hell: Support offered to virtual world members who complain of abuse. *The Mirror.* Retrieved from thefreelibrary.com

Bartol, A. & Bartol, C. (2005). *Criminal behavior: A psychosocial approach* (7th Ed.). Upper Saddle River, NJ: Pearson Education.

Baum, K., Catalan, S., Rand, M. & Rose, K. (2009). Stalking victimization in the United States. *Bureau of Justice Statistics – National Crime Victimization Survey,* (January 2009, NCJ 224527). Retrieved from http://www.ncvc.org

Bernstein, M. S., Monroy-Hernandez, A., Harry, D., Andre, P., Panovich, K., & Vargas, G. (2010). 4chan and /b/: An analysis of anonymity and ephemerality in a large online community. *Proceedings of the Fifth International AAAI Conference on Weblogs and Social Media.* Retrieved from http://eprints.soton.ac.uk/272345/1/4chan-icwsm.pdf

Biegel, A. (1985). Long-term psychological effects of rape in 35 rape victims. *The American Journal of Psychiatry, 142*(11), 1338. Retrieved from http://ajp.psychiatryonline.org/journal.aspx?journalid=13

Bierhoff, H-W. & Vornefeld, B. (2004). The social psychology of trust with applications in the Internet. *Analyze & Kritik, 26*(2), 48-62. Retrieved from http://www.analyse-und-kritik.net/en/2004-1/content.htm

Blascovich, J. & Bailenson, J. (2011). Infinite reality: Avatars, eternal life, new worlds, and the dawn of the virtual revolution. New York, NY: Harper Collins.

Blavin, J. H. (2002). Gore, Gibson, and Goldsmith: The evolution of Internet metaphors in law and commentary. *Harvard Journal of Law & Technology, 16*(1), 265-285. Retrieved from http://jolt.law.harvard.edu/

Boase, J., Horrigan, J. B., Wellman, B., & Raine, L. (2006). The strength of Internet ties. *Pew Internet and American Life Project.* Retrieved from http://www.pewinternet.org/~/media//Files/Reports/2006/PIP_Internet_ties.pdf.pdf

Boellstorff, T. (2008). *Coming of age in Second Life: An anthropologist explores the virtually human.* [Myilibrary version]. Retrieved from: http://lib.myilibrary.com.proxy.lib.sfu.ca/Open.aspx?id=215846&loc=&srch=undefined&src=0

Boulard, G. (2001). Public Internet/private lives. *State Legislatures, 27*(2), 39-43. Retrieved from http://www.ncsl.org/programs/pubs/00slmag.htm

Bowker, N. & Tuffin, K. (2006). Dicing with deception: People with disabilities' strategies for managing safety and identity online. *Journal of Computer-mediated Communication, 8*(2). doi: 10.1111/j.1083-6101.2003.tb00209.x

boyd, d. m. & Ellison, N. B. (2008). Social network sites: Definition, history, and scholarship. *Journal of Computer-mediated Communication, 13*, 210-230. doi: 10.1111/j.1083-6101.2007.00393.x

Brenner, S. (2008). Fantasy crime: The role of criminal law in virtual worlds. *Vanderbilt Journal of Entertainment and Technology Law, 11*, 1 – 106. Retrieved from http://law.vanderbilt.edu/publications/journal-entertainment-technology-law/index.aspx

Brynko, B. (2011). Trust in social networking. *Information Today,* July/August 2011. Retrieved from http://www.infotoday.com/it/itnew.htm

Bugeja, M. J. (2007). Second thoughts about second life. *The Chronicle of Higher Education, 53*. Retrieved from: http://chronicle.com

Burrows, B. (1999). Worlds of knowledge: Europe and the global science and technology agenda. *Futures, 28*(4), 389-390. doi: 10.1016/0016-3287(96)88238-3

Canadian Employment Law Today (2011, June 24). Vancouver rioters fired after being identified. *Canadian Employment Law Today*. Retrieved from http://www.employmentlawtoday.com/ArticleView.aspx?l=1&articleid=2508

Carthage, J. (2009, April 7, 8pm). Field trip: Social aspects of virtual worlds. *Beyond Blogging Conference* in Second Life, [IBM Developer, Web log message]. Retrieved from Lotusphere, IBM 9, Second Life www.ibm.com/lotus/lotusphere

Castronova, E. (2004-2005). The right to play. *New York Law School Legal Review, 49*, 185-210. Retrieved from http://www.nyls.edu/academics/jd_programs/law_review

Chen, M. (2005). Addressing social dilemmas and fostering cooperation through computer games. *Proceedings of Digital Game Research Association (DiGRA) 2005 Conference: Changing Views – World in Play,* 1-7. Retrieved from http://www.digra.org/dl/display_html?chid=06278.44316.pdf

Chisholm, J. F. (2006). Cyberspace violence against girls and adolescent females. *New York Academy of Sciences,* 74-89. doi:10.1196/annals.1385.022

Citron, D. K. (2008). Cyber civil rights. *Boston University Law Review, 89*(61), 61-125. Retrieved from http://www.bu.edu/law/prospective/jd/journals/index.html

Cohen, J. E. (2007). Cyberspace as/and space. *Columbia Law Review, 107*(210), 210-256. Retrieved from http://www.columbialawreview.org

ComScore (2012). Top 10 need-to-knows about social networking and where it's headed. *ComScore*, 2012. Retrieved from http://www.comscore.com/Press_Events/Presentations_Whitepapers/2011/it_is_a_social_world_top_10_need-to-knows_about_social_networking

Copeland, L. (2000). Quickstudy: Packet-switched vs. circuit-switched networks. *Computerworld Quickstudies.* Retrieved from: Computerworld.com

Cosmides, L., & Tooby, J. (1992). Cognitive adaptations for social exchange. In J. Barkow, L. Cosmides, & J. Tooby (Eds.), *The adapted mind* (pp. 163-228). New York, NY: Oxford University Press.

Cyber-bullying. (2012). Cyber-bullying and the law fact sheet. In *Media awareness fact sheet.* Retrieved from http://www.media-awareness.ca/english/resources/educational/teaching_backgrounders/cyberbullying/cyberbullying_law2_h4.cfm

Cyberspace. (2012). *Webopedia.* Retrieved from http://www.webopedia.com/TERM/C/cyberspace.html

D'Ovidio, R. & Doyle, J. (2003). A study on cyberstalking: Understanding investigative hurdles. *FBI Law Enforcement Bulletin, 72*(3), 10-17. Retrieved from http://www.fbi.gov/publications/leb/leb.htm

Davidson, S. J. (2008). An immersive perspective on the Second Life virtual world. *The Computer & Internet Lawyer, 25*(3), 1-16. Retrieved from http://www.aspenpublishers.com/

DeKeseredy, W. S., Ellis, D. & Alvi, S. (2005). Woman Abuse. In *Deviance + crime: Theory, research and policy,* (3rd ed., pp. 89-125). Ottawa, Ont: Anderson Publishing

Denial of service attack. (2001). In *Software Engineering Institute of Carnegie Mellon.* Retrieved from http://www.cert.org/tech_tips/denial_of_service.html

Department of Justice, Canada. (2011). Criminal harassment: A handbook for police and crown prosecutors. *Family Violence Initiative* (December 01, 2011). Retrieved from http://www.justice.gc.ca

Dibbell, J. (1993). A rape in cyberspace or how an evil clown, a Haitian trickster spirit, two wizards, and a cast of dozens turned a database into a society. *Village Voice* reprinted in *Annual Survey of America Law, 3*(471), 471-490. Retrieved from http://www1.law.nyu.edu/pubs/annualsurvey/about_us/index.html

Dibbell, J. (2008). Mutilated furries, Flying phalluses: Put the blame on griefers, the sociopaths of the virtual world. *Wired, 16*(02). Retrieved from http://www.wired.com

Dirty.com. (2012). *The Dirty.com.* Retrieved from http://thedirty.com/

Distributed denial of service attack. (2000-2012). WhatIsMyIPAddress. Retrieved from http://whatismyipaddress.com/ddos-attack

Donnath, J. & boyd, d. (2004). Public displays of connection. *BT Technology Journal, 22*(4), 71-82. doi: 10.1023/B:BTTJ.0000047585.06264.cc

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends": Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*(2007), 1143-1168. doi: 10.1111/j.1083-6101.2007.00367.x

EVE faq. (2012). What is EVE? Frequently asked questions, *EVE Online.* Retrieved from http://www.eveonline.com/faq/what-is-eve-online/

Ever Quest II. (2012). World Description. *Ever Quest II homepage*. Retrieved from http://www.everquest2.com/

Facebook. (2012). Key facts. *About, newsroom.* Retrieved from http://newsroom.fb.com/content/default.aspx?NewsAreaId=22

Facebook. (2012). Key facts. *Statistics, newsroom.* Retrieved from http://newsroom.fb.com/content/default.aspx?NewsAreaId=22)

Finlayson, A. (2005, March 30). Online gamer killed for selling virtual weapon. *Reuters.* Retrieved from fairfaxmedia.newspaperdirect.com/

Flame War. (2012). In *Urban dictionary online.* Retrieved from http://www.urbandictionary.com

Flaming. (2012). In *Urban Dictionary online.* Retrieved from: http://www.urbandictionary.com

Flaming. (2012). In *Wikipedia.* Retrieved from http://en.wikipedia.org/wiki/

Forsyth, D. R. (2006). *Group Dynamics* (4th ed.). Belmont, CA: Thomson Wadsworth.

Franks, M. A. (2011). Unwilling avatars: Idealism and discrimination in cyberspace. *Columbia Journal of Gender Law, 20*(2), 225-261. Retrieved from http://www.columbia.edu/cu/jgl/

Fukuchi, A. (2011). A balance of convenience: The use of burden-shifting devices in criminal cyberharassment law. *Boston College Legal Review, 52*(1), 289-338. Retrieved from http://www.bc.edu/schools/law/lawreviews/bclawreview.html

Fullhouse, R. (2011). Vancouver riot: Post your photos. *Facebook.* Retrieved from https://www.facebook.com/vancouverriot2011photos/info

Galannxhi, H. & Nah, F. F. (2007). Deception in cyberspace: A comparison of text-only vs. avatar-supported medium. *International Journal of Human-Computer Studies, 65*(9), 770-783. doi: 10.1016/j.ijhcs.2007.04.005

Gauntlet. (2012). *Wikipedia.* Retrieved from http://en.wikipedia.org/wiki/Gauntlet_(1985_video_game)

Gibson, W. (1984). *Neuromancer.* New York, NY: Berkley Publishing Group.

Gilbert, E. & Karahalios, K. (2009). Predicting tie strength with social media. In *Proceedings of the 27th International Conference on Human Factors in Computing Systems.* doi: 10.1145/1518701.1518736

Goldsmith & Wu, (2006). *Who controls the Internet?: Illusions of a borderless world.* (Myilibrary ebook). Retrieved from http://lib.myilibrary.com.proxy.lib.sfu.ca/Open.aspx?id=53247&loc=&srch=undefined&src=0

Gorey, K., Richter, N., & Schnider, E. (2001). Guilt, isolation, and hopelessness among female survivors of childhood sexual abuse: Effectiveness of group work intervention. *Child Abuse and Neglect, 25*(2001), 347-355. doi: 10.1016/S0145-2134(00)00255-6

Gottfredson, M. R. & Hirschi, T. (1990). *A General Theory of Crime.* Stanford, CA: Stanford University Press.

Gratch, J. & Kelly, J. (2009). MMOGs: Beyond the wildest imagination. *Journal of Interactive Learning Research, 20*(2), 175-187. Retrieved from http://www.editlib.org.proxy.lib.sfu.ca/index.cfm?fuseaction=Reader.ViewIssues&source_code=JILR

Gribbon, A. (2011). A brief history of the Internet. *New Statesman, 140*(5066), 30. Retrieved from http://www.newstateman.com

Griefing. (2004). *Urban Dictionary Online.* Retrieved from http://www.urbandictionary.com/

Griefing. (2012). *Wikipedia.* Retrieved from http://en.wikipedia.org

Griffiths, C. (2007). *Canadian Criminal Justice: A Primer, Third Ed*. Toronto, Ont.: Thomson/Nelson Publishing.

Gunkel, D. J. (2010). The real problem: Avatars, metaphysics, and online social interaction. *The New Media Society 12*(127). doi: 10.1177/1461444809341443

Hafner, K. & Lyon, M. (1996). *Where wizards stay up late.* New York, NY: Simon & Schuster.

Hardin, R. (1996). The street-level epistemology of trust. *Politics Society, 21*(4), 505-529. doi: 10.1177/0032329293021004006

Hardin, R. (1996). Trustworthiness. *Ethics, 107*(1), 26-42. Retrieved from http://www.jstor.org/stable/2382242

Helliwell, J. F. & Putnam, R. D. (2004). The social context of well-being. *Philosophical Transactions of the Royal Society,* 359(1449), 1435-1446. doi: 1.1098/rstb.2004.1522

History.com. (1999, January, 19). Man charged in California cyberstalking case. *This Day in History – Crime,* January 19, 1999. Retrieved from http://www.history.com/this-day-in-history/man-charged-in-california-cyberstalking-case

Hof, R. D. (2006). My virtual life. *Business Week,* May 1, 2006. Retrieved from http://www.businessweek.com/magazine/content/06_18/b3982001.htm

Holt, T. J. & Bossler, A. M. (2008). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*(1), 1-25. doi: 10.1080/01639620701876577

Howie, M. (2009, January 19). Rape crisis to open office in cyberspace world. *The Scotsman.* Retrieved from http://www.thescotsman.com

Huff, C., Johnson, D. G., & Miller, K. (2003). Virtual Harms and Real Responsibility. *IEEE Technology and Society Magazine,* Summer, 2003, 12-19. Retrieved from http://www.ieee.org

Huh, S. & Williams, D. (2010). Dude looks like a lady: Gender swapping in an online game. In W. S. Bainbridge (Ed.), *Online worlds: Convergence of the real and the virtual,* (pp. 161-174). London, UK : Springer-Verlag.

Hunter, D. (2003). Cyberspace as place and the tragedy of the digital anti-commons. *California Law Review, 91*(2), 439-519. Retrieved from http://clr.boalt.org

Hunter, D. & Lastowka, F. G. (2003). To kill an avatar. *Legal Affairs*, July-August 2003. Retrieved from: Legal Affairs Online.

Hunter, D. & Lastowka, F. G. (2005). Virtual crimes. *New York Law School Legal Review, 293,* 293-316. Retrieved from http://www.nylslawreview.com/

IN FULL FORCE. (2012). In The Free Dictionary Online. Retrieved from http://idioms.thefreedictionary.com

Infosec Island (2012). F.B.I. warns companies of anonymous DDoS attacks. *Infosec Island,* Friday, May, 25, 2012. Retrieved from http://www.infosecisland.com

Introjection. (2004). In K. Barber (Ed.), *Canadian Oxford Dictionary*, (2nd ed., p. 791). Don Mills, Ont.: Oxford University Press.

IP (nd). What's my IP? Retrieved from http://www.whatsmyip.us/

Jennett, C., Cox, A. L., Cairns, P., Dhoparee, S., Epps, A., Tijs, T., & Walton, A. (2008). Measuring and defining the experience of immersion in games. Retrieved from http://www-users.cs.york.ac.uk/~pcairns/papers/JennettIJHCS08.pdf

Johnson, D. R. & Post, D. G. (1996). Law and Borders: the Rise of Law in Cyberspace, *Stanford Law Review, 48*(5), pp. 1367-1402. Retrieved from http://stanfordlawreview.org

Joyce, R. A. (2008). Pornography and the Internet. *Internet Computing, IEEE, 12*(4), 74-77. doi: 10.1109/MIC.2008.83

Kane, S. F. (2009). Virtual judgment: Legal implications of online gaming. *IEEE Security & Privacy.* doi: 10.1109/MSP.2009.81

Kaneva. (2012). *About Kaneva*. Retrieved from http://www.kaneva.com/\

Kay, R. (2007). Online social networks: These sites can facilitate connections in your industry or around the world. *ComputerWorld, 41*(4), 56. Retrieved from http://www.computerworld.com

Kennedy, R. (2009). Law in virtual worlds. *Journal of Internet Law, 12*(10), 3-10. Retrieved from http://www.aspenpublishers.com

Kenney, J. S. (2010). *Canadian Victims of Crime: Critical insights.* Toronto, Ont: Canadian Scholars' Press.

Kleinrock, L. (2010). An Early History of the Internet. *IEEE Communications Magazine, August 2010,* 26 – 36. Retrieved from http://ieee.org

Kleinrock, L. (2002). Creating a Mathematical Theory of Computer Networks. *Operations Research, 50*(1), 125-131. Retrieved from http://or.journal.informs.org

Kollock, P. & Smith, M. A. (1999). Communities in cyberspace. In M.A. Smith & P. Kollock (Eds.), *Communities in Cyberspace* (pp3 – 25). New York, NY: Routledge.

Korsgaard, M. A., Picot, A. Wigand, R. T., Welpe, I. M., & Assmann, J. J. (2010). Cooperation, coordination, and trust in virtual teams: Insights from virtual games. In W.S. Bainbridge (Ed.), *Online worlds: Convergence of the real and the virtual,* (pp. 253-264). London, UK : Springer-Verlag.

Kreidler, M. (2005). Group therapy for survivors of childhood sexual abuse who have chronic mental illness. *Archives of Psychiatric Nursing, 19*(4), 176-183. doi: 10.1016/j.apnu.2005.05.003

Krikke, J. (2003). Samurai Romanesque, J2ME, and the battle for mobile cyberspace. *Computer Graphics and Applications, IEEE, 23*(1), 16-23. Retrieved from http://ieee.org

Lastowka, F. G. & Hunter, D. (2004). The laws of the virtual worlds. *California Law Review, 92*(1), 1-73. Retrieved from http://www.jstor.org/stable/3481444

Lastowka, F. G. & Hunter, D. L. (2004-2005). Virtual crimes. *New York Law School Legal Review, 49,* 293-316. Retrieved from http://www.nylslawreview.com/

Lea, M. & Spears, R. (1995). Love at first byte? Building personal relationships over computer networks. In J. T. Wood & S. Duck (Eds,), *Understudied relationships: Off the beaten track* (pp. 197-233). London, UK: Sage.

Ledgerwood, G. (2009). Virtually liable. *Washington & Lee Law Review, 66*, 811-865. Retrieved from http://law.wlu.edu/journals/lawreview/

Lemley, M. A. (2003). Place and cyberspace. *California Law Review, 91*(2), 525-542. Retrieved from http://www.jstor.org/stable/3481337

Lessig, L. (1999). *Code and Other Laws of Cyberspace.* New York, NY: Basic Books.

Lilly, J. R., Cullen, F. T., & Ball, R. A. (2007). *Criminological Theory: Context and Consequences* (4th ed.). Thousand Oaks, CA: Sage.

Lim, H. Y. F. (2010). Virtual world, virtual land but real property. *Singapore Journal of Legal Studies, 304-327.* Retrieved from http://www.law.nus.edu.sg/sjls

Lin H. & Sun, C. T. (2005). The 'white-eyed' player culture: Grief play and construction of deviance in MMORPGs. *Proceedings of DiGRA 2005 Conference: Changing Views – Worlds in Play.* Retrieved from http://www.digra.org/dl/display_html?chid=06278.44316.pdf

LinkedIn (2012). Homepage. *Linked in.* Retrieved from http://ca.linkedin.com/)

Lombardi, J. & Lombardi, M. (2010). Opening the Metaverse. In W. S. Bainbridge (Ed.) *Online worlds: Convergence of the real and the virtual.* London, UK: Springer.

Lulz. (2012). *Urban Dictionary Online.* Retrieved from http://www.urbandictionary.com/

Lynn, R. (2007). Virtual rape is traumatic, but is it a crime? *Wired, 05-04-07.* Retrieved from http://www.wired.com/culture/lifestyle/commentary/sexdrive/2007/05/sexdrive_o5o4

MacKinnon, R. (2006). Virtual rape. *Journal of Computer-Mediated Communication, 2*(4). doi: 10.1111/j.1083-6101.1997.tb00200.x

Mann, B. L. (2008). Social networking websites – a concatenation of impersonation, denigration, sexual aggressive solicitation, cyber-bullying or happy slapping videos. *International Journal of Law and Information Technology, 1-16.* doi: 10.1093/ijlit/ean008

Margolick, D. (2009). Slimed online. *Conde Nast Portfolio, 3*(2), 80. Retrieved from http://www.condenast.com/

Marcum, C. D., Ricketts, M. L, & Higgins, G. E. (2010). Assessing sex experiences of online victimization: An examination of adolescent online behaviors using routine activity theory. *Criminal Justice Review, 35*(412). doi: 10.1177/0734016809360331

Markova, I. & Gillespie, A. (2008). Preface. *Trust and Distrust: Sociocultural Perspectives* (pp. xvii to xvix). [IE book/Kindle Edition]. Charlotte, VA: Information Age Publishing.

Martey, R. M. & Stromer-Galley, J. (2007). The digital dollhouse: Context and socialnorms in The Sims Online. *Games and Culture, 2*(4), 314-333. doi: 10.1177/1555412007309583

McCall, R. (2003). Online harassment and cyberstalking: Victim access to crisis, referral and support services in Canada concepts and recommendations. *Victim Assistance Online Resources.* Retrieved from http://www.vaonline.org/

McLaughlin, C. & Vitak, J. (2012). Norm evolution and violation on Facebook. *New Media Society, 14*(2), 299-315. doi: 10.1177/1461444811412712

Melvin, J. (2012, January 20). SOPA stopped after unprecedented online protests. *The National Post Online*. Retrieved from http://news.nationalpost.com/2012/01/20/sopa-stopped-after-unprecedented-online-protests/

Mennecke, B. E., Triplett, J. L., Hassall, L. M., Conde, Z. J. & Heer, R. (2011). An examination of a theory of embodied social presence in virtual worlds. *Decision Sciences, 42*(2), 413-450. doi: 10.1111/j.1540-5915.2011.00317.x

Meyers, D. G. & Spencer, S. J. (2007). Conformity. In D. G. Meyers & S. J. Spencer (Eds.), *Social Psychology* (3rd Canadian ed., pp. 170-201). New York, NY: McGraw-Hill Ryerson

Mitchell, W. (1996). City of Bits: Space, Place, and the Infobahn. Kindle Edition. Cambridge, MA: MIT Publishing,

Moor, P. J., Heuvelman, A., & Verleur, R. (2010). Flaming on YouTube. *Computers in Human Behavior, 26*(2010), 1536-1546. doi: 10.1016/j.chb.2010.05.023

Mullen, P.E., Pathé, G.W., Purcell, R., & Stuart, G. W. (1999). Study of stalkers. *American Journal of Psychiatry, 156*(8), 1244-1249. Retrieved from http://ajp.psychiatryonline.org.proxy.lib.sfu.ca/journal.aspx?journalid=13

MySpace (2012). *About Us. MySpace*. Retrieved from http://www.myspace.com/

Nakamura, L. (2002). Cybertypes: Race, identity, and ethnicity on the Internet. New York, NY: Routledge

Netiquette. (2004). *Urban Dictionary Online.* Retrieved from http://www.urbandictionary.com/

Newbie. (2004). In, K. Barber (Ed.), *Canadian Oxford Dictionary* (2nd ed., p. 1045). Don Mills, Ont.: Oxford University Press.

Nissenbaum, H. (2001). Securing trust online: Wisdom or oxymoron? *Boston University Law Review,* 635, 2001. Retrieved from http://bu.edu/law/lawreview/

Occupy Wall Street. (2012). *Wikipedia*. Retrieved from http://en.wikipedia.org /w/index.php?title=Occupy_Wall_Street&printable=yes

Ogilvie, E. (2000). Cyberstalking. *Australian Institute of Criminology Trends & Issues in Crime and Criminal Justice, No. 166*, September 2000. Retrieved from http://www.aic.gov.au/documents/4/7/A/%7B47A7FA60-8EBF-498A-BB9E-D61BC512C053%7Dti166.pdf

Ogles, J. (2004). Google bombing. *Links and Law Technical Background – Google Bombing.* Retrieved from http://www.linksandlaw.com/technicalbackground-google-bombing.htm

Ontario Ministry of the Attorney General (2009). A self-help guide: How to make an application for a restraining order. *Small Claims Court Guides to Procedures.* Retrieved from http://www.attorneygeneral.jus.gov.on.ca/english/family guides/restraining_order/guide_how_to_make_an_application_for_a_restraining_ order.pdf

Palank, J. (2006). Face it: 'Book' no secret to employers; social sites used as background check. *The Washington Times*, July 17, 2006. Retrieved from http://www.washingtontimes.com/

Parks, M. (2011). Social Network Sites as Virtual Communities. In Z. Papacharissi, (Ed.), *A networked self: Identity, community, and culture on social network sites* (pp.105 – 123). New York, NY: Routledge.

Patriotic Nigras. (2011). *Encyclopedia Dramatica.* Retrieved from http://encyclopediadramatica.se/

Peña, J. & Hancock, J. T. (2006). An analysis of socioemotional and task communication in online multiplayer video games. *Communication Research, 33*(1), 92-109. doi: 10.1177/0093650205283103

Pentecost, K. (2011). Imagined communities in cyberspace. *Social Alternatives, 30*(2), 44-47. Retrieved from http://www.socialalternatives.com

Perritt, H. J Jr. (1996). Jurisdiction in cyberspace. *Villanova Law Review, 41*(1), 1-129. Retrieved from http://www.law.villanove.edu/lawreview/

Pew Research. (2008). Personal Networks and Community Survey (Princeton Survey Research Associates International for the Pew Internet & American Life Project) (July 9 – August 10, 2008). Retrieved from http://www.pewinternet.org/ ~/media//Files/Questionnaire/2009/PIAL%20Networks%20FINAL%20Topline.pdf

Pimentel, J. R. C. & Elenkov D. S. (2010). Did I catch your drift: Examining antecedents of it, flaming in multicultural business settings. *Review of Business Research, 10*(2), 10 – 18. Retrieved from http://www.iabe.org/domains/iabe/journal/aspx?journalid=5

Powers, T. M. (2003). Real wrongs in virtual communities. *Ethics and Information Technology 5*(4), 191-198. Retrieved from http://www.springer.com

Putnam, R. D, Leonardi, R. & Nanetti, R. Y. (1993). Making democracy work: Civic traditions in modern Italy. COCO *The Cooperative Commons* – Summary of research findings. Princeton, NJ: Princeton University Press, [E book]. Retrieved from: http://www.cooperationcommons.com/node/369

Rape. (1998). Rape defined in international law. *UN Chronicle,* (*02517329*)*, 35*(3). Retrieved from http://www.un.org/wcm/content/site/chronicle/

Rape. (2012). Vancouver Rape Crisis Centre. Retrieved from http://www.rapereliefshelter.bc.ca/learn/faq#t3n102

Reid, E. (1999). Hierarchy and power: Social control in cyberspace. In M.A. Smith & P. Kollock, (Eds.), *Communities in Cyberspace* (pp107-133). New York, NY: Routledge.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: Applying cyberslifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior, 38*(11), 1149-1169. doi: 10.1177/0093854811421448

Rheingold, H. (2000). *The Virtual Community: Homesteading on the Electronic Frontier.* Revised Edition. Cambridge, MA: MIT Press. (Original work published 1993).

Richards, J. A. (1936). *The Philosophy of Rhetoric.* Oxford, UK: Oxford University Press.

Riva, G. & Galimberti, C. (1998). The psychology of cyberspace: A socio-cognitive framework to computer-mediated communication. *New Ideas in Psychology, 15*(2), 141-158. doi: 10.1016/S0732-118X(97)00015-9

Roberts, L. (2008). Jurisdictional and definitional concerns with computer-mediated interpersonal crimes: An analysis on cyber-stalking. *International Journal of Cyber Criminology, 2*(1), 271-285. Retrieved from http://www.cyberrimejournal.com/

Roberts-Roach, R. (nd). The impact of cyberstalking on U.S. media law. *University of Houston, Clear-Lake.* Retrieved from http://www.tamraroberds.com/

Rosenberg, J. & Egbert, N. (2011). Online impression management: Personality traits and concerns for secondary goals as predictors of self-presentation tactics on Facebook. *Journal of Computer-Mediated Communication, 17*, 1-18. doi: 10.1111/j.1083-6101.2011.01.01560.x

Rotter, J. B. (1967). A new scale for the measurement of interpersonal trust. *Journal of Personality, 35*(4), 651-665. Retrieved from http://www.blackwellpublishing.com/journal.asp?ref=0022-3506

Scott, A., Semmens, L. & Willoughby, L. (2010). Women and the Internet: The natural history of a research project. *Communication & Society, 2*(4), 541-565. doi: 10.1080/136911899359547

Second Life. (2012). FAQ. *Second Life.* Retrieved from http://community.secondlife.com/t5/English-Knowledge-Base/Search-FAQ/ta-p/846121

Smart, J., Paffendorf, J., & Cascio, J. (2007). The metaverse roadmap: Pathways to the 3D web – A cross-industry public foresight project. Retrieved from: http://www.metaverseroadmap.org

Smith, J. H. (2010). Trusting the avatar. *Games and Culture, 5*(3), 298-313. doi: 10.1177/1555412009359764

Smith, W. P. & Kidder, D. L. (2010). You've been tagged! (Then again, maybe not): Employers and Facebook. *Business Horizons, 53I*, 491-499. doi: 10.1016/j.bushor.2010.04.004

Smyth, S. (2010). *Cybercrime in Canadian Criminal Law*. Toronto, Ont.: Thomson Reuters.

Stalking. (2000). Trends & Issues in crime and criminal justice. *Criminology Research Council,* ISBN 0817-8542. Retrieved from http://www.criminologyresearchcouncil.gov.au/

Star Wars Galaxies. (2012). Homepage. *Star Wars Galaxies*. Retrieved from *Star Wars Galaxies,* private server at http://www.swgalaxies.net/.)

Stephenson, N. (1992). *Snow Crash. New* York, NY: Bantam.

Subroutine Subprogram/subroutine. (2004). In K. Barber (Ed.), *Canadian Oxford dictionary* (2nd ed., p. 1551). Don Mills, Ont.: Oxford University Press.

Suler, J. R. (2004). The online disinhibition effect. In *The psychology of cyberspace.* Retrieved from http://users.rider.edu/~suler/psycyber/disinhibit.html

Suler, J. R. & Phillips, W. L. (1998). The bad boys of cyberspace: Deviant behavior in a multimedia chat community. *CyberPsychology & Behavior, 1*(3), 275-294. Retrieved from http://www.liebertpub.com/cyber

Taddeo, M. (2009). Defining trust and e-trust: Old theories and new problems. *International Journal of Technology and Human Interaction, 5*(2), 23-35. Retrieved from http://taddeo.philosophyofinformation.net/publications/rwv_etrust.pdf

Taddeo, M. & Floridi, L. (2011). The case for e-trust. *Ethics in Information Technology, 13*, 1-3. doi: 10.1007/s10676-010-9163-1

Tidwell, L. C. & Walther, J. B. (2002). Computer-mediated communication effects on disclosure, impressions, and interpersonal evaluations: Getting to know one another a bit at a time. *Human Communication Research, 28*(3), 317-348. doi: 10.1111/j.1468-2958.2002.tb00811.x

Toading. (2007). In *Urban Dictionary Online.* Retrieved from http://www.urbandictionary .com/

Traud, A. L., Mucha, P. J., & Porter, M. A. (2012). Social structure of Facebook networks. *Physica A, 391*, 4165-4180. doi: 10.1016/j.physa.2011.12.021

Trust. (2004). In K. Barber (Ed.), *Canadian Oxford dictionary* (2nd ed., p. 1671). Don Mills, Ont.: Oxford University Press.

Tseng, Y-S. (2011). Governing virtual worlds: Interration 2.0. *Washington Journal of Law & Policy, 35*, 547-570. Retrieved from http://www.law.wustl.edu/journal/

Turkle, S. (1994). Constructions and reconstructions of self in virtual reality: Playing in the MUDs. *Mind, Culture, and Activity, 1*(3), 158-167. Retrieved from http://lchc.ucsd.edu/mca/

Turkle, S. (1995). *Life on the Screen.* New York, NY: Simon & Schuster Paperbacks.

Turkle, S. (1999). Cyberspace and Identity. *Contemporary Sociology, 28*(6), 643-648. Retrieved from http://csx.sagepub.com/

Turkle, S. (2005). The Second Self: Computers and the Human Spirit. Cambridge, MA: MIT Press.

Twitter. (2012). About. *Twitter.* Retrieved from https://twitter.com/about

United States Department of Justice. (1999). 1999 report on cyberstalking: A new challenge for law enforcement and industry. *A report from the Attorney General to the Vice President*, (*August 1999*). Retrieved from http://www.cybercrime.gov/cyberstalking.htm

United States Department of Justice. (2009). Stalking victimization in the United States. *Bureau of Justice Statistics Special Report*, (January 2009, NCJ 224527). Retrieved from http://www.ncvc.org

Valenti, J. (2007, April 6). Women: How the web because a sexists' paradise: Everyone receives abuse online but the sheer hatred thrown at women bloggers has left some in fear for their lives. *Guardian,* final edition. Retrieved from http://www.guardian.co.uk/

Vallor, S. (2011). Flourishing on Facebook: Virtual friendship & new social media. *Ethics in Information Technology, Springer Science+Business Media B.V. 2011*. doi: 10.1007/s10676-010-9262-2

Verdun-Jones, S. N. (2007). *Criminal Law in Canada: Cases, questions, and the Code.* Toronto, Ont: Thomson Canada Limited.

Wall, D. S. & Williams, M. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology & Criminal Justice.* doi: 10.1177/1748895807082064

Walther, J. B. (2007). Selective self-presentation in computer-mediated communication: Hyperpersonal dimensions of technology, language, and cognition. *Computers in Human Behavior, 23*(5), 2538-2557. doi: 10.1016/j.chb.2006.05.002

Walther, J. B., Van Der Heide, B., Kim, S-Y., Westerman, D., & Tong, S. T. (2008). The role of friends' appearance and behavior on evaluations of individuals on Facebook: Are we known by the company we keep? *Human Communication Research 34*(1), 28-49. doi: 10.1111/j.1468-2958.2007.00312.x

Wang, S. S., Moon, S., Kwon, K. H., Evans, C. A., & Stefanone, M. A. (2010). Face off: Implications of visual cues on initiating friendship on Facebook. *Computers in Human Behavior, 26,* 226-234. doi: 10.1016/j.chb.2009.10.001

Weinstock, D. (1999). Building trust in divided societies. *The Journal of Political Philosophy, 7*(3), 287-307. doi: 10.1111/1467-9760.00078

Westrup, D., Fremouw, W. J., Thompson, R. N., & Lewis, S. F. (1999). The psychological impact of stalking on female undergraduates. *Journal of Forensic Science, 44*(3), 554-557. Retrieved from http://library-resources.cqu.edu.au/JFS/PDF/vol_44/iss_3/JFSCH13.pdf

White, D. (2002). In *R. v. Basha*, 2002. N.L. Provincial Court, 2002, Carswell Nfld 322).

Williams, D., Ducheneaut, N., Xiong, L., Zhang, Y., Yee, N., & Nichell, E. (2006). From tree house to barracks: The social life of guilds in World of Warcraft. *Games and Culture, 1*(4), 338-361. doi: 10.1177/155541299692616

Wired. (1999). Cyberstalking law invoked. *Wired,* January 25, 1999. Retrieved from http://www.wired.com/politics/law/news/1999/01/17504

Wolfendale, J. (2008). My avatar, my self: Virtual harm and attachment. *Ethics and Information Technology.* doi: 10.1007/s10676-006-9125-z

World of Warcraft (WoW). (2012). Battle.net WOW GameGuide. *Blizzard Entertainment Online.* Retrieved from: http://us.battle.net/wow/en/game/guide/

Yahoo! Answers. (2012). Yahoo! Retrieved from http://answers.yahoo.com/question /index?qid=20100311142711AAbFM7v

Yee, N. (2006). The demographics, motivations, and derived experiences of users of massively-multiuser online graphical environments. *PRESENCE: Tele-operators and Virtual Environments, 15*, 309-329. Retrieved from http://www.mitpressjournals.org/loi/pres

Yee, N. (2010). Changing the rules: Social architectures in virtual worlds. In W.S. Bainbridge, (Ed.), *Online worlds: Convergence of the real and the virtual,* (pp. 213-224). London, UK : Springer-Verlag.

Yee, N. & Bailenson, J. (2007). The Proteus effect: The effect of transformed self-representation on behavior. *Human Communication Research 33,* 271-290. doi: 10.1111/j.1468-1928.2007.00299.x

Yee, N., Bailenson, J. M., Urbanek, M., Chang, F., & Merget, D. (2007). The unbearable likeness of being digital: The persistence of nonverbal social norms in online virtual environments. *CyberPsychology & Behavior, 10*(1), 115-121. doi: 10.1089/cpb.2006.9984

YouTube. (2012). YouTube partner program. Retrieved from http://www.youtube.com/yt/creators/partner.html

Zakon, R. H. (2010). Hobbes' Internet Timeline 10.1: The Definitive ARPAnet & Internet History. Retrieved from Zakon Group, www.zakon.org/robert/internet/timeline

Zekos, G. I. (2005). State cyberspace jurisdiction and personal cyberspace jurisdiction. *International Journal of Law and Information Technology, 15*(1), 1 – 37. doi: 10.1093/ijlit/eai029

Zimbardo, P. G. (2007). Revisiting the Stanford prison experiment: A lesson in the power of situation*, Chronicle of Higher Education, 53*(30), B6-B7. Retrieved from http://chronicle.com/

Appendices

Appendix A - Assault: Canadian Criminal Code

s. 265 (1) **Assault** – A person commits an assault when

a) without the consent of another person, he applies force intentionally to that other person, directly or indirectly;

b) he attempts or threatens, by an act or a gesture, to apply force to another person, if he has, or causes that other person to believe on reasonable grounds that he has, present ability to effect his purpose; or

c) while openly wearing or carrying a weapon or an imitation thereof, he accosts or impedes another person or begs.

(2) **Application** – this section applies to all forms of assault, including sexual assault, sexual assault with a weapon, threats to a third party or causing bodily harm and aggravated sexual assault.

(3) **Consent** – For the purposes of this section, no consent is obtained where the complainant submits or does not resist by reason of

(a) the application of force to the complainant or to a person other than the complainant;

(b) threats or fear of the application of force to the complainant or to a person other than the complainant;

(c) fraud; or

(d) the exercise of authority.

(4) **Accused's belief as to consent** – Where an accused alleged that he believed that the complainant consented to the conduct that is the subject-matter of the charge, a judge, if satisfied that there is sufficient evidence and that, if believed by the jury, the evidence would constitute a defence, shall instruct the jury, when reviewing all the evidence relating to the determination of the honesty of the accused's belief, to consider the presence or absence of reasonable grounds for that belief.

s. 273. (1) **Aggravated sexual assault** – Every one commits an aggravated sexual assault who, in committing a sexual assault, wounds, maims, disfigures or endangers the life of the complainant.

s. 273.1 (1) **Meaning of "consent"** – Subject to subsection (2) and subsection 265(3), "consent" means, for the purposes of sections 271, 272, and 273, the voluntary agreement of the complainant to engage in the sexual activity in question.

(2) **Where no consent obtained** – No consent is obtained, for the purposes of sections 271, 272, and 273, where

(a) the agreement is expressed by the words or conduct of a person other than the complainant;

(b) the complainant is incapable of consenting to the activity;

(c) the accused induces the complainant to engage in the activity by abusing a position of trust, power or authority;

(d) the complainant expresses, by words or conduct, a lack of agreement to engage in the activity; or

(e) the complainant, having consented to engage in sexual activity, expresses by words or conduct, a lack of agreement to continue to engage in the activity

(3) Subsection (2) not limiting – Nothing in subsection (2) shall be construed as limiting the circumstances in which no consent is obtained.

s. 273.2 **Where belief in consent not a defence** – It is not a defence to a charge under section 271, 272 or 273 that the accused believed that the complainant consented to the activity that forms the subject-matter of the charge, where

(a) the accused's belief arose from the accused's

(i) self-induced intoxication, or

(ii) recklessness or willful blindness; or

(b) the accused did not take reasonable steps, in the circumstances known to the accused at the time, to ascertain that the complainant was consenting

Appendix B - Harassment: Canadian Criminal Code

s. 264. (1) **Criminal Harassment** – No person shall, without lawful authority and knowing that another person is harassed or recklessly as to whether the other person is harassed, engage in conduct referred to in subsection (2) that causes that other person reasonably, in all the circumstances, to fear for their safety or the safety of anyone known to them.

(2) Prohibited conduct – The conduct mentioned in subsection (1) consists of

(a) repeatedly following from place to place the other person or anyone known to them;

(b) repeatedly communicating with, either direct or indirectly, the other person or anyone known to them;

(c) besetting or watching the dwelling-house, or place where the other person, or anyone known to them, resides, works, carries on business or happens to be; or

(d) engaging in threatening conduct directed at the other person or any member of their family.

(3) Punishment – Every person who contravenes this section is guilty of

(a) an indictable offence and is liable to imprisonment for a term not exceeding ten years; or

(b) an offence punishable on summary conviction

s. 264.1(1) **Uttering threats** – Every one commits an offence who, in any manner, knowingly utters, conveys or causes any person to receive a threat

(a) to cause death or bodily harm to any person;

(b) to burn, destroy or damage real or personal property; or

(c) to kill, poison or injure an animal or bird that is the property of any person

Any person found guilty of uttering threats is liable to imprisonment of a term to not exceed five years.

Appendix C – U.S. Code 18 Section 2261A

Whoever--

(1) travels in interstate or foreign commerce or within the special maritime and territorial jurisdiction of the United States, or enters or leaves Indian country, with the intent to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate another person, and in the course of, or as a result of, such travel places that person in reasonable fear of the death of, or serious bodily injury to, or causes substantial emotional distress to that person, a member of the immediate family (as defined in section 115) of that person, or the spouse or intimate partner of that person; or

(2) with the intent--

(A) to kill, injure, harass, or place under surveillance with intent to kill, injure, harass, or intimidate, or cause substantial emotional distress to a person in another State or tribal jurisdiction or within the special maritime and territorial jurisdiction of the United States; or

(B) to place a person in another State or tribal jurisdiction, or within the special maritime and territorial jurisdiction of the United States, in reasonable fear of the death of, or serious bodily injury to--

(i) that person;

(ii) a member of the immediate family (as defined in section 115 [1] of that person; or

(iii) a spouse or intimate partner of that person;

uses the mail, any interactive computer service, or any facility of interstate or foreign commerce to engage in a course of conduct that causes substantial emotional distress to that person or places that person in reasonable fear of the death of, or serious bodily injury to, any of the persons described in clauses (i) through (iii) of subparagraph (B); [2] shall be punished as provided in section 2261 (b) of this title.

Section 2261 (B):

(b) **Penalties** - A person who violates this section or section 2261A shall be fined under this title, imprisoned--

(1) for life or any term of years, if death of the victim results;

(2) for not more than 20 years if permanent disfigurement or life threatening bodily injury to the victim results;

(3) for not more than 10 years, if serious bodily injury to the victim results or if the offender uses a dangerous weapon during the offense;

(4) as provided for the applicable conduct under chapter 109A if the offense would constitute an offense under chapter 109A (without regard to whether the offense was committed in the special maritime and territorial jurisdiction of the United States or in a Federal prison); and

(5) for not more than 5 years, in any other case,or both fined and imprisoned.

(6) Whoever commits the crime of stalking in violation of a temporary or permanent civil or criminal injunction, restraining order, no-contact order, or other order described in section 2266 of title 18, United States Code, shall be punished by imprisonment for not less than 1 year.

UNITED STATES FEDERAL LAWS

United States Federal Law H.R. 3402: (1) Under the Federal Crime

(a) Cyber harassment, Cyber stalking, etc. in violation of the Women's Violence Act, Department of Justice Reauthorization Act of 2005, H.R. 3402, titled "Preventing Cyber stalking" and numbered as § 113, §113(a)(3) provides that Section 223(a)(1)(C) applies to "any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet; Cyber-stalking and Cyber-harassment laws in violation of the Communications Act, 47 U.S.C. § 223(a)(1)(C) and § 223(h)(1)(B).

(b) H.R. 3402 INCLUDES CYBER: Slander, Libel and Harassment. FIRST: Under Sec. 113. FEDERAL "Preventing Cyberstalking": To strengthen stalking prosecution tools, this section amends the Communications Act of 1934 (47 U.S.C 223)(h)(1) to expand the definition of a telecommunications device to include any device or software that uses the Internet and possible Internet technologies such as voice over internet services. This amendment will allow

federal prosecutors more discretion in charging stalking cases that occur entirely over the Internet

SECOND: The Communications FEDERAL Act, at 47 U.S.C Section 223(a)(1)(C) has prohibited the making of telephone calls of the utilization of telecommunication devices "without disclosing (one's) IDENTITY to annoy, abuse, threaten, or harass any person at the called number or who receives the communications." The FEDERAL Communication Act provides for fines and imprisonment of up to (2) two years for violations.

Appendix D – Robbery: Canadian Criminal Code

s. 343. **Robbery** – every one commits robbery who

(a) steals, and for the purpose of extorting whatever is stolen or to prevent or overcome resistance to the stealing, uses violence or threats of violence to a person or property;

(b) steals from any person and, at the time he steals or immediately before or immediately thereafter, wounds, beats, strikes or uses any personal violence to that person;

(c) assaults any person with intent to steal from him; or

(d) steals from any person while armed with an offensive weapon or imitation thereof.

Appendix E – Communications Decency Act

Communications Decency Act, 47 U.S.C. § 230 (c)

1. Treatment of publisher or speaker. No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.
2. Civil liability. No provider or user of an interactive computer service shall be held liable on account of – (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not, such material is constitutionally protected; or (B) any action to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Appendix F – Ethics Exemption

Statement of Ethics Exemption
Data in the Public Domain
30 November 2011
Re: [2011s0606] Violent Victimization in Cyberspace: An Analysis of Place, Conduct, Perception, and Law

Hilary Kim Morden
School of Criminology
Simon Fraser University

cc: Dr. Sara Smyth

In accordance with your correspondence of 29 November 2011 in which Dr. Smyth confirms that your project complies with the provisions of R20.01 as shown below please take this correspondence as exemption from the requirements of Ethics Review.

Regards,
Hal Weinberg, Ph.D.
Director, Office of Research Ethics
Simon Fraser University

> 1.4 Research in the public domain about a living individual, based exclusively on publicly available information, documents, records, works, performances, actuarial materials, or third party interviews, is not required to undergo research ethics review. However, such research requires ethics review if the individual is approached directly for interviews or for access to private papers. The 'public domain' includes all information that is available under FOI (Freedom of Information) legislation in British Columbia and Canada, whether or not the information has been exposed to the public.
>
> 1.7 Research on public policy issues, public institutions, and other matters that in a free and democratic society can properly be considered as part of the public domain is not required to undergo ethics review, even when interviews with individuals occupying positions connected to such matters are involved. Public policy is defined as follows:
>
> a. Research protocols that require contact with human participants as part of the study and whose regular occupational duties involve communicating with the public on behalf of their organizations (such as public relations officers, official spokespersons, diplomatic officials, freedom of information officers, archivists, etc., or the Chief Executive of an organization) do not require ethics review, to the degree that answering questions posed by the public is within the ordinary duties

of the participant and are within the acceptable limits of disclosure defined by the participants' employers;

b. Research protocols in which inquiries are referred to other members of an organization by a public-relations officer, official spokesperson, etc., of the organization, do not require ethics review, to the degree that their inquiries are in keeping with the initial protocol and the substance of the interviews are attributable.

Index of Cases

R. v. Krushel [2000], 142 C.C.C. (3d) 1 (Ont. C.A) leave to appeal to S.C.C. [2002] S.C.C.A. No. 293 (QL)).

R v. Labrentz, 2010, Alberta Provincial court, 2010 ABPC 11, 27, Alta. L.R. (5th) 319; 322.

R v. Leasak, 2007 ABCA 38 (Alta. C.A.).

R v. Moss, 2011, ONSC 5143m 98 W.C.B. (2d) 71.

R. v. Wenc, 2009 ABCA 328 (Alta. C.A.).

R. v. Sillipp [1997], 120 C.C.C. (3d) 384 (Alta.C.A.), leave to appeal to S.C.C. [1998] S.C.C.A. No. 3 (QL).

R v. Vandoodwaard, 2009, Ontario Supreme Court of Justice, 2009 Carswell Ont. 7468).

Register.com v. Verio, Inc., 126 F.Supp.2d 238, 249-50 (S.D.N.Y.2000).

Remsburg v. Docusearch, Inc, US District Court for the District of New Hampshire, 2002, Civil No. 00-211-B DNH 90; 2002 U.S. Dist. Lexis 79522005).

Rowan v. U.S. Post Office Dep't. 397 U.S. 728 (1970).

State v. Dellapenta, (Los Angeles Superior Court, 1999).