Social and Ethical Considerations in Virtual Worlds

Robert W. Kerbs
Computer Science Department
California State Polytechnic University, Pomona, USA
rwkerbs@csupomona.edu

Abstract

While networking technology facilitates the use of online services such as real-time instant messaging and anywhere-anytime multiplayer gaming, societal and ethical issues can influence the desirability of providing these services unmonitored to minors (i.e. users whose parents are legally responsible for them). In many countries and provinces, access to alcohol, tobacco and pornographic products is regulated by organizations that have prescribed guidelines restricting access to these goods. Such regulations aim to protect adolescents from making less objective decisions than those made by adults. Consequently, age restrictions usually account for the type of measure forbidding the sale of such products. The unmonitored distribution of electronic materials through the Internet has become a 21st century issue — since age is not easily verifiable, enforcing age restrictions on users is becoming increasingly difficult, if not impossible to monitor. The subsequent ramifications resulting from a lack of enforcement are numerous to all users of the Internet. This paper analyzes the current state-of-affairs of online virtual worlds in terms of what many people deem acceptable and unacceptable forms of behavior. An emphasis on these important issues will hopefully enlighten the public as well as providers of various Internet-related services.

1. Introduction

The general public began becoming aware of the value of being *connected* to the Internet with the introduction of the World-Wide Web (WWW) in 1994 [1]. In these ten short years the Internet's expanse has grown to include not only high-speed delivery of information to industry and academia but also to the home. In terms of numbers of users it now possesses more 380 million people worldwide (with another 170,000 people added every day) [2] — this is in addition to the one billion users who subscribe to mobile communication services [3].

The Internet can provide a myriad of services. It is frequently utilized for business transactions, online information exchange, shopping, learning, voting, teleworking, and of course online gaming. Under this backdrop lies the potential for better communication among people, better efficiencies of scale in commerce and enriched personal lives. However, along with these possibilities comes changes in terms of social and ethical behaviors. This paper's purpose is to introduce some of the issues relating to acceptable and unacceptable online behaviors.

This paper is organized as follows: in the next section the online environments that people participate in is described in terms of a virtual world; the next section covers some of the popular activities that are taking place in virtual worlds; this is followed by some suggestions for preventative measures that can be taken today to minimize a user's exposure to undesirable behavior; the last section provides analyses and conclusions.

1.1. Virtual Worlds

The definition of what a virtual world has changed over the years. In the early 1970's a game called Colossal Cave (by William Crowther) was introduced. While the graphics would be considered to be primitive when compared with today's standards, many users would utilize their strong imaginative abilities and believe that they had entered an actual virtual world consisting of different mappings of the caves of Kentucky, USA. The physical reality of entering and moving around a cave was supplanted with iconic representations of ideas and concepts facilitating a like experience. While this represents a novel example of a virtual world the definition has expanded significantly since that time.

When considered in broader terms, virtual worlds are a newer phenomenon encompassing many of the areas mentioned in the introduction. Younger generations have grasped these new environs without hesitation while many adults do not understand and/or fully comprehend what the WWW is — or the Internet. Consequently, ethics and social considerations in virtual environments is an area that most people would agree is something that should be seriously looked at.

Important issues requiring consideration include what happens to human interaction when most communication is through the computer? Since users are able to access virtual worlds do they feel less likely to suffer penalties otherwise realized in the real-world? Which and whose laws should be applied to online communication due to the the large geographic nature of the Internet? Rather than try to answer these core questions directly, background on the type of activities that are taking place today will be described. This will hopefully better outline the scope of today's virtual worlds.

2. Activities in Virtual Worlds

While most activities carried out over the Internet are innocuous, others could be considered questionable – not satisfying accepted social and ethical norms. These activities are characterized by user-initiated actions frequently detached from the fear of consequence that might be realized in the physical world. Illegal file-sharing, the possibility of sending spam to millions, and the accessibility of explicit adult-oriented materials are examples of potentially destructive behaviors that can adversely affect millions of users, businesses and organizations. Below are a number of online activities that millions of users partake in regularly.

2.1. Gaming

Video games have been around for over 30 years. The industry has provided technical advancements in many areas, including: use of both the CRT and LCD as cost-effective output devices, use of 2D/3D graphics for both draft and photo-realistic representation of images and the development of a variety of input devices. Advancements in game platform manufacturing brought about economies-of-scale for the rest of the consumer computing industry so that by the time the personal computer was introduced prices for RAM and ROM were at a level that the consumer could afford.

The introduction of the arcade video game into the mainstream brought with it interesting developments[1]. For one, it was quickly determined that users will not tolerate reading instruction manuals. Second, if a user cannot begin to use software in approximately 15 seconds there is a good chance the user will not use the software again. Finally, if instructions are absolutely necessary they must be presented clearly and succinctly [4].

We are at a similar point in time today with the introduction of online games. The difference this time is that the games utilize a distributed computing model. These models present many challenges themselves that researchers are trying to solve such as guaranteed bandwidth, quality-of-service issues, and secure playing environments [5].

2.2. Addicts, Dealers and Users

The computer industry is the only industry this author can think of that refers to their customers as users – similar to illicit drug dealers who sell their wares to their own users. This brings up the question of whether society is becoming too dependent on the computer? Surely the utilization of the computer to aid with mundane tasks has increased productivity in the workplace, but the social ramifications are not clear.

Some psychologists regard certain behavior patterns as addictive in nature. In scenarios relevant to this paper the user is interested in role-playing in the virtual world. Through instant communication the user is provided with immediate feedback reinforcing the behavior. In most cases the behavior being reinforced is harmless while in other cases the user possesses the ability, and motivation, to manipulate the situation to his or her advantage — feedback which encourages destructive behavior. A vivid example of self-destructive addictive behavior is the young computer game enthusiast who, after playing Diablo II for five hours at a cyber-café game terminal, was found slumped over, dead [6]. While this may be an extreme case, it does personify the extreme with which someone will go to satisfy an online addiction in the 21st century.

2.3. Chat Rooms

One virtual world where user interaction occurs is the online chat room. Chat rooms are environments where a user fills out an online profile that other users can see. The purpose is to attract and converse with like-minded individuals. These profiles frequently entail personal information such as name, address, phone number, as well as other information. Publication of such personal information online, and the anonymity with which other people can possibility view it, can result in various undesirable consequences including: identity theft, identity impersonation and identity assassination. Needless-to-say, security mechanisms have not been implemented to fully address these situations (see the prevention section below for some solutions).

2.4. Stalking / Cyber-Stalking

While the online delivery of data and services does aid consumers on whole, criminals can exploit these same consumers. The extent to which criminal behavior may be taken is characterized in a disturbing way with stalking. Stalking, known online as cyber-stalking, is not a new

[1] The first arcade video game was Computer Space [4].

phenomenon. What is new is that it is taking the form of an extension from the physical world to the virtual world [7]. In the traditional sense, stalking refers to the act of pursuing prey in a stealth-like way — its extension to virtual worlds can include harassment or unwelcome contact with another individual[2].

While it would seem natural that to be cyber-stalked a stalker must have access to a computer and a connection to the Internet, this is not always the case. Petherick [8] offers an example of a stalker whose rejected romantic attempts in the physical world spilled over to the virtual world. The stalker retaliated by posting a woman's personal information online including how her home security system could be bypassed. He also posted fictitious sexual fantasies of the woman on multiple forums. The victim placed messages on her door stating that the online postings were false. The stalker responded online by stating that the notes were only *tests* to see who was worthy. The harassment continued to a point where the woman had to leave her home – she also suffered emotionally from the ordeal. This is an extreme case. Thankfully, few cases have progressed from the physical world to the virtual world.

2.5. Children and the WWW

In 1998, the US Federal Trade Commission (FTC) released a report stating that 89% of web sites, whose general audience are children, collect personally identifiable information, but only 23% of the web sites instructed a child to obtain authorization before releasing the information [10]. In 1998 the US Congress enacted the Children's Online Privacy Protection Act (COPPA) requiring the FTC to set rules for websites that collect data for children under 13 years of age [11]. COPPA went into effect April 2000 and in April 2001 the FTC performed a survey of information practice compliance. It was found that although 90% of the surveyed websites now posted a privacy policy full compliance with COPPA was not obtained [12].

3. Prevention

There are a number of preventative measures that one can take to minimize the chance of becoming a victim, or your child, of a crime perpetrated either partially or totally online. The possibilities generally fall into two broad categories. The first, enforcement from large overseeing regulatory bodies is a complicated and controversial approach that might take years to implement due to its complexity and corresponding politics. The second includes steps that can be taken by users themselves that minimize exposure of personal information.

3.1. Regulation of Computer Games

The regulation of entertainment oriented material can be controversial. As Mikael Pawlo points out in [13], computer games are a form of art. Consequently, many people believe that there should be absolutely no form of regulation in their content. In essence, the belief is that the beauty is in the eye of the beholder. Additionally, this argument espouses that in a free market, the consumer will ultimately determine if the game is something of value that people are willing to pay for – similar to the success, or failure, of many arcade games.

On the other hand, some people believe that the best way to deal with minors accessing inappropriate materials is through a rating system in conjunction with distribution control mechanisms [14]. The idea is to come up with an easily understandable, but effective, rating system similar to the one utilized for movie theaters. In conjunction with the rating system would be enforced distribution mechanisms that would limit access to material that might have a negative influence on children.

Due to public concern of violence in video games, the Interactive Digital Software Association (IDSA) created the Entertainment Software Rating Board (ESRB) in 1994. ESRB's charter is to independently apply and enforce ratings, advertising guidelines, and online privacy principles adopted by the industry. This is accomplished through a two-part rating system. The first part utilizes a rating symbol that is placed on the front of a game – there are currently five possible ratings (EC for early childhood; E for everyone; T for teen; M for mature; AO for adults only). The second part is a content descriptor that is placed on the back only if ESRB believes there are elements of the game that consumers should be concerned about. The problem with this approach is that ESRB cannot enforce ratings at the retail level.

Figure 1 – four of ESRB's five possible ratings

Enforcement issues characterize ESRB's failings. While ESRB might be a good idea to help parents who physically go to video rental centers and arcades with their children, without an enforcement mechanism in place children will be able to get their hands on just about any game that they might want to take a look at. Which brings us to online games.

As of this writing there is no way that a computer game offered over the Internet can be effectively blocked

[2] It has been estimated that in the USA 8.1% of women and 2.2% of men have been stalked in their lives [9].

by an independent body. Yes, parents can use software to control access to only certain web pages on home computers. The problem is that a minor will simply utilize a friend's computer, a cyber café, or some other computer, that does have access to the web site of interest. It is arguably easier for a minor to view a specific website than it is for a minor to purchase alcohol or cigarettes. In short, distribution control by an overseeing authority seems very far off in the future – due to lack of enforcement infrastructure.

3.2. *email* and *remail*

There are a number of techniques that can be easily implemented to limit abuse of a user's email account. When creating an email account, it is recommended to select one that is gender-neutral. For communicating with people you don't know, one might consider using a *public* email account; such as a yahoo or msn email account.

If you have a web site don't include a mailto: tag in the html web pages. Programs called spambots and spiders can traverse and parse web pages with the intent of extracting email accounts. It is best to use an image of your email account if you want to post one on a web page.

Another technique is to represent your email address as a series of *character entities*. These are codes that, when rendered in a web browser, shows your correct email address, but a spambot or spider cannot easily detect what it is. For instance, the corresponding character entities for my my rwkerbs@csupomona.edu email account would be: &#114;&#119;&#107;&#101;&#114;&#98;&#115;&#64;&#99;&#115;&#117;&#112;&#111;&#109;&#111;&#110;&#97;&#46;&#101;&#100;&#117;.

Users who wish to control the anonymity of an email account can utilize an email intermediary called a remailer. Once one signs up with one of these entities emails can be sent to users and newsgroups without the senders name, or real email account, being relayed to the recipient. The remailer effectively strips away this information, assigns an unrelated email account to the message (like asp123@remailerOrg.com) and delivers the message. Users can respond to the remailer account. When the remailer receives a response it can strip the recipient's name and email account from the message and delivers it to the original requester.

One common technique utilized for handling email on certain websites is to require the user to fill out a web form. While not as good as an image, it will make the spambot or spider work harder to get your email address.

It is recommended that one analyze the headers associated with email that you might send – it might contain information of a personal nature that you would not want distributed. This data might contain name and email address, for instance. When forwarding email remove headers from the prior email. The email can be culled for all email accounts that it might contain.

Finally, there are a few other measures a user could take. Be careful not to put anything in your email signature that you would not mind having distributed to an open audience. It is recommended to not place your email address in your email signature – the idea is that the recipient will know you well enough to either reply to your email, or knows how to look it up in a form of address book. Finally, it is not recommended to use the "Mail this Document to a Friend" feature available on many web sites. There would be the possibility that you would add your friend to a possible spam list.

3.3. Online Profiles

At a very young age we are taught not to talk to strangers. While this concept is easily articulated in a simple sentence for the physical world, it becomes more complicated in virtual worlds. In general terms it is recommended that one limit the release of personal information when communicating in online forums, chat-rooms and bulletin boards. Information of concern is obviously name, address and telephone numbers and may include name and location of school for children as well as mom and dad's work details. Consider using a pseudonym online to hide you and your child's identity. Don't participate in an online virtual world if your email account is listed on the site. Remember that people online may not be who they claim to be. Little Susie who says she is 10 years old may actually be an adult with a history of child molestation. A child's online profile should be carefully reviewed by a guardian.

3.4. Usenet (Newsgroups)

Many of the solutions presented in the aforementioned sections also apply to newsgroups, however there are a few other actions one can take to protect one's privacy. Many newsgroups are moderated for content and appropriateness of posting. The moderator reviews each message before it is posted online. It is recommended, if at all possible, to participate in these types of newsgroups. The communication with other members can be more thoughtful, and safe, when compared with unmoderated newsgroups due to the moderator's ability to remove messages before they can even be posted. In order to minimize spam, only participate in newsgroups that do not list your email account – it is recommended to use a remailer for communicating with other people. Your online profile should limit your personal data.

3.5 Web Browsing (anonymously)

Unbeknownst to many people is the ability for web sites to collect your personal information and track your web browsing habits. For instance, every time you visit a website or check your email, your IP address and domain name can be determined. Some websites try to install spyware and adware programs on your computer to collect private information. These programs can utilize log files and cookies to keep track of your movements through the web. A recommended solution to this problem is to use SSL encryption software between your computer and a proxy server. Proper configuration will result in anonymous web browsing without cookies even reaching your computer. There are many service providers, many of them free, that can provide this service.

4. Analyses and Conclusion

The computer has evolved from a tool used solely for business, research and governmental purposes to an instrument characterized by social interaction in *virtual worlds*. In this context, like-minded people can converse and interact online in a way that is both enjoyable and satisfying. However, virtual worlds also bring with them pause for concern. These concerns include, but are not limited to: the loss of one's privacy, the fear of being exploited and the loss of identity. While it might be possible for these concerns to be addressed and regulated by governing bodies, the breadth of this paper's coverage has shown that effective enforcement of online behavior is, at least, a very complicated undertaking – not one that will be quickly or easily solved. Fortunately, there are a number of mechanisms people can utilize to help traverse these new worlds in a safe, secure and confident manner. This paper has proposed a number of well-known examples as potential solutions.

References

[1] Vinton Cerf, (1997). Speech given at ACM97: The Next 50 Years of Computing.

[2] Erwin Staudt, (2001, April 2), The Future of Learning - Learning for the Future: Shaping the Transition. Paper presented at the 20th ICDE World Conference on Open Learning.

[3] ETSI. (2002), Human Factors (HF): Potential Harmonized UI Elements for Mobile Terminals and Services (ETSI TR 102 125 V1.1.1 (2002-10)). Sophia Antipolis Cedex, France: European Telecommunications Standards Institute.

[4] Nolan Bushnell, (1996), Relationships Between Fun and the Computer Business, Communications of the ACM, vol. 39, no. 8, pp 31-37.

[5] Robert Kerbs, (2003), "Internet Gaming in the era of IPv6", Proceedings of the 2nd International Conference on Application and Development of Computer Games, pp. 31-36.

[6] Staff. (2003, January 13). Computer Addict Dead at Screen. The Sydney Morning Herald.

[7] Trudy Gregorie, (2000), Cyberstalking: Dangers on the Information Highway. Arlington, VA: National Center for Victims of Crime.

[8] Wayne Petherick, (2003), "Cyber-Stalking: Obsessional Pursuit and the Digital Criminal," http://www.crimelibrary.com/criminology/cyberstalking/index.html.

[9] Bureau of Justice Statistics (BJS), 1999. Sourcebook of Criminal Justice Statistics 1998. Washington, DC: U.S. Department of Justice. Citing National Institute of Justice, 1998, Stalking in America: Findings from the National Violence Against Women Survey, Washington, DC: U.S. Department of Justice.

[10] Sara Baase, A Gift of Fire: Social, Legal, and Ethical Issues for Computers and the Internet, 2nd Edition, Pearson Education, Upper Saddle River, NJ, 2003.

[11] Federal Trade Commission (FTC), "You, Your Privacy and COPPA," http://www.ftc.gov/bcp/conline/pubs/buspubs/coppakit.pdf (Current October 2003).

[12] Federal Trade Commission (FTC), "Protecting Children's Privacy Under COPPA: A Survey on Compliance," http://www.ftc.gov/os/2002/04/coppasurvey.pdf (April 2002).

[13] Mikael Pawlo, (2003, January 3), Regulating Computer Games, http://grep.law.harvard.edu/article.pl?sid=03/01/03/1942201&mode=flat.

[14] Paul Szynol, (2003, January 3), Violence, Video Games, etc, http://research.yale.edu/lawmeme/modules.php?name=News&file=article&sid=784.