SYRACUSE JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 31 2014-2015 ARTICLE 4, PAGE 98

PRIVACY EXPECTATIONS IN ONLINE VIDEO GAMES: IN LIGHT OF EDWARD SNOWDEN'S NSA DOCUMENT LEAK

Matthew Knopf

ABSTRACT

On December 9, 2013, the British Newspaper *The Guardian*, published documents from the National Security Administration provided by the whistleblower Edward Snowden. These documents revealed that surveillance agencies of the United States and United Kingdom governments were conducting intelligence operations in a search for terrorists inside of massive multiplayer online video games, such as *World of Warcraft* and *Second Life*. Online video game players live across the globe and within the United States and many of the computer servers on which video games operate are inside of the United States. The revelations of these documents lead to questions of whether there are any expectations of privacy for video game players and the communications between players within those video games. Violations of privacy could hinder player anonymity, a key component of certain types of online gaming that encourages escapism. Conversely, ending anonymity could encourage fairer and more civil discourse in the virtual gaming worlds. In the end, it is in the best interests of the gaming companies to continue to cooperate with governments in order to monitor and detect suspicious activity. It is most likely that gamers do not have an expectation of privacy in the virtual world.

INTRODUCTION

On December 9, 2013, the British Newspaper *The Guardian* published documents from the National Security Administration ("NSA documents") provided by the whistleblower Edward Snowden.[1] These documents revealed that surveillance agencies of the United States and United Kingdom governments were conducting intelligence operations in a search for terrorists inside of massive multiplayer online ("MMO") video games such as *World of Warcraft* and *Second Life*.[2] The documents contained a memo and a series of essays that detailed the ways in which video games, even those video games that do not directly connect to the Internet, could be used as recruitment and communication tools for terrorists.[3] However, these operations have brought about privacy concerns for some who worry that their government could or would listen to their conversations as they are playing these videos games.[4] It is not clear how the government collected or accessed the data or communication from these video games.[5] It is likely that government agents created their own profiles and avatars in these games to access the virtual worlds. Additionally, privacy concerns have not be assuaged by the fact that there is no indication from the documents that any of the intelligence operations led to the foiling of any terrorist plots or to the arrest of any criminal.[6] The National Security Administration ("NSA")

---

[1] *NSA files: games and virtual environments paper*, THE GUARDIAN (Dec. 9, 2013), http://www.theguardian.com/world/interactive/2013/dec/09/nsa-files-games-virtual-environments-paper-pdf; *See* James Ball, *Xbox Live among services targeted by US and UK spy agencies*, THE GUARDIAN (Dec. 9, 2013, 6:26 PM), http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life.

[2] *See* Ball, *supra* note 1.

[3] *See NSA documents on games and virtual worlds,* PROPUBLICA, http://www.propublica.org/documents/item/889134-games (last visited on Feb. 14, 2014) [hereinafter *NSA Documents*].

[4] Ball, *supra* note 1.

[5] *Id.*

[6] *Id.*

and the federal government may have free reign to spy on foreign peoples and foreign governments, but under the U.S. Constitution it does not have the legal authority to spy on American citizens without a warrant.[7]

Online video games have players who live across the globe and within the United States. Many of the computer servers on which the video games operate and communicate are inside of the United States.[8] Since the intelligence collecting process has not been revealed, it is unclear if the NSA or other federal agencies have been accessing the data and the monitoring communications of innocent Americans whose identity and nationality may have been concealed behind their virtual avatar.[9] The debate over the expectation of privacy concerning different types of Internet communication is growing, especially concerning social media.[10] Violations of privacy could hinder player anonymity, which is a key component of certain types of online gaming that encourages escapism. On the other hand, ending anonymity could encourage fairer and more civil discourse in the virtual gaming worlds.[11] The revelations of these documents has led to the question of whether there are any expectations of privacy for video game players and the communications between players which occur within those video games.

---

[7] *See* U.S. CONST. amend. IV.

[8] For Example, *World of Warcraft*, which is owned and operated by Blizzard Entertainment, has over seven million subscribers around the world, servers that run the game processes around the world, and their headquarters are here in the United States. *See Privacy Policy*, BLIZZARD ENTM'T (last updated July 28, 2014), http://us.blizzard.com/en-us/company/about/privacy.html [hereinafter Blizzard's Privacy Policy]; *See also* Luke Karmali, *World of Warcraft down to 7.7 Million Subscribers*, IGN (July 26, 2013), http://www.ign.com/articles/2013/07/26/world-of-warcraft-down-to-77-million-subscribers.

[9] Ball, *supra* note 1.

[10] Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, 17 RICH. J.L. & TECH. 12, 12-13 (2011).

[11] Jaikumar Vijayan, *Gaming giant Blizzard ends online anonymity, stirs up storm*, COMPUTERWORLD (July 9, 2010), http://www.computerworld.com/s/article/9179042/Gaming_giant_Blizzard_ends_online_anonymity_stirs_up_storm.

This note will review many different aspects of online video games and video game communications in the world after the leaks shown by Edward Snowden. This note will first examine whether or not there is a difference between video game consoles and computers that could affect the application of the law. Next, the note will discuss the many interests the government may have for monitoring the activity of online video game players, followed by a survey of privacy laws in the United States and how they could affect online video games. The note will then discuss anonymity in video games and if that element of anonymity is enough to warrant an expectation of privacy. Finally the note will discuss how the big businesses that make these online games handle private information and how that may affect a gamer's expectation of privacy.

I. COMPUTERS VERSUS VIDEO GAME CONSOLES

The definition of a computer is becoming blurred, but this does not have an effect on the legal expectations of the user. For legal purposes, the most important factor is ability of both computer and video game consoles to connect to the Internet. This connection to the Internet is important because this places the gaming system in connection with interstate commerce.

For those not familiar with the different between video game consoles and computers, there is very little difference between the hard ware and software used for video games played on either a computer or video game console. For computers, computer games are downloaded to the player's computer either from a disk or an Internet service platform, such as Steam.[12] Once the game is installed onto the computer and the computer is connected to the Internet, the player can

[12] *Welcome to Steam*, STEAM, http://store.steampowered.com/about/ (last visited Sept. 16, 2014); Bradley Mitchell, *Online Games: Using computer networks to play games online*, ABOUT.COM, http://compnetworking.about.com/od/homenetworkuses/a/network-online-games.htm (last visited Sept. 16, 2014).

then access game.[13] The Internet connection of course is provided by the user's router or Internet Service Provider, such as Comcast, Optimum, or Verizon. Once inside a game, the player is usually prompted to create an avatar or profile to access the online components of the game.[14] That avatar is how the player will be represented to the rest of the online game's community.[15]

Console gaming requires that the player first own such a console, such as the PlayStation 4 or Xbox One. Each game console manufacturer maintains its own separate Internet service for online games. This Internet service then connects to the player's local router, just like a computer. Xbox consoles connect to Xbox Live and PlayStation consoles connect to The PlayStation Network. In order to access the consoles features, the player must create a profile for the particular network that the console is connected.[16] This profile will be the avatar and profile that appear for all games that the player plays on that network. [17] For the newer consoles including Xbox One and PlayStation 4, the player must also pay a subscription fee in order to access the network. Once the player has set up their profile they may either install a video game through a disk or download it from the console's network. [18] Once installed the player can access the game's online features, which in turn connect to the Internet through the console's network. [19] Newer consoles, such as the PlayStation 4 and the Xbox One, also allow for the download of

---

[13] Mitchell, *supra* note 12.

[14] *World of Warcraft Beginner's Guide: Chapter 1 Getting Started*, BATTLE.NET, http://us.battle.net/wow/en/game/guide/getting-started (last visited Sept. 16, 2014) [hereinafter *World of Warcraft Beginner's Guide: Chapter 1*].

[15] *Id.*

[16] Kathryn Montminy, *How to Create a PlayStation Network Account,* ABOUT.COM, http://psp.about.com/od/pspforkids/ss/How-To-Create-A-Playstation-Network-Account.htm (last visited Sept. 16, 2014).

[17] *Id*.

[18] *Id.*

[19] *Id.*

applications that allow a user to connect to websites and other Internet based services, such as Amazon Prime and Netflix through their network.[20] These capabilities of newer consoles further blur the line between console and computer.

Additional complications arise when discussing mobile gaming devices and mobile phones. Mobile phones have the ability to access the Internet through both wireless communications provided by an Internet provider and through "3G" or "4GLTE" networks maintained by cellphone carriers such as AT&T and Verizon.[21] Additionally, hand held devices specifically made for playing video games, such as the PlayStation Vita, can connect to the console manufactures network. Specifically, the PlayStation Vita can also connect to Sony's PlayStation Network. [22] The mobile or handheld device can either connect to the Internet through "3G" provided by a cell phone company such as AT&T or by connecting an USB cable or Bluetooth connection to a correlated video game console. Thus, in the case of the PlayStation Vita it can connect to the Internet through the PlayStation 3 or PlayStation 4.[23]

The difference between console gaming and computer gaming does not lie in the hardware of the console or the computer and does not lie with their ability to connect to the Internet. The difference may be in the software that the console uses and the essential purpose of the system. This is important as this note may use the term (or similar terms) "online video games" to discuss both games played on a computer and games played on a video game console. The essential purpose of the system and the online video games themselves may lead gamers to

[20] *PlayStation 4 Overview*, http://us.playstation.com/ps4/index.htm (last visited Feb. 14, 2014).

[21] Brian Jung, *How Does the Internet Work on Cell Phones?*, CHRON.COM, http://smallbusiness.chron.com/Internet-work-cell-phones-55688.html (last visited Feb. 16, 2014).

[22] Chelsea Stark, *PlayStation Vita: Everything you Need to Know,* MASHABLE (Feb. 22, 2012, 8:47 PM), http://mashable.com/2012/02/22/playstation-vita-faq/.

[23] *Id.*

have an expectation of privacy as discussed later in the note. Differing from computers, video game consoles and computers are not simply connecting to the Internet through a browser, thereby making many features of video games a concern of government.

II. WHY WOULD A TERRORIST OR CRIMINAL BE INTERESTED IN VIDEO GAMES?

Online video games create a number of issues for the government. However, the question that should be held in mind while reviewing those concerns is, if an expectation of privacy is found to exist, whether these issues warrant a breach of privacy by the government.

One of the major reasons that criminals or terrorists would be interested in online gaming is the massive amount of money being spent on virtual currencies and in game purchases.[24] Most online games use some sort of virtual economy or virtual currency to allow players to make purchases, with real money, while playing the game.[25] For example *Eve Online* has a massive player base with over 400,000 players participating in the game's virtual market.[26] *Eve Online* is a game where players build spaceships and traverse a virtual galaxy.[27] In order to build those virtual ships players can buy and sell raw materials which, in turn creates the game's own fluctuating commodities markets. Players of *Eve Online* can even form trade coalitions and banks.[28] Virtual economies have gotten so complicated that some video game companies have hired economic analysts to help them create and regulate the economies.[29] Since purchasing in

[24] Erik Kain, *Massive 'EVE Online' Battle Could Cost $500,000 In Real Money*, FORBES (Jan. 29, 2014, 4:55 PM), http://www.forbes.com/sites/erikkain/2014/01/29/massive-eve-online-battle-could-cost-500000-in-real-money/.

[25] Brad Plumer, *The Economics of Video Games*, WASH. POST (Sept. 28, 2012), http://www.washingtonpost.com/blogs/wonkblog/wp/2012/09/28/the-economics-of-video-games/.

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

the virtual worlds requires real dollars, these virtual currencies and economies can have real world consequence.[30] The NSA documents estimated that there is approximately one to two billion dollars' worth of intangible goods in the online game *Second Life*.[31] The NSA documents went on to chart the exchange rate for virtual currencies to real dollars for a number of online games.[32] With the ability to hide behind their avatars, criminals and terrorists could use these currencies to raise money or transfer money in the form of virtual currency to fund terrorist activity.

In addition to the flow of in-game cash, the leaked NSA documents specifically mention a game created by terrorist group Lebanese Hezbollah called *Special Forces 2*.[33] The NSA documents state that the game is sold for ten dollars a copy and that money goes to "fund terrorist organizations."[34] The NSA documents claim that this game contains multiplayer features that allow for online text and voice chat of up to 60 players.[35] The NSA documents claim that games like Hezbollah's *Special Forces 2* can be used for the recruitment and training of terrorists by providing weapons training and realistic battle field simulations.[36] It is ironic that this game, as the NSA documents point out, is based off another online game *America's Army*, which was produced by the United States Army for recruitment and training of United States troops and is free to download.[37] This could indicate a double standard. *America's Army* is currently on its

[30] *NSA Documents*, *supra* note 3.

[31] *Id.*

[32] *Id.*

[33] *Id.*

[34] *Id.*

[35] *NSA Documents*, *supra* note 3.

[36] *Id.*

[37] *Id.*

third iteration *America's Army 3* and has substantially similar goals of Hezbollah's *Special Forces 2*.[38] *America's Army 3* describes itself as a "stunningly realistic" experience that provides "authentic military elements including training, technology, weapons, and audio than any other military game."[39] Additionally, the in game play allows for multiplayer communication.[40] The hypocrisy is furthered by the fact that *America's Army 3* is currently free to download and play.[41] Hypocrisy aside, there may be some merit to the concerns of the government.

The biggest concern of the NSA documents is the ability of online games to provide easy communications between multiple players.[42] The NSA document gives examples of the types of communications online games offer including email, voice over internet protocol, chat, proxies and web forms. [43] The NSA documents detail how a single *World of Warcraft* player can set up a "guild" or group to coordinate and communicate verbally and non-verbally either in a group chat or player to player. [44] The NSA documents detail the government's worries that terrorist groups could use these same means of communication, almost anonymously, to communicate to each other. The NSA documents additionally consider the convergence of mediums that online games allow. [45] The NSA documents detail how soon, the MMO game *Second Life* may allow the game's players to text and voice call phone numbers almost anonymously. [46] The merger of

[38] *AA3 Home*, AMERICA'S ARMY 3, http://aa3.americasarmy.com/ (last visited Mar. 16, 2014).

[39] *America's Army 3*, STEAM, http://store.steampowered.com/app/13140/ (last visited Mar. 16, 2014).

[40] *Id.*

[41] *Id.*

[42] *NSA Documents*, *supra* note 3.

[43] *Id.*

[44] *Id.* at 33.

[45] *Id.* at 3.

[46] *Id.*

cellphones and online video games opens up the door to additional possibilities of communication. The NSA documents claim that all of these different types of communication offer terrorists essentially private meeting places that can be used for planning, collaboration, communications, and training. [47]

These concerns over communication in online video games are compounded by the fact that the NSA, with few exceptions, cannot differentiate the traffic of these online games from normal traffic on the Internet. [48] Therefore, in order to locate terror cells or criminals within the virtual world, the NSA would have to rely on human intelligence gathering practices, also known as HUMINT.[49] Absent new developments in searching capabilities by the NSA, this will be the method for the intelligence gathering for the foreseeable future. HUMINT could include government agents creating avatars and profiles in these online games. The government agents would access the game in order to recruit and mine for intelligence and data within the virtual world. [50] In fact, there were so many agents from different agencies within these gaming virtual worlds according to the NSA document that "de-confliction" groups were required to make sure the agencies intelligence operations were not interfering with each other.[51]

There are a series of questions that open up the NSA's operation to suspicion. Should the NSA, FBI, or any government entity or official play video games with the general public? Additionally, when the NSA is collecting in-game data, or intelligence on a certain player ID,

---

[47] *NSA Documents*, *supra* note 3.

[48] *Id.*

[49] *Id; News & Information*, INTelligence*: Human Intelligence*, CENTRAL INTELLIGENCE AGENCY (Apr. 30, 2013, 12:41 PM), https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/intelligence-human-intelligence.html

[50] *NSA Documents*, *supra* note 3.

[51] *Id.*; Ball, *supra* note 1.

avatar, or group, or guild of players, how does the NSA identify who the player is? What information about the player is collected? Is the NSA able to differentiate between American players and foreign players? If the NSA is able to match a player avatar to a certain console or computer through IP or MAC addresses, does that matching create a violation of privacy? Is there an expectation by the players to privacy or to maintain their avatars anonymously?

Many of the questions above cannot be answered because of the lack of specific operational details in the NSA documents and the lack of governmental transparency. Additionally, there are many other popular types of communication which may be in the government's interest to monitor. But, if the government's fears are realized then the government may have an argument for monitoring online video game communication.

A. Are the Government's Fears Legitimate?

The government's fears may be legitimate. Although the NSA documents do not claim to show any success in preventing terrorism, there are news stories that could show some support to the government's fears.

In 2010, a teenager in Victoria, British Columbia was sentenced to life in prison after confessing to rape and murder over the chat logs of *World of Warcraft*.[52] The chat logs were only one part of a mountain of evidence used to convict him.[53] The teenager said he had bragged about his crime while playing *World of Warcraft* because he thought the chat logs were less likely to be saved.[54]

---

[52] Justin Olivetti, *Teenager Killer Confesses Crime in World Of Warcraft Chat, Sentenced to Life in Prison*, ENGAGET (Nov. 5, 2011, 12:00 PM), http://massively.joystiq.com/2011/11/05/teenage-killer-confesses-crime-in-world-of-warcraft-chat-senten/.

[53] *Id.*

[54] *Id.*

Another incident occurred in 2011, when FBI agents arrested two students for allegedly fraudulent sales and purchases of virtual currency while playing *World of Warcraft*.[55] According to a government document made public by the whistleblower and hacker group LulzSec, criminal syndicates and gangs such as MS-13 used PlayStation 3 and Microsoft Xbox 360's live chat features to communicate with each other in order to recruit members and conduct criminal activity.[56] These documents were released in 2010 and detailed how the gang specifically used video game communications to communicate covertly to group members overseas in order avoid detection by police. [57]

It is, of course, arguable that these are isolated incidents. Since the NSA documents do not show any concrete evidence of successful terrorism prevention, it is difficult to balance or measure the true threat level that these types of communications possess. Thus, if there is an expectation of privacy, it may be hard to balance a possible danger (or lack thereof) against the violations of that privacy. However, if there is no expectation of privacy than the balancing of privacy versus police power may not be necessary.

III. VIDEO GAMES AND PRIVACY

There have been numerous attempts to regulate video game content, especially violence in video games. The documents leaked by Edward Snowden brought privacy concerns to the forefront of American political debate. Many of the surveillance programs began in the early

[55] Darlene Storm, *Intelligence Agencies Hunting for Terrorists in World of Warcraft,* COMPUTER WORLD (Apr. 13, 2011, 7:41 PM), http://www.computerworld.com/article/2471127/endpoint-security/intelligence-agencies-hunting-for-terrorists-in-world-of-warcraft.html.

[56] *(U//LES) LulzSec Release: New Jersey Fusion Center: MS-13 Using Game Consoles to Communicate*, PUBLIC INTELLIGENCE (June 25, 2011), https://publicintelligence.net/ules-lulzsec-release-new-jersey-fusion-center-ms-13-using-game-consoles-to-communicate/.

[57] *Id.*

2000s in response to September 11th terrorist attacks with the intention to prevent other terrorist threats. But there are no specific laws that focus on communication within video games. Thus, the focus remains on the protection of privacy in general, privacy on computers and general Internet communication.

A. Privacy Law

Griswold v. Connecticut first established a United States citizen's right to privacy, stating that the Bill of Rights has "penumbras, formed by emanations from those guarantees that help give them life and substance."[58] Stated without the weird term "penumbra," the Supreme Court found that a right to privacy must exist because the idea of a right of privacy is interwoven in the principles and ideas of the Bill of Rights.[59] *Griswold v. Connecticut* dealt with the prohibition of the use of contraceptives.[60] Although the case is far too old to deal with technological issues, it does set a precedent of expectations of privacy within one's own home.

One of the most famous examples of technology versus privacy concerns that made its way to the Supreme Court occurred in *Kyllo v. United States*.[61] The police in *Kyllo* used a thermal imaging device, without a search warrant, to determine if the amount of heat emanating from the defendants home was consistent with the high-intensity lamps typically used for indoor marijuana growth.[62] As Danielle Keats Citron analyzed in her article, the Court was invited to limit Fourth Amendment protection to activities in the home that can be regarded as "intimate"

[58] Griswold v. Conn., 381 U.S. 479, 484 (1965).

[59] *Id.*

[60] *Id.* at 480.

[61] Kyllo v. United States, 533 U.S. 27 (2001).

[62] *Id.*

but chose not to do so.[63] The Court instead chose to focus on whether or not the activity was invasive. [64]

Another Supreme Court case, *United States v. Jones,* addressed the use of GPS tracking to monitor a specific persons movements and their connection to local drug activity in the District of Columbia.[65] In *Jones,* the defendant argued that the collection of data about his movement could lead to the incidental collection of intimate details of his life and therefore a violation of his privacy.[66] Here, the court again dodged the issue of intimate privacy in one's own home.[67] The Court in *Jones* held instead, that the defendant's rights were violated not because of an expectation of privacy, but instead because law enforcement physically occupied his private property for the purpose of obtaining information on the defendant.[68] David Witte contends that in their ruling in *Jones*, the Supreme Court sought to avoid ruling that there was a reasonable expectation of privacy in an individual's location on Earth.[69] He contends that instead, the Supreme Court established a constitutional minimum. [70]

---

[63] Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. 262, 268 (2013).

[64] *Id*. at 268.

[65] United States v. Jones, 132 S. Ct. 945, 949 (2012).

[66] *Id.* at 948.

[67] Derek S. Witte, *Privacy Deleted: Is It Too Late to Protect Our Privacy Online?,* 17 J. Internet L. 1, 16 (2014) [hereinafter Witte, *Privacy Deleted*] (citing United States v. Jones, 625 F.3d 766 (D.C. Cir. 2010)).

[68] *Id.* at 16.

[69] Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV. 717, 738 (2013) [hereinafter Witte, *Bleeding Data*].

[70] *Id.*

B. Legislative Protections of Privacy

Prior to the Snowden leaks, not much had been written regarding privacy concerns and video games. Additionally, there has not yet been a Supreme Court case determining the legality of the NSA's video game or Internet surveillance programs. Therefore, it may be prudent to look for congressional action or legislation for indications on whether there are any privacy protections for video games.

In the article *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery* in the *South Carolina Law Review*, Derek Witte provides a comprehensive chart concerning various federal statutes concerning personal data shared online.[71] Witte analyzes that there may be little protection for personal data on social networking sites through federal statutes. [72] But the question remains if the same can be said about online gaming.

The two relevant statues on Witte's chart are the Wire Tap Act and the Electronic Communications Privacy Act. The Wiretap Act made it unlawful for any individual to intercept a communication to which they are not a party. [73] There is an exception for law enforcement, but they may do so only with a valid court order. [74] In 1986, the Electronic Communications Privacy Act extended the protections to include electronic communications. The act defines "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic

---

[71] *Id.* at 742-748.

[72] *Id.*

[73] Witte, *Privacy Deleted*, *supra* note 67, at 1-16.

[74] *Id.*

or photo-optical system that affects interstate or foreign commerce."[75] The Stored Communications Act added stored communications to the list of protected types of electronic communications.[76] The Electronic Communications Privacy Act has since been affected or amended by the USA Patriot Act and the Foreign Intelligence Surveillance Act.

The Foreign Intelligence Surveillance Act ("FISA") gives procedures to the government to conduct physical and electronic surveillance of "foreign intelligence information" between "foreign powers" and "agents of foreign powers."[77] The part of the statue to note here is the fact that "agents of foreign powers" includes possible United States citizens. Thus, the statue attempts to protect United States citizens by requiring that in order for the government to conduct the surveillance, the government must obtain a warrant and show probable cause.[78] Alone this may seem as sufficient protection, however it has come to light that while conducting surveillance on foreign targets, the government has "incidentally" obtained data on United States citizens.[79] These fears of over the extension or additional "incidental" collection of data is compounded when taking into account the amount of personal and private data that can be gleaned from private computers and video game consoles.

IV. IS THERE AN EXPECTATION OF PRIVACY IN THE VIRTUAL WORLD?

According to the NSA documents as discussed above, the NSA has very limited capabilities when trying to identify and pierce the Internet traffic of online games. Accordingly,

[75] 18 U.S.C. § 2510 (2002).

[76] 18 U.S.C § 2701 (2014).

[77] 50 U.S.C. § 1801 (2010).

[78] Act of Oct. 25, 1978, Pub. L. 95-511, 92 Stat. 1783.

[79] Chris Strohm, *NSA Phone Data on U.S. Locations Incidental Chief Says,* BLOOMBERG BUSINESS (Dec. 11, 2013, 4:35 PM), http://www.bloomberg.com/news/2013-12-11/nsa-phone-data-on-u-s-locations-incidental-chief-says.html.

the NSA documents revealed that strategies in collecting intelligence within online games involve HUMINT as well as the creation of profiles and avatars by government officials.[80] This tactic appears may have important legal difference from the collection of big data. Much like social media, a large portion of online games occurs in a virtual world that is open to everyone that has a profile or avatar in that game.[81] But does this mean that the government then has the right to create its own avatar and participate in the online world? Courts have not reached a conclusion as to whether the fourth amendment reaches spaces on the Internet.[82]

Since there are many different types of communication and activities in video games, it might be reasonable to expect different levels of protection within the online game. For example, in the game *Second Life*, the player can create many different types of structures and virtual places for their avatar to "live" or with which to interact.[83] These creations could present many possible scenarios that could indicate a level of expectation of privacy. It also raises the question of how the virtual home should be treated. On one hand, if another player were to try and access the virtual home, the player would have the ability to choose whether or not the other player can enter. [84] This could give a player a sense of privacy and autonomy.[85] On the other hand the online game and the virtual home is simply virtual code that passes along through the Internet and into the public commerce. Additionally, does the expectation of the player change since the company that runs the online game will always have access to the code that creates the virtual world it

[80] *NSA Documents*, *supra* note 3.

[81] *World of Warcraft Beginner's Guide: Chapter 1*, *supra* note 14.

[82] Marc Jonathan Blitz, *Stanley in Cyberspace: Why the Privacy Protection of the First Amendment Should Be More Like That of the Fourth*, 62 Hastings L.J. 357, 372 (2010) [hereinafter Blitz, *Stanley in Cyberspace*].

[83] *Create*, SECOND LIFE, http://secondlife.com/whatis/create/?lang=en-US, (last visited Feb. 16, 2014).

[84] *Id.*

[85] Blitz, *Stanley in Cyberspace*, *supra* note 82, at 375-376.

maintains? Marc Blitz argues that there may be a sense of trust and an expectation of privacy between players and the companies that create the game.[86] This trust, he argues, is similar to bank and phone records that require the government to obtain a warrant before the company divulges any information. [87] Blitz notes that the Supreme Court has been hesitant to extend protections of privacy where the information is open to the public.[88] Thus the question of an expectation of privacy may still be up for debate.

If the government agent only maintains access to the public areas of the online world, then the agent most likely can avoid privacy breaches and act similar to a mole or undercover officer. As discussed, there may be little in the eyes of the law that a player should expect in terms of privacy in public spaces.[89] And while the government may be able to view the public information on a gamer's avatar or profile, it needs assistance in some form to identify the people behind the avatar. This leads to either two situations: either the government asks or subpoenas the gaming company, or the government uses data mining programs or hacks a player's account. Either situation could tread on a fundamental piece of some online video games or that is anonymity.

A. Anonymity

At first glance, video games and communication through video games looks a lot like social media, such as Facebook or Twitter, and usual Internet communication, such as Skype or any other type of video chat. But one of the most important factors of certain types of video

[86] Blitz, *Stanley in* Cyberspace, *supra* note 82, at 376.

[87] *Id.*

[88] *Id.*

[89] *Id.*

games is the ability to "virtually" become a different person, and he idea that video games are a form of escapism is not new.[90]

The ability to hide behind a user name in place of a real name is an enticing one for criminals. But, it can also allow for a video game player to be expressive and communicate in ways that the player does not feel is possible in the real world.[91] This expression can be both negative and positive. John Suler proposes that this phenomenon, known as "The Online Disinhibition Effect," is responsible for the callous behavior often seen in YouTube video comments.[92]

The Online Disinhibition Effect is made up of various components: Dissociative Anonymity, Invisibility, Dissociative Imagination, and Minimization of Authority.[93] Together these factors give an Internet user or online gamer the ability to act without, or to feel as if they are acting without, taking responsibility for their own actions.[94] The Online Disinhibition Effect applies not only to comments on YouTube, but also to online gaming. This decreases the Internet user or gamers inhibitions and gives them the freedom to act outside of their comfort zone.[95] While it allows the players certain freedoms and privacy, it can also have negative effects.

---

[90] Gordon Calleja, *Digital Games and Escapism*, ACADEMIA.EDU, http://www.academia.edu/2962309/Digital_Games_and_Escapism (last visited Sept. 19, 2014).

[91] *See* Marc Jonathan Blitz, *A First Amendment for Second Life: What Virtual Worlds Mean for the Law of Video Games*, 11 VAND. J. ENT. & TECH. L. 779 (2009).

[92] *See* John Suler, *The Online Disinhibition Effect*, 7 CYBERPSYCHOLOGY & BEHAVIOR 321 (2004), *available at* http://online.liebertpub.com/doi/pdf/10.1089/1094931041291295.

[93] Cam Robinson, *Reality Check - Why Are Online Gamers Jerks? (Video),* GAMESPOT (Nov. 10, 2013), http://www.gamespot.com/videos/reality-check-why-are-online-gamers-jerks/2300-6416026/ (last visited Feb. 15, 2014) (citing Suler, *supra* note 92).

[94] *Id.*

[95] *Id.*

A recent study conducted by the Nanyang Technological University and Singapore and Shanghai Jiao Tong University found that anonymity, among other things, does, in fact, make individuals more likely to cheat and engage in bad behavior.[96] However, the researchers also found that the players considered themselves to be part of a social group where the norm was to cheat, which may have attributed to the cheating. [97] Thus, the study claimed that socials norms, such as cheating, could be subject to change. [98] Additionally, the study concluded that cheating may not be part of anonymous gaming, but instead anonymous gaming could create social groups and a sense of belonging. [99]

While the arguments over mean YouTube comments or angry "Tweets" from peoples' Twitter accounts rage on, it is important to note that there is a difference between common Internet communications and online video game worlds. Many of these virtual worlds were specifically created to give players the ability to "escape," become someone else, or assume the roles of heroic fantasy characters.[100] For many people this is a chance to create their own private story.[101] In the case of *Second Life*, a large portion of the game's environment, and the core element of the game, is based around the idea of a living out a life separate from the player's real life, generating your own stories and experiences.[102]

---

[96] Chris Pereira, *Anonymity Encourages Bad Behavior in Online Games,* IGN (Jan. 9, 2014), http://www.ign.com/articles/2014/01/09/anonymity-encourages-bad-behavior-in-online-games.

[97] *Id.*

[98] *Id.*

[99] *Id.*

[100] *What is World of Warcraft*, WORLD OF WARCRAFT, http://us.battle.net/wow/en/game/guide/ (last visited Sept. 14, 2014).

[101] *Id.*

[102] *What is Second Life?*, SECOND LIFE, http://secondlife.com/whatis/?lang=en-US (last visited Sept. 14, 2014).

Thus, the aspect of anonymity could indicate an expectation of privacy for many gamers. There may be an expectation from the gamer when they create an avatar in an online video game that they have some privacy. This is compounded by the fact that most gamers play within their own homes and on their own video game consoles. As discussed above, until recently many video game consoles sole purpose was to play these video games. But the release of the new consoles and the development of inter woven cellphone apps and social media has affected gaming in many ways, which could hinder online video game player's expectation of privacy.

B. Non-legal Remedies To Government Fears of Anonymity?

Video games used to be separated from social media, however that difference has recently started to erode. Many video game companies and social media companies have started to provide ways to link player's social media accounts to their online video game accounts.

In 2010, *World of Warcraft* and *Second Life* changed their privacy policies for the forum comments.[103] The online games now require that certain forum postings by a player must use their real names. Blizzard Entertainment Inc., which runs *World of Warcraft*, has since implemented a new system called Real ID.[104] Real ID is a system that allows a player to link their in-game avatar with their account information, including their full names. [105] While Blizzard does place restrictions on which of the gamers fellow players can see the Real ID information, it does allow Blizzard to view that information.[106]

---

[103] Vijayan, *supra* note 11.

[104] *Id.*

[105] *Id.*

[106] Blizzard *Privacy Policy*, *supra* note 8.

In 2013 Google sought to address vicious comments on YouTube by requiring that YouTube accounts be linked to Google+ accounts.[107] Google+ is the Google equivalent of Facebook, and requires that a member's photo and name be associated with their account.[108] Thus, if there is a chance that a post can be associated to an actual person, then there is less of a chance that the comment will be mean or cruel. [109]

Many video game companies have followed suite, including the PlayStation Network and Xbox Live. PlayStation Network now allows and encourages users to connect their PlayStation Network accounts to their social medial accounts.[110] Sony has also included new features in their Play Station 4 that give players additional abilities to share their in-game activities with other players. Sony went as far as to include a share button on their new gaming controllers for the PlayStation 4.[111] These new sharing tools allow the gaming companies to collect more data on their users and better identify either trouble or dangerous users. But these features also end a large amount of anonymity once enjoyed by the gamers. While the features and privacy features are controllable, it definitely removes some of the expectations of privacy from video games.

Cam Robinson, a journalist at GameSpot, proposes that a possible way to address online gaming anonymity is through the Kinect.[112] If the player's face or eyes could be associated or even seen by other players, then video game users might be more inclined to be less callous

---

[107] Paul Tassi, *Google Plus Creates Uproar Over Forced YouTube Integration,* FORBES (Nov. 9, 2013, 10:24AM http://www.forbes.com/sites/insertcoin/2013/11/09/google-plus-creates-uproar-over-forced-youtube-integration/.

[108] *Id.*

[109] *Id.*

[110] Stephen Totilo, *Study The PS4's Social Network Settings Before Putting It Online*, KOTAKU (Nov. 13, 2013, 4:30 PM), http://kotaku.com/these-are-the-social-network-settings-your-ps4-would-li-1463946510.

[111] *Social Sharing and Connectivity*, IGN, http://www.ign.com/wikis/playstation-4/Social_Sharing_and_Connectivity (last visited Feb. 16, 2014).

[112] Robinson, *supra* note 93.

towards each other.[113] Reducing anonymity online and in video games could lead to a reduction in the attitude of the players towards each other and reduce the possibility criminals seeing video games or Internet communications as viable options to avoid the police. Thus, associating a person with their own online persona could have implications in the legal world. Ending anonymity in gaming could end a criminal's use of video games as a vehicle to commit crimes.

It could be argued that due to the nature of gaming and gamers there is no need for ending anonymity. Gamers tend to be self-regulating. Most large gaming companies hire "moderators" to monitor the activity of the players for cheating and rude behavior that could otherwise ruin the game for the other players. For example, *World of Warcraft* employs "Game Masters" who can chat in game with players to monitor and report on in game activity that violates their terms of use policies for the game.[114] Additionally, many games include a reporting system where players can report the abuse and cheating of other players. For example, online video games that are installed and operated on a computer through Steam use the "Valve Anti-Cheat System" which includes the ability for gamers to report other gamers who cheat.[115] An extreme example of gamer self-regulation occurred when a teenager in Austin, Texas was flagged and reported to the police for a comment the player had made while playing *League of Legends* - an online multiplayer game - about shooting a school full of kids.[116] The teenager allegedly made the comment jokingly, but a woman in Canada was able to look up the teenager's

[113] *Id.*

[114] *Game Master Interaction, Battle.net Support*, BLIZZARD ENTM'T. (last updated Oct. 18, 2014), https://us.battle.net/support/en/article/game-master-interaction-policy.

[115] *Valve Anti-Cheat System (VAC)*, *Steam Support*, VALVE CORP., https://support.steampowered.com/kb_article.php?ref=7849-Radz-6869 (last visited Mar. 10, 2015).

[116] Robby Soave, *Texas teen makes violent joke during video game, is jailed for months*, DAILY CALLER (June 27, 2013, 8:02 PM), http://dailycaller.com/2013/06/27/texas-teen-makes-violent-joke-during-video-game-is-jailed-for-months/.

address and report him to the Austin Police. The police charged him for making a terrorist threat.[117] These new additions to the online video game industry make it increasingly hard for gamers to argue for an expectation of privacy.

If companies included illegal or suspicious behavior to the list of reportable offenses, government agencies such as the NSA and the FBI would not need to have their own players in the game. However, as stated in the NSA documents, it is difficult for the NSA to differentiate between online gaming traffic and regular Internet traffic.[118] This has led to government agents creating their own avatars and profiles in games in order to search for terrorists and criminals. [119] But, that method is, of course, limited if the government cannot access or identify the people behind the avatars. Thus, the government must rely on the big businesses to provide them with the data and intelligence.

V. VIDEO GAMES AND BIG BUSINESS

Derek Witte makes the argument that the United States Supreme Court has openly opposed the creation of "Big Brother" but that "Big Brother" already exists in the form of major tech companies such as Google and Facebook.[120] He goes on to argue that lawmakers must step up to protect the fundamental right of privacy before it is lost.[121] Witte contends that lawmakers must fight for new legislation because consumers, the average citizen, are powerless to bring about such changes to protect privacy.[122] With the massive amounts of data that could be

[117] *Id*.

[118] *NSA Documents*, *supra* note 3.

[119] *Id.*

[120] Witte, *Privacy Deleted*, *supra* note 67, at 13.

[121] *Id.*

[122] *Id.*

collected through video game avatars, profiles, and video game purchases, these concerns extend to the online gaming world. Or is there something different about video games and video game consumers?

At the time it was announced, the new Xbox One was met with a surprising controversy concerning one of its technologies, the Kinect. The new Xbox One comes with Kinect, a technology that combines a camera and microphone, which allows the consumer to interact with the Xbox One through hand motions and voice commands.[123] The Kinect has incredible capabilities that allow it to recognize individuals.[124] At their announcement of the Xbox One, Microsoft stated that their new console would be always connected to the online servers. After the announcement, consumers became concerned that the Xbox One would always be on, and through the Kinect, the Xbox One would be watching their every move, even when they were not playing video games.[125] Microsoft insisted that the Kinect was an essential and integrated part of the Xbox One and thus need to be plugged in all the time to the Xbox One.[126] Player's fears were compounded when they learned soon after the Xbox One announcement that Microsoft had provided the NSA and the FBI with encryption workarounds needed to access other Microsoft products, such as Skype video calls, Outlook email, and online chats.[127] While Microsoft has not given a clear reason regarding the reverse in policy, months later Microsoft quietly removed the

---

[123] *Xbox Privacy Statement*, MICROSOFT (last updated Nov. 2014), http://www.microsoft.com/privacystatement/en-us/xbox/default.aspx.

[124] Brian Crecente, *Privacy concerns threaten to overshadow Microsoft's new console*, POLYGON (June 5, 2013, 11:14 AM), http://www.polygon.com/2013/6/5/4398440/privacy-microsoft-xbox-one.

[125] Yannick Lejacq, *Game on for surveillance? Privacy advocates concerned over new consoles,* NBC NEWS, http://www.nbcnews.com/tech/video-games/game-surveillance-privacy-advocates-concerned-over-new-consoles-f6C10732136 (last visited Feb. 16, 2014).

[126] *Id.*

[127] Larry Frum, *Microsoft backtracks on Xbox One sharing policies*, CNN (last updated June 21, 2013, 12:45 PM) http://www.cnn.com/2013/06/19/tech/gaming-gadgets/xbox-drm/.

always-on feature for the Xbox One and changed their Privacy Policy.[128] Thus, consumers and media attention was able to create a change in a company's privacy policy.

But has that event made a serious impact on what data Microsoft, Sony, and other online gaming companies collect? The answer is: not really. Microsoft still collects data from the Kinect and so do most online video game companies.[129]

A. Have Gamers Given Up Their Privacy Rights?

New data analytics have opened new doors for gaming companies.[130] In the gaming context, analytics use in-game data and information gathered from the player's actions as a way of learning gamers' behavioral patterns while the play. [131] This allows the companies to learn many things about their players, such as when and for how long gamers view a specific advertisement. [132] Additionally, for a fee, the companies are able to forward the data to online players, thereby allowing the players to use the data to improve their own gaming skills. These data collection improvements often come at a price. The video game company could use analytics to collect private data about a player's Internet usage among other private information. [133] Often, many companies do not update their privacy policies to inform the players about the

---

[128] *Id.*

[129] *Id.*

[130] Joseph Gregory, *Analytics in Video Games: Gamer's Best Friend or Privacy Nightmare?*, N. Y. LAW SCHOOL INSTITUTE FOR INFORMATION LAW AND POLICY LEGAL BLOG NETWORK, *available at* http://web.archive.org/web/20130601192517/http://www.allyourlawarebelongtous.com/analytics-in-video-games-gamer%E2%80%99s-best-friend-or-privacy-nightmare.

[131] *Id.*

[132] *Id.*

[133] *Id.*

collection of this data, and in order to gain access to MMO's the player has often already given authorization to the company to collect the data. [134]

What types of personal and private information do these video game companies actually have access to? Blizzard Entertainment's privacy policy may be a good analysis of a company's information policies. Blizzard owns and created some of the most popular massive multiplayer online games to date, including *World of Warcraft*, *StarCraft* and *Diablo*.[135] As Blizzard Entertainment's privacy policy states, the company may collect information concerning the consumer's:

> (1) the purchase of goods or services though our on-line stores, (2) product or account registration, or registration for on-line game participation, (3) player match-up services, (4) message boards or forums, (5) eCards or Recruit-a-Friend e-mails, (6) warranty registrations, (7) contest registrations, (8) a consumer complaint, (9) surveys, (10) customer service or technical support, and/or (11) newsletters. Personal information collected may include your name, home address, phone number, and/or e-mail address.[136]

Blizzard is quick to point out that the information is always given up voluntarily. Of course that does not mean that you will have access to the online game if you refuse to give up the information. "We do not require this information to gain access to our sites, however, you will not be able to utilize certain products, services, or features that require registration or receive materials such as newsletters unless such information is provided."[137] Like many video game companies, Blizzard uses the consumer's personal information to create analytic data "for

---

[134] *Id.*

[135] Blizzard's Privacy Policy, *supra* note 8.

[136] *Id.*

[137] *Id.*

internal marketing, profiling, or demographic purposes."[138] As discussed above this could have both positive and negative consequences.

More interesting information on Blizzard Entertainment's Privacy Policy is contained within the section describing with whom Blizzard may share this information with. This includes third party vendors who fulfill product orders or prizes, process mailings, or process, analyze, and/or store data on Blizzard's behalf.[139] In addition to third party vendors, Blizzard also claims your information as an asset of their company, "as with any business, your personal information is also an asset of Blizzard and will become part of our normal business records. As such, we may also disclose your personal information to a third party if we decide to sell a line of business to that third party…"[140] The the privacy policy does not clearly identify these third parties. At a minimum, Blizzard is partnered with at least twenty-one companies that create ancillary products, such as board games and manga, for their game universes.[141] Accordingly, at least twenty-one companies may have access to the consumer's information than the consumer may have intended.

Additionally, Blizzard keeps track of Internet Protocol ("IP") addresses, which is the unique number assigned to an individual user's server or Internet Service Provider ("ISP").[142] IP's allow site tracking and can be used for security purposes.[143] But the information can also be

[138] *Id*.

[139] *Id.*

[140] Blizzard's Privacy Policy, *supra* note 8.

[141] Manga are Japanese comics and graphic novels. *Partners*, BLIZZARD ENTM'T, http://us.blizzard.com/en-us/company/about/partners.html (last visited Feb. 16, 2014).

[142] Blizzard's Privacy Policy, *supra* note 8.

[143] *Id.*

used to report aggregated information. [144] Tracking and server information can be used to determine the location of a computer or console.[145]

Furthermore, when all of the data collected by the company is viewed together, the gaming companies can create vastly detailed pictures of the activity that occurs on a player's computer or gaming console.[146] Some consumers do not even realize they are forfeiting their personal information to major corporations. [147] Most consumers have not considered what might happen after they hand over their data. [148] While the government is limited by legislation on the sale and use of our personal information, private companies are not limited. [149] Corporations bear the burden of maintaining the cloud storage and the physical servers that process and store all of their online games' processes and information, which is not cheap. [150] However, the usage and buying or selling of our personal information to marketing companies or corporate partners can be lucrative.[151]

There is also the issue as to whether or not these companies comply or assist the government in pursuing criminals and terrorists. The Privacy Policy states that Blizzard will comply with any disclosure requirements mandated by law, or if the players' actions or conduct may cause harm to any other party either intentionally or unintentionally, and to anyone else who

---

[144] *Id*.

[145] Stephanie Crawford, *What is an IP address?*, HOWSTUFFWORKS, http://computer.howstuffworks.com/Internet/basics/question549.htm (last visited Feb. 16, 2014).

[146] Witte, *Bleeding Data*, *supra* note 69.

[147] *Id.*

[148] *Id.*

[149] *Id.*

[150] *Id.*

[151] Jason Morris & Edward Lavandera, *Why Big Companies buy, sell your data,* CNN (last updated Aug. 23, 2012, 3:52 PM), http://www.cnn.com/2012/08/23/tech/web/big-data-acxiom/.

could be harmed by the activities.[152] Because the government limits the amount of disclosure, it is unclear how much personal information companies divulge to the government.[153]

Previously, the government had a gag order on companies preventing them from even disclosing the fact that requests for data were made by the government. [154] It was only after the document leaks by Edward Snowden that the government slightly relaxed this policy. [155] Of course the transparency reports later released by the companies may be unreliable as companies only release information they feel necessary to reassure customers. [156] It would be more effective if the government were more transparent and released the information on the data requests themselves. [157]

To Blizzard's credit, it does provide clear statements regarding when and how players can opt out of programs. [158] Additionally, Blizzard claims to have taken steps to assure that all the information they collect will remain secure, such as partnering with Truste, a data protection company. [159] However, Blizzard refuses to guarantee the security of the information that is in the hands of third parties. [160] With all the data and access a gamer gives to a big video game company, it is not likely that a gamer would have any expectation of privacy from that company.

---

[152] Blizzard's Privacy Policy, *supra* note 8.

[153] Criag Timberg & Adam Goldman*, U.S. to allow companies to disclose more details on government requests for data*, WASH. POST (Jan. 27, 2014), http://www.washingtonpost.com/business/technology/us-to-allow-companies-to-disclose-more-details-on-government-requests-for-data/2014/01/27/3cc96226-8796-11e3-a5bd-844629433ba3_story.html.

[154] *Id.*

[155] *Id.*

[156] *Id.*

[157] *Id.*

[158] Blizzard's Privacy Policy, *supra* note 8.

[159] *Id.*

[160] *Id.*

The only remaining question is whether these companies will continue to support the government's actions.

B. Future Government and Businesses Action Together.

Companies will most likely continue to work with governments and governmental agencies. In exchange for user information from the gaming companies, government can provide both security and protection from criminals and civil remedies. These companies also seek to protect their own users from criminals and terrorists. Doing so is in their best interest, as breaches of data and fraud can hurt both their profits and public image. Government surveillance and technology can help companies avoid data breaches such as the PlayStation Network data breach in 2009.[161] The breach of Sony PlayStation Network in 2011 leaked a possible 77 million users' account information, including names, addresses, and possible credit card data, in one of the largest internet security break-ins ever.[162] The breach cost Sony an estimated 170 million dollars.[163] The company also faced lawsuits from private citizens and governments in the United States and Europe. [164] Thus, companies have an incentive to comply with government regulations that protect consumer data and government authorities that can help investigate if a breach occurs.

Businesses and governments are also acting together on many different issues. For example, in 2012, New York Attorney General Eric Schneiderman announced "Operation Game

---

[161] Liana Baker & Jim Finkle, *Sony PlayStation suffers massive data breach*, REUTERS (Apr. 26, 2011, 7:36 PM), http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426.

[162] *Id.*

[163] IDT911, *Two Years On, Lessons Learned From the Playstation Data Breach,* IDENTITY THEFT 911 BLOG (MAY 13, 2013), http://www.idt911blog.com/2013/05/two-years-on-lessons-learned-from-the-playstation-data-breach/.

[164] *Id*.

Over."[165] The goal of the program was to remove all registered sex offenders from several online gaming services.[166] Over 3,500 accounts were removed by Microsoft, Apple, Blizzard, Electronic Arts, Disney, Warner Bros. and Sony, with each company consenting to the operation.[167]

Video game companies and big businesses are not in the business of data protection. They are in the business of making money for their shareholders. And while gamers may want to have a feeling of anonymity or privacy, that protection most likely does not exist.

CONCLUSION

Future technologies create increasing challenges to law enforcement officials and lawyers trying to keep up with the law. Richard Kemp states that prediction is the next big step on the road to the "Internet of everything," with "processors in your fridge to let you know when the yoghurt's going off or you're nearly out of milk; autonomous vehicles; expert systems; virtual helpers and other smart machines."[168] He predicts the growing consumer demand for social media and mobile data and an increase in cloud computer storage. [169]

The availability of alternate means of communication, such as pay as you go cell phones, and video chat programs, such as Skype, Facebook, and Internet chat rooms give criminals a wide range of communication options. The vast amount of different modes of communication,

---

[165] Richard Mitchell, *New York State removes sex offenders from Xbox live*, ENGADGET (April 5, 2012, 4:40 PM) http://www.engadget.com/2012/04/05/new-york-state-removes-sex-offenders-from-xbox-live-more/ (last visited Feb. 15, 2014).

[166] *Id.*

[167] *Id.*

[168] Richard Kemp, *Trends in Information Technology Law: Looking Ahead to 2014*, KEMPLITTLE, http://www.kemplittle.com/site/articles/kl_bytes/Trends_in_Information_Technology_Law_Looking_Ahead_to_2014 (last visited Feb. 15, 2014).

[169] *Id.*

Internet or otherwise, may undermined or reduce the effectiveness for surveillance in video games. This is especially true when there is no evidence that these surveillance programs have had any effect in deterring or preventing terrorism or crime.[170]

It is not all bad news for those who enjoy playing video games. A report by Benjamin Engelstatter of the Centre for Economic Research, Scott Cunningham of Baylor University, and Michael Ward of the University of Texas, have suggested that an increase in sales of either violent or non-violent crime can be associated with a decrease in violent and non-violent crime.[171]

Since the Supreme Court has not addressed many of the issues facing online gaming and virtual worlds concerning privacy, it is not clear whether gamers should have expectation of privacy from government intrusion. While many parts of the online game itself maybe public, there are many aspects of online video games that are private or appear to be private. It is hard to justify an expectation of privacy when the corporation that runs the game servers and systems claims ownership of all the personal information a player provides. The corporation also claims ownership of all in game actions and materials and which could compliment self-regulation of online games. Since it is also unclear the extent to which government and private corporations share information, there is no way to verify if the government has already viewed or accessed a player's personal information.

Anonymity in online games has its perks and its down sides. Anonymity allows for self-expression and self-discovery without fear of persecution. However anonymity can lead to

---

[170] *NSA Documents*, *supra* note 3.

[171] Benedict Carey, *Shooting in the Dark,* N. Y. TIMES (Feb. 12, 2013), *available at* http://www.nytimes.com/2013/02/12/science/studying-the-effects-of-playing-violent-video-games.html?pagewanted=1&_r=4&ref=science.

cheating. Additionally, anonymity can allow criminals and terrorists to act and communicate without the possibility of government supervision. Additionally, despite any expectations there are no specific laws or rulings by the Supreme Court that give gamers an expectation of privacy with in the games that they play. Furthermore, there are no clear rules as to what parts of a video game experience may be protected. Are single player experiences more private than multiplayer experiences? Do they deserve the same protections simply because they are played using the same hardware and software? Privacy concerns grow as technology grows and develops.

The leaked NSA documents most likely only describe the tip of the iceberg in government surveillance capabilities both in online games and on the Internet at large. But since the government has not been transparent about its data collection capabilities, it remains unclear what laws if any the government has violated. And thus, some may find it upsetting that despite the revelation that government agents are playing video games with you, they may not have violated any privacy laws. However, it is possible that many online video game players may now have a greater interest in a job with the FBI or NSA. In conclusion, a gamer does not have expectation of privacy, but there should be more transparency for the government's actions.