FIGHTING ON A NEW BATTLEFIELD ARMED WITH OLD LAWS: HOW TO MONITOR TERRORISM IN THE VIRTUAL WORLD[†]

Lisa Ugelow[*]
Lance J. Hoffman[**]

INTRODUCTION

The United States has always relied in part on surveillance practices to obtain information about foreign governments, international and domestic organizations, and citizens of the United States. The twentieth century exemplifies this behavior. In 1918, the Overman Committee was established to investigate pro-German sentiments, and later investigated the influence of Communist Bolsheviks in the United States.[1] In 1930, the Fish Committee was established to investigate people and organizations suspected of being involved with or supporting Communist activities in the United States.[2] From 1934–1937, the Special Committee on Un-American Activities Authorized to Investigate Nazi Propaganda and Certain Other Propaganda Activities, also known as the McCormack-Dickstein Committee, was formed to investigate how Nazi propaganda came into the United

† Work on this paper was supported in part by funding from the Offices of the Vice President for Research, the Dean of the School of Engineering and Applied Science, and the Provost of The George Washington University. Errors and opinions stated are solely those of the authors and do not necessarily reflect the opinions of The George Washington University or of any entities thereof.

* Recipient of her LL.M. in National Security and U.S. Foreign Relations Law from The George Washington University Law School and her J.D. from Albany Law School in New York.

** Distinguished Research Professor of Computer Science and Director, Cyber Security Policy and Research Institute, The George Washington University.

1 Regin Schmidt, RED SCARE: FBI AND THE ORIGINS OF ANTICOMMUNISM IN THE UNITED STATES, 1919–1943, 136.

2 Crystal Hoffer, *The Birth of Anticommunist National Rhetoric: The Fish Committee Hearings in 1930s Seattle*, GREAT DEPRESSION IN WASHINGTON STATE (Spring 2009), http://depts.washington.edu/depress/fish_committee.shtml#_ednref2.

States, and to investigate the organizations spreading it.[3] During World War II, the House Committee on Un-American Activities ("HUAC") was established as a special investigating committee of the House of Representatives.[4] HUAC succeeded the Fish Committee and the McCormack-Dickstein Committee, and was developed to investigate alleged disloyalty and subversive actions by private citizens, public employees, and those organizations suspected of having Communist ties.[5] HUAC became a permanent committee in 1945,[6] but it slowly lost favor until it was denounced by President Harry Truman in 1959 as the "most un-American thing in the country today."[7]

However, surveillance by the United States became hotly contested again in the 1970s, due to the widespread disapproval of the Vietnam War and the unfolding of the Watergate scandal. The United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, more commonly known as the Church Committee, investigated intelligence-gathering methods by the Central Intelligence Agency and the Federal Bureau of Investigation for illegality. New laws, such as the Foreign Intelligence Surveillance Act, regarding proper surveillance procedures were developed as a result of these investigations.

Due to the globalization of computer usage and the Internet, the effectiveness and applicability of these laws may be diminishing. Terrorists have become quite sophisticated in carrying out their terrorism plans, and it seems like the rest of the world is always reacting defensively to the newest terrorism means. However, the non-terrorists could be on the offensive by exploring a possible new medium that can be used by terrorist organizations—virtual worlds.

Although there has been no public proof to date of terrorists devising plots in virtual worlds such as World of Warcraft,[8] Second Life,[9]

---

3 Sam Tanenhaus, *Investigating Un-American Activities, Now and Then*, N.Y. TIMES: ARTS BEAT (Mar. 9, 2011, 5:00 PM), http://artsbeat.blogs.nytimes.com/2011/03/09/investigating-un-american-activities-now-and-then/.

4 *HUAC (House Un-American Activities Committee)*, HISTORY.COM, http://www.history.com/topics/house-un-american-activities-committee (last visited Feb. 17, 2012).

5 *Id.*

6 *See* ROBERT K. CARR, THE HOUSE COMMITTEE ON UN-AMERICAN ACTIVITIES 1945–1950, at 19 (1952) (describing HUAC as "one of the most remarkable procedural coups in modern Congressional history").

7 STEPHEN J. WHITFIELD, THE CULTURE OF THE COLD WAR 124 (1996) (internal quotation marks omitted).

8 WORLD OF WARCRAFT, http://us.battle.net/wow/en/ (last visited May 9, 2011).

9 SECOND LIFE, http://secondlife.com/ (last visited May 9, 2011).

and others, some members of Congress[10] and some terrorism experts[11] fear that this is next on the agenda for terrorist organizations. Terrorists can be rehearsing attacks in these virtual worlds, just like the United States military trains with commercial "shoot-em-up games."[12] Virtual world massive multiplayer games make it easy to contact and assemble plotters from around the world. Virtual worlds are hard to monitor because a user account name is a pseudonym for the individual user, the access is global, and the language used may be hard to decode. Therefore, using virtual worlds to carry out terrorist activities, recruit, communicate, and launder money may require the United States either to use existing law or create new legislation that permits the federal government or Internet service providers ("ISPs") to monitor this type of conduct in the virtual world.

This Article is divided into three Parts: I. Surveillance before the terrorist attacks on September 11, 2001 ("9/11") in the United States;[13] II. Surveillance post-9/11; and III. Surveillance in the virtual world. Specifically, Part I will provide a general discussion about United States surveillance law before 9/11. Part II will discuss how surveillance law changed due to 9/11. Finally, Part III will focus on the applicability of the United States' surveillance laws to virtual worlds and how to protect the United States from the possible use of virtual worlds to engage in terrorist activity.

I. SURVEILLANCE BEFORE 9/11

Citizens of the United States have always been entitled to protection from intrusions by the federal government into their private conversations and communications. The Fourth Amendment of the United States Constitution and statutory provisions such as Title III of the Omnibus Crime Control and Safe Streets Act ("Wiretap Act"), the Foreign Intelligence Surveillance Act ("FISA"), and the Communica-

10 *See* Sharon Weinberger, *Congress Freaks Out Over Second Life Terrorism*, WIRED (Apr. 4, 2008, 12:44 PM), http://www.wired.com/dangerroom/2008/04/second-life/ ("One of the concerns, brought up by some members of Congress, was that *Second Life* could be used [to] launder terrorist funds.").

11 Natalie O'Brien, *Spies Watch Rise of Virtual Terrorists*, AUSTRALIAN (July 31, 2007, 12:00 AM), http://www.news.com.au/top-stories/spies-watch-rise-of-virtual-terrorists/story-e6frfkp9-1111114075761 ("[T]errorism experts are warning that [Second Life] attacks have ramifications for the real world.").

12 Noah Shachtman, *Pentagon Researcher Conjures Warcraft Terror Plot*, WIRED (Sept. 15, 2008, 5:22 PM), http://www.wired.com/dangerroom/2008/09/world-of-warcra/.

13 NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT (2004).

tions Assistance for Law Enforcement Act ("CALEA") have protected this right. However, each of these laws has loopholes that can be used to circumvent ordinary privacy expectations. Additionally, National Security Letters can also be used to obtain records of transactional data, further circumventing privacy expectations. This Part will address the enactment and application of each of these laws prior to 9/11.

A. Fourth Amendment Protection

One way the federal government is prohibited from monitoring its citizens' communications is through the Fourth Amendment of the United States Constitution. The Fourth Amendment states, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause . . . ."[14] An individual's Fourth Amendment rights are implicated when the federal government's conduct amounts to a "search."

In the United States Supreme Court case, *Katz v. United States*, Justice Harlan, in his concurring opinion, established a two-prong test to determine when government action constitutes a search.[15] First, does the individual have an actual (subjective) expectation of privacy? Second, does society recognize that this expectation is (objectively) reasonable?[16] The standard to evaluate whether a search is reasonable requires assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed to advance a legitimate governmental interest.

When an individual is in public, such as driving, talking outside to a friend, or shopping at a mall, there is no reasonable expectation of privacy. Because anyone can observe his or her behavior, an individual does not have an actual expectation of privacy regarding conduct in public. Furthermore, there is no objective expectation of privacy in these scenarios because it would be unreasonable for society to think that actions in public are private actions entitled to Fourth Amendment protection. In contrast, conduct in one's home is considered private because a home is one's personal space, and the home is considered sacrosanct. However, if individuals present *outside* of one's private home can hear a conversation occurring inside the home, or can smell an odor coming from the home, there is no

14 U.S. CONST. amend. IV.

15 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

16 *Id.*

reasonable expectation of privacy in the contents of that conversation or odor.[17] Only activity contained within the home is covered by an increased expectation of privacy. Once the activity can be observed or noticed outside the home, it loses this higher form of protection. Under most circumstances, conduct *inside* an individual's home is expected to be protected from government intrusion; society would find this expectation reasonable because a government's interest in intruding into the sanctity of one's home is generally outweighed by an individual's privacy interest.[18]

Generally, a search is considered unreasonable unless there is a warrant issued by a neutral magistrate supported by probable cause. However, there are some exceptions to the Fourth Amendment warrant requirement for a search. The ones relevant here are consent to be searched,[19] exigent circumstances,[20] and whether evidence is located in plain view.[21] First, the consent exception applies when an individual voluntarily agrees to be monitored under certain circumstances. This voluntary agreement eliminates any reasonable expectation of privacy in such conduct. Second, exigent circumstances exist when there is an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, to forestall the imminent escape of a suspect, or to thwart the destruction of evidence. There is no standard test for determining whether such circumstances exist, and in each case the extraordinary situation must be measured by the facts known by officials.[22] However, those circumstances must "cause a reasonable person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts."[23] Exigency may be

17 *Reasonable Expectation of Privacy*, EFF SURVEILLANCE SELF-DEFENSE PROJECT, https://ssd.eff.org/your-computer/govt/privacy (last visited May 9, 2011).

18 *See Katz*, 389 U.S. at 361 (Harlan, J., concurring) ("[A] man's home is, for most purposes, a place where he expects privacy . . . .").

19 J. SCOTT HARR & KÄREN M. HESS, CONSTITUTIONAL LAW AND THE CRIMINAL JUSTICE SYSTEM 219 (3d ed. 2005).

20 United States v. Smith, 797 F.2d 836, 840 (10th Cir. 1986) (explaining that a warrantless search conducted by police officers is constitutional when there are exigent circumstances, and any seizure of evidence as a result is permissible).

21 Horton v. California, 496 U.S. 128, 133 (1990) (determining that a warrantless seizure of evidence in plain sight is not prohibited by the Fourth Amendment).

22 People v. Ramey, 545 P.2d 1333, 1341 (Cal. 1976) (discussing whether exigent circumstances exist is based upon an evaluation of the facts as they are known to an officer).

23 United States v. McConney, 728 F.2d 1195, 1199 (9th Cir.), *cert. denied*, 469 U.S. 824 (1984).

determined by a variety of factors, such as the degree of urgency involved, the amount of time needed to get a warrant, whether evidence is about to be removed or destroyed, and/or ready destructibility of the evidence.[24] Third, the plain view doctrine is applicable when three factors are satisfied: a) the officer is lawfully present at the place where the evidence can be plainly viewed; b) the officer has a lawful right of access to the object; and c) the incriminating character of the object is "immediately apparent."[25] If any of these exceptions apply, then there is no reasonable expectation of privacy;[26] therefore, the protections afforded by the Fourth Amendment are not implicated.

B. Title III of the Omnibus Crime Control and Safe Streets Act

Another mechanism prohibiting the federal government from monitoring its citizens' communications is Title III of the Omnibus Crime Control and Safe Street Act of 1968.[27] Title III is better known as the Wiretap Act.[28] Briefly, the Wiretap Act addresses the issuance of domestic criminal surveillance warrants. Specifically, the Wiretap Act: "[1] prohibits the unauthorized, nonconsensual interception of 'wire, oral, or electronic communications'[29] by government agencies as well as private parties[; 2] establishes procedures for obtaining warrants to authorize wiretapping by government officials[;] and [3] regulates the disclosure and use of authorized intercepted communications by investigative and law enforcement officers."[30]

The procedures established in order to obtain a warrant authorizing wiretapping by a government official are similar to the Fourth Amendment warrant requirement. The Wiretap Act permits a judge to issue a warrant authorizing interception of communications for up to thirty days upon a showing of probable cause that the interception

---

24 United States v. Reed, 935 F.2d 641, 642 (4th Cir.), *cert. denied*, 502 U.S. 960 (1991) (discussing various factors to consider when determining if exigent circumstances exist).

25 *Horton*, 496 U.S. at 136–37 (internal quotation marks omitted) (outlining the elements of the plain view doctrine in order to establish the constitutionality of a warrantless search under these circumstances).

26 *Reasonable Expectation of Privacy*, *supra* note 17.

27 18 U.S.C. §§ 2510–2522 (2006).

28 *The Nature and Scope of Governmental Electronic Surveillance Activity*, CENTER FOR DEMOCRACY & TECH. (July 2006), http://www.cdt.org/wiretap/wiretap_overview.html.

29 18 U.S.C. § 2511(1)(a) (2006). The term "electronic communications" was added by Title I of the Electronic Communications Privacy Act in 1986. *See Privacy & Civil Liberties*, JUST. INFO. SHARING, http://it.ojp.gov/default.aspx?area=privacy&page=1284 (last visited Feb. 6, 2012).

30 *Privacy & Civil Liberties*, *supra* note 29.

will reveal evidence that "an individual is committing, has committed, or is about to commit a particular offense" listed in 18 U.S.C. § 2516.[31]

However, the Wiretap Act's warrant requirement can be overcome by a variety of exceptions. First, like the exigent circumstances exception to the Fourth Amendment warrant requirement, the Wiretap Act's warrant requirement can be overcome by

> any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that . . . an emergency situation exists that involves . . . immediate danger of death or serious physical injury to any person, [or there are] conspiratorial activities threatening the national security interest . . . that require[] a wire, oral, or electronic communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained . . . .[32]

Basically, this exception applies when it has been reasonably determined that an emergency situation exists that requires information to be intercepted without delay. An emergency situation is one that could result in immediate death or serious physical injury to any person, or that involves a conspiracy that threatens the national security interest of the United States.

Second, like the consent exception to the Fourth Amendment warrant requirement, the Wiretap Act also has a consent exception. This exception states that "[i]t shall not be unlawful . . . for a person acting under color of law to intercept a[n] . . . electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception."[33] In regards to this exception, a "person" is defined to include an "agent of the United States . . . , any individual, partnership, association, . . . or corporation[.]"[34]

Third, the Wiretap Act has an ISP exception. This exception makes the warrant requirement of the Wiretap Act inapplicable in regards to the "intercept[ion], disclos[ure], or use" of an "electronic communication" by a "provider of [a] wire or electronic communication service . . . engaged in any activity which is a necessary incident to . . . the protection of the rights or property of the provider of that service . . . ."[35] Basically, this exception gives a service provider the

---

31 18 U.S.C. § 2518(3)(a).
32 *Id.* § 2518(7).
33 *Id.* § 2511(2)(c).
34 *Id.* § 2510(6).
35 *Id.* § 2511(2)(a)(i).

right "to intercept and monitor [communications] placed over their facilities in order to combat fraud and theft of service."[36] With that said, this exception does not allow service providers to engage in unlimited screening.[37] However, a service provider and its agents can engage in reasonable screening, which means that a balance is reached between the service provider's interests to safeguard its rights and property, and its users' right to privacy in their electronic communications.[38]

C. Foreign Intelligence Surveillance Act

FISA governs the process for electronic surveillance of foreign intelligence information within the United States.[39] Under FISA, a warrant is required to obtain information through electronic surveillance. FISA provides four distinct definitions of what constitutes "electronic surveillance."[40] These definitions are as follows:

> (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
>
> (2) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511(2)(i) of Title 18;
>
> . . . .
>
> (4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire . . . communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.[41]

---

36 United States v. Villanueva, 32 F. Supp. 2d 635, 639 (S.D.N.Y. 1998).

37 *See* United States v. Auler, 539 F.2d 642, 646 (7th Cir. 1976) ("This authority of the telephone company to intercept and disclose wire communications is not unlimited.").

38 *See* United States v. Harvey, 540 F.2d 1345, 1351 (8th Cir. 1976) ("The federal courts . . . have construed the statute to impose a standard of reasonableness upon the investigating communication carrier.").

39 Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (2006).

40 *Id.* § 1801(f)(1)–(4).

41 *Id.* § 1801(f)(1)–(2), (4).

In other words, the government is required to obtain a warrant to engage in electronic surveillance when it is intentionally targeting a United States citizen who has a reasonable expectation of privacy; it acquires communication without the consent of any party; or it obtains information from something other than a wire communication when an individual has a reasonable expectation of privacy.

The procedure to get a warrant under FISA requires the Department of Justice ("DOJ") to apply to the Foreign Intelligence Surveillance Court ("FISC") to receive a court order authorizing surveillance of foreign agents.[42] The federal agent applying for a court order only needs to demonstrate probable cause to believe that the "target of the electronic surveillance is a foreign power or an agent of a foreign power,"[43] that "a significant purpose" of the surveillance is "to obtain foreign intelligence information," and that appropriate "minimization procedures" are in place.[44] The minimization requirement is implemented to minimize the collection, retention, and dissemination of information.[45] The agent does not need to demonstrate that the commission of a crime is imminent.[46] However, there is an additional requirement if the target includes United States persons, which are defined as United States citizens, permanent resident aliens, and United States corporations. This additional requirement that must be proven by the federal agent is that "the target knowingly engages in sabotage or international terrorism or is preparing for such activities."[47]

The FISA warrant requirement is also subject to a few exceptions. The only relevant exception here gives the President authority to engage in electronic surveillance to acquire foreign intelligence information without a FISC order when the Attorney General certifies that there is "no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person

---

42 *Id.* § 1805.

43 *Id.* § 1804(a)(4)(A). For purposes of FISA, agents of foreign powers include agents of foreign political organizations and groups engaged in international terrorism, as well as agents of foreign nations. *Id.* § 1801(b).

44 *Id.* § 1804(a)(5), (7)(B).

45 *Foreign Intelligence Surveillance Act (FISA)*, ELECTRONIC PRIVACY INFO. CTR., http://epic.org/privacy/terrorism/fisa/ (last visited Feb. 20, 2012) (explaining that "[m]inimization procedures are designed to prevent the broad power of foreign intelligence gathering from being used for routine criminal investigations" (internal quotation marks omitted)).

46 *Id.*

47 *Id.*

is a party," provided the surveillance is directed solely at communications among or between foreign powers.[48]

D. Communications Assistance for Law Enforcement Act

CALEA was enacted by Congress in 1994 because of law enforcement's concern that the increased use of digital telephone exchange switches would make tapping phone lines harder or impossible.[49] Basically, CALEA requires telephone companies to design their networks in a way that makes it easier for the federal government to conduct criminal investigations using wiretapping of telephone networks.[50] The purpose of CALEA is to enhance the ability of law enforcement and intelligence agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment, facilities, and services to ensure that they have built-in surveillance capabilities, which allow federal agencies to monitor all telephone traffic under certain circumstances.[51]

E. National Security Letters

A National Security Letter ("NSL") is a type of administrative subpoena that is used by federal agencies to obtain various records and data pertaining to an individual from a particular entity or organization.[52] NSLs can only request non-content information, such as transactional records, phone numbers dialed, or e-mail addresses in the "to" or "from" field.[53] An NSL does not have to be supported by probable cause or have judicial oversight.[54]

National Security Letters were first used in 1986 to circumvent the Right to Financial Privacy Act[55] in counterintelligence cases and were limited to foreign powers or persons who the FBI had reasonable

48 50 U.S.C. § 1802(a)(1)(B).

49 *CALEA*, ELECTRONIC FRONTIER FOUND., http://www.eff.org/issues/calea (last visited May 9, 2011).

50 Communications Assistance for Law Enforcement Act, 47 U.S.C. §§ 1001–1010 (2006).

51 *Id.*

52 *National Security Letters*, ELECTRONIC PRIVACY INFO. CTR., http://epic.org/privacy/nsl/#overview (last visited May 9, 2011).

53 *Overview: What Does an NSL Do?*, ELECTRONIC PRIVACY INFO. CTR., http://epic.org/privacy/nsl/#overview (last visited Feb. 20, 2012).

54 *Legal Authority for NSL Power*, ELECTRONIC PRIVACY INFO. CTR., http://epic.org/privacy/nsl/#authority (last visited Feb. 20, 2012).

55 *Id.*

cause to believe were agents of a foreign power.[56] Compliance with this NSL was voluntary, and state consumer privacy laws usually permitted institutions to decline these requests.[57] This remedy never identified any penalties for failing to comply with an NSL request.[58] In 1993, restrictions regarding obtaining information from a "foreign power" were relaxed, and the use of NSLs was expanded to include any person suspected of communicating with foreign agents regarding espionage or terrorism.[59]

NSLs are different from traditional subpoenas or warrants. First, they contain a non-disclosure provision. An entity that receives an NSL is prohibited from disclosing to anyone that they received an NSL or the contents of the NSL.[60] Second, they do not require judicial oversight—the judicial branch is not required to approve the issuance of an NSL.[61] This has led to some problems in implementation, as described later.[62]

II. SURVEILLANCE AFTER 9/11

The events that occurred on September 11, 2001 have greatly impacted the law enforcement landscape of the United States. Since 9/11, the United States has been more aggressively developing policies and using tactics to protect United States citizens from terrorist attacks and punish those responsible for them. These policies address actual attacks on United States soil or overseas against United States citizens, the aiding and abetting of terrorist activities, and the planning of terrorist activities. Many rights and laws that existed prior to 9/11, such as the Fourth Amendment protection against unreasonable searches, the Wiretap Act, FISA, CALEA, and the use of National Security Letters have been adapted or reinterpreted since 9/11 to accommodate these new policies and tactics.

---

56 Barton Gellman, *The FBI's Secret Scrutiny*, WASH. POST, Nov. 6, 2005, at A1.

57 Right to Financial Privacy Act, 12 U.S.C. § 3405 (2006).

58 *Id.*

59 *Basic Look at National Security Letters*, USA TODAY, Mar. 9, 2007, http://www.usatoday.com/news/washington/2007-03-09-1844717959_x.htm.

60 *National Security Letters*, *supra* note 52. Following enactment of the PATRIOT Reauthorization Act of 2005, however, entities receiving NSLs may disclose if doing so to seek legal advice or otherwise comply with the NSL. *Id.* Various cases, such as *Doe v. Holder*, 640 F. Supp. 2d 517 (S.D.N.Y. 2000), and *Doe v. Mukasey*, 549 F.3d 861 (2d Cir. 2008), have challenged the non-disclosure requirement as unconstitutional, which has resulted in limitations being placed on the non-disclosure requirement.

61 *National Security Letters*, *supra* note 52.

62 *See infra* p. 1049.

A. Fourth Amendment Protection

Although the text of the Fourth Amendment of the United States Constitution has not been altered, the interpretation of what constitutes a reasonable search and when an exception to the warrant requirement is applicable has been interpreted more broadly since 9/11. For example, during the Bush Administration, President George W. Bush authorized the warrantless eavesdropping on Americans and others inside the United States to find evidence of terrorist activity.[63] This program included the monitoring of international telephone calls and international e-mail messages.[64] The Bush administration viewed this behavior as necessary so the federal government could move quickly to monitor communications that may disclose threats to the United States.[65] Victims of this warrantless surveillance have attempted to seek redress in federal courts. While most cases have been dismissed, some cases, such as the case that was formerly known as *Al-Haramain Islamic Foundation, Inc. v. Bush*,[66] have been decided against the United States.[67] However, this pro-plaintiff outcome is unusual, and *Al-Haramain* may have turned out differently if it had been heard in a federal court that tends to favor the government on national security matters.[68]

Although it is hard to prove that the Fourth Amendment has been interpreted differently since 9/11, Jameel Jaffer, an attorney with the American Civil Liberties Union, acknowledges that "[i]f you take a broad look at the big Fourth Amendment cases that have been decided since 9/11 . . . it's pretty clear that, in applying the 'reasona-

63 *Bush Administration's Warrantless Wiretapping Program*, WASH. POST, Feb. 12, 2008, http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051500999.html.

64 *Id.*

65 *Id.*

66 507 F.3d 1190 (9th Cir. 2007).

67 Kevin Bankston, *Court Rejects Government's Executive Power Claims and Rules That Warrantless Wiretapping Violated Law*, ELECTRONIC FRONTIER FOUND. (Mar. 31, 2010), https://www.eff.org/deeplinks/2010/03/court-rules-warrantless-wiretapping-illegal (last visited July 24, 2011); Burke Hansen, *Bush-Authored Warrantless Wiretapping Suffers Abrupt Defeat*, REGISTER, Apr. 2, 2010, http://www.theregister.co.uk/2010/04/02/warantless_wiretapping_defeat/.

68 Hansen, *supra* note 67; David Kravets, *Feds Appeal Warrantless-Wiretapping Defeat*, WIRED: THREAT LEVEL (Feb. 22, 2011, 4:14 PM), http://www.wired.com/threatlevel/2011/02/feds-appealing-wiretap-defeat/ (acknowledging the oddity of the San Francisco federal judge ruling against the federal government in a national security case).

bleness' test, the courts have been more deferential to the executive since 9/11 than they were before 9/11."[69]

B. Title III of the Omnibus Crime Control and Safe Streets Act

The Wiretap Act was modified after 9/11 by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("PATRIOT"), the PATRIOT Reauthorization Acts in 2006, and the FISA Amendments Act of 2008. Most significantly, the PATRIOT Act of 2001 added terrorist and computer crimes to the Wiretap Act's predicated offense list.[70]

C. Foreign Intelligence Surveillance Act

FISA was also modified after 9/11 by the PATRIOT Act of 2001, the Intelligence Reform and Terrorism Prevention Act of 2004, and the FISA Amendments Act of 2008. The PATRIOT Act made a variety of changes to FISA. First, it eased the restrictions on foreign intelligence gathering within the United States. The PATRIOT Act did this by permitting "roving" surveillance, which allows the interception of any communications made to or by an intelligence target without specifying the particular telephone line, computer, or other facility to be monitored.[71] The probable cause standard now requires only that a significant purpose of surveillance be the gathering of foreign intelligence information, instead of it being the sole or primary purpose.[72] Second, the United States intelligence community was given greater access to information discovered during a criminal investigation, which meant that "the wall" between criminal investigation and intelligence gathering was eliminated.[73] Lastly, the PATRIOT Act prohibits a cause of action in any court against a provider of a wire or electronic communication service, landlord, custodian, or any other person that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under such Act.[74]

---

69 E-mail from Jameel Jaffer, Attorney, Am. Civil Liberties Union, to author (Apr. 6, 2011, 5:48 PM) (on file with author).

70 PATRIOT Act of 2001 § 814, Pub. L. No. 107-56, 115 Stat. 382 (codified as amended at 18 U.S.C. § 1030 (2006)).

71 *Id.* tit. 2, § 206.

72 *Id.* § 218.

73 *Id.* § 203(a), (c).

74 *Id.* § 225.

The Intelligence Reform and Terrorism Prevention Act of 2004 amended the definition of a "foreign power or agent of a foreign power" by adding the "Lone Wolf" Amendment.[75] Under FISA, the "Lone Wolf" Amendment makes a non-United States person who engages in international terrorism or activities in preparation for international terrorism an "agent of a foreign power" regardless of that individual's actual status.[76] This Amendment was added to FISA in response to the FBI's failure to prosecute Zacarias Moussaoui.[77] The FBI and Immigration and Naturalization Service in Minneapolis detained Moussaoui on August 16, 2001 for a visa waiver violation.[78] Although the FBI soon discovered that Moussaoui held jihadist beliefs and was suspected of being an Islamic extremist, the FBI failed to get a court order under FISA from the FISC authorizing surveillance because the FBI believed that FISA standards could not be met since the FBI could not find any evidence that Moussaoui was an agent of a foreign power.[79] However, in the aftermath of the 9/11 terrorist attacks, there was speculation that Moussaoui was the missing twentieth hijacker, and the failure on the part of law enforcement and the intelligence side to fully investigate Moussaoui when he was in FBI custody prior to the 9/11 attacks became a huge point of criticism.[80] The United States wanted to ensure that a "lone wolf" would not slip through the cracks again.

The FISA Amendments of 2008 also made a variety of alterations to FISA. They allow eavesdropping in emergencies without court approval, provided the government files required papers within a week, and they expand the range of persons being targeted by warrantless electronic surveillance.[81] Specifically, the Amendments permit the FISC to have jurisdiction over a United States person reasonably believed to be located outside the United States in order to acquire foreign intelligence information.[82] Finally, the Amendments provide immunity for any electronic communication service provider that

75 Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742 (2004).

76 Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801(b)(1) (2006).

77 *See* Patricia L. Bellia, *The "Lone Wolf" Amendment and the Future of Foreign Intelligence Surveillance Law*, 50 VILL. L. REV. 425, 426 (2005) (stating that the "Moussaoui episode" prompted the FISA amendment).

78 *Id.* at 425.

79 *Id.* at 425–26.

80 *Id.* at 426.

81 *FISA Amendments Act of 2008*, WALL ST. J., June 19, 2008, http://online.wsj.com/article/SB121391360949290049.html.

82 *Id.*

provides information, facilities, or assistance to the Attorney General and the Director of National Intelligence,[83] in addition to their previous immunities.

D. Communications Assistance for Law Enforcement Act

CALEA has been modified post-9/11 as well. The biggest change occurred in 2004 when CALEA mandates were extended to the Internet.[84] The DOJ, the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), the FBI, and the Drug Enforcement Administration ("DEA") filed a joint petition with the Federal Communications Commission ("FCC") to expand their powers to include the ability to monitor Voice-over-Internet-Protocol ("VoIP") and broadband Internet communications in order to monitor Web traffic as well as phone calls.[85] The FCC adopted these requests in a "First Report and Order," which was reaffirmed in 2006 in a "Second Report and Order."[86]

Furthermore, the role of CALEA has significantly increased. From 2004 to 2007, there was a 62% growth in the number of wiretaps performed under CALEA and more than a 3000% growth in the interception of digital files, such as e-mail.[87]

E. National Security Letters

As a result of 9/11 and the Bush Administration, the PATRIOT Act significantly expanded the use of NSLs. For example, the number of NSLs that are issued each year has increased. Now, the FBI issues more than 30,000 NSLs a year.[88] Additionally, NSLs are now used to scrutinize United States citizens, residents, or visitors who are not suspected to be part of any criminal investigation.[89]

NSLs do have their limitations. For example, they cannot be utilized as a way to eavesdrop or read the contents of e-mail. However, since 9/11 NSLs have allowed investigators to "obtain sensitive information such as the web sites a person visits, a list of e-mail addresses with which a person has corresponded, or even unmask the

---

83 *Id.*

84 CALEA FAQ, ELECTRONIC FRONTIER FOUNDATION, (Mar. 5, 2012), https://www.eff.org/pages/calea-faq.

85 *Communications Assistance for Law Enforcement Act (CALEA)*, FED. COMMS. COMMISSION (Feb. 21, 2007), http://www.fcc.gov/calea/.

86 *Id.*

87 Ryan Singel, *Point, Click . . . Eavesdrop: How the FBI Wiretap Net Operates*, WIRED (Aug. 29, 2007), http://www.wired.com/politics/security/news/2007/08/wiretap?currentPage=3.

88 Gellman, *supra* note 56.

89 *Id.*

identity of a person who has posted anonymous speech on a political website."[90]

III. SURVEILLANCE IN THE VIRTUAL WORLD

The virtual world is a three-dimensional computer-generated portrayal of the real world but existing only in cyberspace.[91] Virtual worlds are set up just like the real world—"users will find the sun, wind, buildings, paved streets, grass, rivers, seas, mountains, islands, and countries, all recreated to look and 'feel' as if users were actually living in cyber reality."[92]

Originally, virtual worlds were just massive multiplayer online role-playing games, or MMORPGs,[93] where a user creates a character to represent himself, which is known as an "avatar."[94] An avatar does not have to be an exact replication of a user, and a user's avatar can take on different and new roles in the virtual world.[95]

However, as time has passed, virtual worlds have become more than just a game.[96] As in the real world, users can go to work, conduct business, attend virtual churches, and join virtual societies.[97] Virtual worlds have become so popular that about 20 to 30 million users actually "spend" more time in virtual worlds than they do in the real world.[98] These worlds are becoming more than a world of make-believe. "[R]eal-life corporations, universities, government agencies, and medical centers are venturing into virtual worlds to hold classes, conduct research, and provide training."[99] Now, virtual worlds are even being used to train soldiers.[100]

---

90 *National Security Letters*, ACLU (Jan. 10, 2011), http://www.aclu.org/national-security-technology-and-liberty/national-security-letters.

91 *See* THE STATE OF PLAY: LAW, GAMES, AND VIRTUAL WORLDS 3 (Jack M. Balkin & Beth Simone Noveck eds., 2006).

92 Bettina M. Chin, *Regulating Your Second Life: Defamation in Virtual Worlds*, 72 BROOK. L. REV. 1303, 1303 (2007). "[Second Life] is ostensibly a free-range graphical environment where users may explore, interact, create, and trade as they do in real life—only this happens, of course, in a 'second life.'" *Id.* at 1304.

93 EDWARD CASTRONOVA, SYNTHETIC WORLDS: THE BUSINESS AND CULTURE OF ONLINE GAMES 9 (2005).

94 THE STATE OF PLAY, *supra* note 91, at 15.

95 *See id.*

96 *See id.* at 16.

97 *See id.* at 15.

98 *See id.* at 16.

99 Chuleenan Svetvilas, *Real Law in the Virtual World*, CAL. LAW. (Jan. 2008), http://www.callawyer.com/clstory.cfm?pubdt=NaN&eid=890855&evid=1.

100 *See* THE STATE OF PLAY, *supra* note 91.

Along with all the benefits that virtual worlds provide, the use of virtual worlds can also cause problems. The main concern regarding virtual worlds has been expressed by intelligence officials who have examined virtual world systems and are convinced that "the qualities that many computer users find so attractive about virtual worlds—including anonymity, global access and the expanded ability to make financial transfers outside normal channels—have turned them into seedbeds for transnational threats."[101] "Unfortunately, what started out as a benign environment where people would congregate to share information or explore fantasy worlds is now offering the opportunity for religious/political extremists to recruit, rehearse, transfer money, and ultimately engage in information warfare or worse with impunity."[102]

This concern that virtual worlds will be used as the next terrorist battlefield raises issues regarding the proper limits that need to be placed on the government's quest to improve security through data collection and analysis and the surveillance of commercial computer systems. The following evaluation of monitoring virtual worlds in relation to the Fourth Amendment of the United States Constitution, the Wiretap Act, FISA, CALEA, and the use of National Security Letters will hopefully shed some light on this growing area of concern.

A. Statutory Application

1. Fourth Amendment Protection

An important consideration is whether the Fourth Amendment protection against unreasonable searches also applies to conduct in the virtual world. One argument is that if virtual world technology is intentionally designed to make humans act as though the virtual world is in some respects real, then the law ought to respect privacy expectations as it does in real life. If so, then if an avatar is out at a shopping mall or driving a car in the virtual world, this conduct would be considered public and no reasonable expectation of privacy would exist (in that virtual world). Contrastingly, if an avatar was engaging in activity within his virtual home, than this would be considered private conduct protected from unwanted intrusion.

---

101 Robert O'Harrow, Jr., *Spies' Battleground Turns Virtual*, WASH. POST, Feb. 6, 2008, http://www.washingtonpost.com/wpdyn/content/article/2008/02/05/AR2008020503144.html?sub=AR.

102 *Id.*

Under this line of thinking, just like in the real world, any search would be subject to the Fourth Amendment warrant requirement and would be considered unreasonable without a warrant. However, the same exceptions to the warrant requirement, such as consent to be searched, exigent circumstances, and evidence located in plain view, would apply. For example, if an individual entering the virtual world is notified that his virtual conduct is monitored and the individual agrees, then just like in real life, there is no reasonable expectation of privacy and the avatar's conduct can be monitored. Arguably, the virtual world is a recognized public community; therefore, whoever develops an avatar voluntarily and knowingly agrees to live and play in this public community, thereby eliminating any reasonable expectation of privacy. Furthermore, some virtual worlds, such as Second Life, include a privacy statement in its "Community Standards."[103] This statement explains that Residents are entitled to a reasonable level of privacy with regard to their Second Lives.[104] This means that sharing personal information about a fellow Resident—including gender, religion, age, marital status, race, sexual preference, and real-world location beyond what is provided by the Resident in the First Life page of their Resident profile—is a violation of that Resident's privacy.[105] Also, remotely monitoring conversations, posting conversation logs, or sharing conversation logs without consent are all prohibited in Second Life and on the Second Life Forums.[106] However, if a person voluntarily shares this information, then there is no reasonable expectation of privacy.[107]

Another exception that may apply to the virtual world could be an exigent circumstance. An exigent circumstance is an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, or to forestall the imminent escape of a suspect or destruction of evidence. There is no standard test for determining whether such circumstances exist, and in each case the extraordinary situation must be measured by the facts known by officials.[108] However, these circumstances would cause a reasonable

---

103 *Community Standards*, SECOND LIFE, http://secondlife.com/corporate/cs.php (last visited Feb. 20, 2012).

104 *Id.*

105 *Id.*

106 *Id.*

107 *See Privacy Policy*, SECOND LIFE, http://secondlife.com/corporate/privacy.php#privacy1 (last visited Feb. 18, 2012) (stating that personal information disclosed while using Second Life "is public information and [the user] should not expect privacy or confidentiality of this information").

108 People v. Ramey, 545 P.2d 1333, 1341 (Cal. 1976).

person to believe that entry (or other relevant prompt action) was necessary to prevent physical harm to the officers or other persons, the destruction of relevant evidence, the escape of a suspect, or some other consequence improperly frustrating legitimate law enforcement efforts.[109] Exigency may be determined by a variety of factors, such as the degree of urgency involved, the amount of time needed to get a warrant, whether evidence is about to be removed or destroyed, and/or ready destructibility of the evidence.[110] Information in the virtual world can easily be deleted and/or encrypted to prevent or greatly hinder understanding of it. Because of this, obtaining a warrant may not be possible before evidence is lost forever, so the government or an internal overseer of the virtual world should be allowed to retrieve or monitor information about an avatar's behavior and activities.

Lastly, the plain view doctrine may apply in the virtual world as well. The real world plain view doctrine requires that three factors must be satisfied: (1) the officer has to be lawfully present at the place where the evidence can be plainly viewed; (2) the officer has to have a lawful right of access to the object; (3) the incriminating character of the object has to be "immediately apparent."[111] This test can also be applied to the virtual world. An overseer, such as Linden Lab, an ISP, or the government is allowed to monitor conduct in the virtual world if the conduct is illegal. Both Linden Lab and an ISP are lawfully present through a contract, such as the Terms of Service, that a user of the virtual world agrees to upon signing up with the service.[112] The government is lawfully present due to the fact that the conduct is illegal. Therefore, the first requirement of lawful presence would be satisfied.[113] Obtaining a warrant could also satisfy the requirement of being lawfully present. Second, upon being lawfully present, if Linden Lab, an ISP, or the government sees terrorist plans or weapons that are left out in the open in the virtual world, like on a table or on the floor, then the second prong would be satisfied. Third, possessing terrorist plans and weapons, such as bombs, although in the virtual world, is still incriminating because its illegality is immediately apparent. Therefore, if these three elements are satis-

109 United States v. McConney, 728 F.2d 1195, 1199 (9th Cir. 1984).

110 United States v. Reed, 935 F. 2d 641, 642 (4th Cir. 1991).

111 Horton v. California, 496 U.S. 128, 136–37 (1990).

112 *Terms of Service*, SECOND LIFE, http://secondlife.com/corporate/tos.php?lang=en-US#tos8 (last visited Feb. 20, 2012) (stating that posting, displaying, or transmitting illegal content is not permitted and will be reported to the authorities).

113 *Horton*, 496 U.S. at 136–37.

fied, then the plain view exception would apply, and there would be no reasonable expectation of privacy in this behavior. Based on this analysis, if a virtual terrorist cell is raided or searched, then this evidence could be seized.

The third element of the plain view doctrine—the incriminating nature must be immediately apparent—may be the hardest to prove. This is because the illegality of conduct, such as possessing terrorist plans or weapons, which occurs in the virtual world, may not be as apparent as it would be in the real world. Conduct in the virtual world could be considered mere thoughts, and it is hard to hold someone accountable for their thoughts.

However, in the real world, an individual can be held accountable for illegal conduct even if the conduct was never achieved. According to the Model Penal Code, a person is guilty of an attempt to commit a crime if an individual "purposely does or omits to do anything that, under the circumstances as he believes them to be, is an act or omission constituting a substantial step in a course of conduct planned to culminate in his commission of the crime."[114] With that said, possessing terrorist plans on its own may not be enough to constitute a substantial step to commit a terrorist act in the real world. However, possessing terrorist plans as well as possessing weapons to carry out a terrorist act in the real world without actually carrying out the act could amount to a substantial step in furtherance of the unlawful conduct. This conduct could result in an individual being prosecuted for an attempt to commit a crime under the criminal law.[115]

With this understanding of criminal attempt law, conduct that may be considered mere thoughts in the virtual world could be evaluated similarly to conduct in the real world that falls under criminal attempt law. Drawing this similarity to criminal attempt law in the real world would allow for the illegality of conduct in the virtual world to be immediately apparent in some situations. For example, just possessing terrorist plans or just possessing weapons on their own in the virtual world, as in the real world, is arguably not enough to prove that the illegality of this conduct is immediately apparent. However, it is possible that these actions taken in the aggregate, meaning possessing both weapons and a terrorist plan, could amount to conduct where the illegality is immediately apparent. This is be-

114 MODEL PENAL CODE § 5.01(1)(c) (1980).

115 This Article does not discuss whether conspiracy or attempt law is applicable in the virtual world.

cause a single thought in the virtual world could be seen as unimportant, but multiple thoughts about engaging in a common criminal activity, such as engaging in a terrorist activity, could be seen as a substantial step making the illegality of this conduct immediately apparent. Therefore, in order for the third element to be satisfied in the plain view doctrine, an avatar would need to possess both virtual terrorist plans and weapons, or a combination of other conduct relating to engaging in a terrorist activity, in the virtual world.

Another argument is that the virtual world is not real, so there is no reasonable expectation of privacy in anything that occurs in it. This means that there is no Fourth Amendment protection. Virtual worlds are fictitious worlds where users voluntarily enter for fun and games. They are open spaces intended for its users to inhabit and interact via avatars. Anyone is welcomed in—all you need is a membership. Basically, the virtual world is a public sphere, like a community. Because of this, an individual may not find surveillance in a virtual world offensive. Furthermore, courts have not found a reasonable expectation of privacy in "matters which occur in a public place or a place otherwise open to the public . . . ."[116] Therefore, if a virtual world is considered a public space (and it is certainly open to the public because anyone can create and maintain an avatar), then there is no reasonable expectation of privacy in conduct that occurs in the virtual world.

2. Title III of the Omnibus Crime Control and Safe Street Act

Another important consideration is whether the Wiretap Act applies to conduct that occurs in the virtual world. As mentioned previously, the Wiretap Act: (1) prohibits the unauthorized, nonconsensual interception of "wire, oral, or electronic communications"[117] by government agencies as well as private parties; (2) establishes procedures for obtaining warrants to authorize wiretapping by government officials; and (3) regulates the disclosure and use of authorized intercepted communications by investigative and law enforcement officers.

Communication that takes place in the virtual world occurs over a wire or electronically; therefore, communication among avatars in the virtual world would be protected from government surveillance

116 Fogel v. Forbes, Inc., 500 F. Supp. 1081, 1087 (E.D. Pa. 1980).

117 Electronic communications were added by Title I of the Electronic Communications Privacy Act in 1986. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, tit. 1, §§ 101(c)(2), 110(b), 100 Stat. 1851, 1859 (current version at 18 U.S.C. § 2510 (2006)).

under the Wiretap Act unless there were an applicable exception. As previously discussed, the Wiretap Act has three applicable exceptions, which can be used to monitor communications in a virtual world absent a warrant. These exceptions are: (1) exigent circumstances; (2) consent to be monitored; and (3) the provider exception.

First, the exigent circumstances exception applies when a federal agent, who has been designated by someone like the Attorney General, "reasonably determines that . . . an emergency situation exists that involves—(i) immediate danger of death or serious physical injury to any person [or] (ii) conspiratorial activities threatening the national security interest . . . that requires a wire, oral, or electronic communication to be intercepted before an order authorizing such interception" can be obtained.[118] Virtual world conduct that is most likely to fall under this exception would be preparatory actions leading up to a terrorist activity because this behavior would constitute "conspiratorial activities threatening the national security interest."[119] This conduct may include the recruitment of terrorists or the communication among terrorists within the virtual world. Therefore, obtaining a warrant to monitor communications occurring in the virtual world under these circumstances would not be required.

Second, the consent exception to the Wiretap Act applies either when an individual, acting under color of law, is a party to the communication or one of the parties consents to have the communication monitored. This analysis is similar to the consent exception analysis under the Fourth Amendment of the United States Constitution.[120] If an individual who enters the virtual world is notified that his virtual conduct is monitored and that individual agrees, then just like in real life, there is no reasonable expectation of privacy and the avatar's conduct can be monitored.

However, the owners of Second Life, Linden Lab, can disclose a user's personal or other account-related information under limited circumstances.[121] For example, Linden Lab can share information "[i]n order to report to law enforcement authorities, or assist in their investigation of, suspected illegal or wrongful activity, or to report any instance in which we believe a person may be in danger[.]"[122] Therefore, by creating an avatar and knowingly and voluntarily agreeing to a virtual world's privacy statement and user agreement, a user has

118 *Id.* § 2518(7).
119 *Id.*
120 *See* HARR & HESS, *supra* note 19, at 219.
121 *Privacy Policy*, *supra* note 107.
122 *Id.*

consented to abide by that virtual world's rules, which may include mandatory reporting of illegal conduct or permitting law enforcement to monitor users if illegal conduct occurs.

Lastly, the provider exception allows a provider of a wire or electronic communication to intercept, disclose, or use any electronic communication if engaged in conduct that is necessarily incident to protecting the rights or property of that service provider. First, a virtual world needs to be a provider of a wire or electronic communication. Virtual worlds, such as Second Life, permit users to post, display, or transmit content throughout the virtual world through a network infrastructure.[123] Therefore, a virtual world that engages in this type of conduct would be a provider of wire or electronic communication. Second, a virtual world's conduct must protect its own rights or property, and not the rights of a third party.[124] Virtual worlds have an interest in protecting themselves from users who engage in illegal conduct, such as terrorist activity, and destroy the tranquility of the virtual world. If virtual worlds become a haven for illegal conduct, then law-abiding users may stop paying for accounts, and, as a result, the virtual worlds may have to shut down. For these reasons, the provider exception could permit virtual worlds to intercept, disclose, and use electronic communication without a warrant.

3. Foreign Intelligence Surveillance Act

An additional issue to consider is whether FISA applies to actions taken in the virtual world. A FISA warrant is required when dealing with the electronic surveillance of foreign intelligence information. In order to obtain a court order authorizing surveillance, FISA's probable cause standard has to be satisfied. This requires first that a federal agent demonstrate that there is probable cause to believe that the target of the surveillance is a foreign power, agent of a foreign power, or a non-United States individual who is engaged in terrorist conduct; and second, that the significant purpose of the surveillance is to obtain foreign intelligence information. Therefore, for federal agents to obtain a FISA warrant to engage in electronic surveillance

123 *Terms of Service*, *supra* note 112.

124 *See, e.g.*, Campiti v. Walonis, 611 F.2d 387, 393 (1st Cir. 1979) (explaining that the provider exception does not apply to a person who is not an agent of the telephone company for monitoring that "had nothing to do with telephone company equipment or rights"); United States v. Auler, 539 F.2d 642, 645–46 (7th Cir. 1976) (discussing how telephone companies that intercept communications under 18 U.S.C. § 2511(2)(a)(i) can share those communications with the federal government only to the degree necessary to protect the telephone company's rights or property).

they would need to show that the virtual world user is a foreign power, agent of a foreign power, or a non-United States individual who is engaged in terrorist conduct. This can be done by finding the subscriber's real world information, such as name, address, and telephone number, through the records held by service providers located in the real world. This information alone may not be enough to satisfy the first prong of the FISA probable cause standard because the information may not link to an actual person or a hacker could have hacked into an innocent user's account. However, once a user's name is identified, then this information could be used by federal agents to cross-match it with lists of known terrorists in the real world to see if the name is one of a known terrorist.

On the other hand, it may be easier to satisfy the second prong because to find a significant purpose an agent does not have to demonstrate that the commission of a crime is imminent, just that the significant purpose for obtaining a warrant is to gather foreign intelligence information. This foreign intelligence information can be found through online conversations among virtual world avatars, online postings in the virtual world, or conduct engaged in by avatars in the virtual world. Since no evidence of an actual crime needs to be proven, this makes satisfying the significant purpose test easier because the analysis of whether a virtual world crime can be prosecuted in real world courts is avoided.

FISA has a variety of definitions as to what conduct constitutes electronic surveillance requiring a warrant. The provisions that may be applicable here are 50 U.S.C. § 1801(f)(1), (2), and (4); however, monitoring conduct in a virtual world falls outside the scope of these provisions. In regards to § 1801(f)(1), agents can target a specific United States person within the United States, and if a reasonable expectation of privacy existed, then a warrant would be required to monitor communications. However, it can be argued that there is no reasonable expectation of privacy in a virtual world because an individual who enters the virtual world is notified that his virtual conduct can be monitored in limited circumstances and if that individual agrees to the terms of use, then just like in real life, there is no reasonable expectation of privacy, and the avatar's conduct can be monitored in these limited circumstances. Second Life, in its Terms of Use, lists one such limited circumstance to be assistance in a law enforcement investigation. Therefore, monitoring virtual world conduct may be outside the scope of FISA § 1801(f)(1), and a FISA order would not need to be obtained to monitor virtual world conduct if a user provides consent.

FISA § 1801(f)(2) pertains to obtaining the contents of wire communications without the consent of any party involved. Virtual worlds that have Terms of Use and/or Privacy Statements require their users to voluntarily and knowingly consent to be monitored in limited circumstances. Since users have to agree to the terms in order to use the services of the virtual world, § 1801(f)(2) also does not apply to the surveillance of conduct in the virtual worlds.

Moreover, § 1801(f)(4) also prohibits surveillance when there is a reasonable expectation of privacy. However, as previously discussed, as long as virtual worlds in their Terms of Use and/or Privacy Policy state that users' conduct is subject to be monitored in limited circumstances, then users of a virtual world have no reasonable expectation of privacy in conduct that falls within those limited circumstances. Therefore, monitoring conduct in virtual worlds falls outside the scope of § 1801(f)(4) as well.

Even if monitoring conduct in the virtual world fell within the scope of 50 U.S.C. § 1801(f)(1), (2), or (4), there is an exception to obtaining a FISA order that would be applicable in this situation. This exception, as discussed earlier, gives the President the authority to engage in electronic surveillance to acquire foreign intelligence information when there is no substantial likelihood that the surveillance will obtain communications to which a United States person is a party; the surveillance must be directed at communications among or between foreign powers. Therefore, as long as it can be proven that the avatars being monitored in the virtual world are agents of a foreign power, then the communications can be monitored without a warrant. This information can possibly be obtained by gaining access to subscriber information from the virtual world host.

Lastly, if monitoring conduct in the virtual world fell within the scope of 50 U.S.C. § 1801(f)(1), (2), or (4), yet the exception discussed above did not apply, then roving surveillance could be used. This is because due to the anonymity of the Internet and virtual worlds, it may be hard for federal agents to identify with precision the individual that they want to monitor. Under FISA, roving surveillance provides a federal agent with the flexibility to intercept communications made to or by an intelligence target without specifying the particular computer to be monitored.

4. Communications Assistance for Law Enforcement Act

It is also important to determine how CALEA applies to conduct in the virtual world. Since CALEA has been extended to the Internet, service providers are expected to work with law enforcement and in-

telligence agents to make monitoring Internet traffic easier. As discussed earlier, a virtual world owner can be categorized as a service provider because it is a network infrastructure that provides connectivity to the Internet that permits its users to communicate through chat, e-mails, and posts.[125] Therefore, requiring virtual worlds to follow CALEA mandates would actually make it easier to monitor conduct in the virtual world.

5. National Security Letters

Lastly, NSLs may be used to obtain information about conduct that occurs in the virtual world. As mentioned above, NSLs have been used by investigators to reveal the identity of a person who has posted anonymous speech on a political website. Therefore, NSLs can be used to unmask the identity of users in the virtual world. Because a user in the virtual world acts anonymously through an avatar, if the avatar's conduct relates to something political, such as terrorism, an NSL can be used as a way to obtain a user's subscription information from the virtual world host. The use of an NSL could be instead of, or to supplement, a subpoena because obtaining an NSL is much easier than obtaining a traditional subpoena.

It is important to note that NSLs have been criticized by a variety of organizations, such as the ACLU, due to their increased usage and abuse by the FBI as a result of the PATRIOT Act.[126] The ACLU has challenged this increased use of NSLs in three court cases—*Doe v. Holder*,[127] *Library Connection v. Gonzales*,[128] and *Internet Archive v. Mukasey*.[129] These cases found that in part or in whole the issuance of an NSL was unconstitutional.[130] Therefore, the further expansion of NSLs to the virtual world may be problematic.

B. Virtual Terrorist Conduct

There has been some growing concern that virtual worlds are actually being used by terrorist organizations to launder money, recruit,

---

125 *See supra* pp. 1056-57.

126 *See National Security Letters*, ACLU (Jan. 10, 2011), http://www.aclu.org/national-security-technology-and-liberty/national-security-letters (describing the ACLU's challenges to the PATRIOT Act and requests for information about the government's use of NSLs).

127 640 F. Supp. 2d 517 (S.D.N.Y. 2000).

128 Library Connection v. Gonzales, 386 F. Supp. 2d 66 (Conn. 2005).

129 Internet Archive v. Mukasey, No. 07-6346-CW (N.D. Cal. 2008); *see National Security Letters*, *supra* note 126.

130 *Id.*

communicate, and engage in virtual world terrorism. For example, Canadian Botnet Analysis Report describes a "dark universe" where "[v]irtual world terrorism facilitates real world terrorism: recruitment, training, communication, radicalization, propagation of toxic content, fund raising and money laundering, and influence operations" within online games.[131] The few examples and general understandings of this "dark universe" are described below.

1. Money Laundering

There are concerns regarding the terrorists' ability to take advantage of challenges in policing the movement of virtual currency, such as Linden dollars, through the transferring of funds between operatives around the world.[132] United States intelligence officials have been cautioning owners of virtual worlds that their programs may be creating security vulnerabilities for terrorists and criminals to move money, organize, and conduct corporate espionage.[133]

Although virtual owners in the United States have only been cautioned about these concerns, other online companies have already been victims of money laundering schemes. For example, recently "authorities in New York . . . charged more than 60 individuals—and arrested 20—in connection with international cyber heists perpetrated against dozens of companies in the United States . . . ."[134] The cyber criminals used a program to hack into the company's online banking webpages and steal passwords.[135] This resulted in more than $800,000 being laundered and sent to the attackers in Eastern Europe.[136] The investigation into this cyber crime and the takedown operation included efforts from a variety of entities—the U.S. Attorney's Office for the Southern District of New York, the FBI, the NYPD, the Department of State Diplomatic Security Service, the New York Office

131 COMBATING ROBOT NETWORKS AND THEIR CONTROLLERS: A STUDY FOR THE PUBLIC SECURITY AND TECHNICAL PROGRAM, BOTNET ANALYSIS, 112 (version 2.0 May 6, 2010), *available at* http://www.scribd.com/doc/51938416/Botnet-Analysis-Report-Final-Unclassified-v2-0.

132 Chris Gourlay & Abul Taher, *Virtual Jihad Hits Second Life Website*, SUNDAY TIMES, Aug. 5, 2007, at 4.

133 O'Harrow, Jr., *supra* note 101.

134 Brian Krebs, *U.S. Charges 37 Alleged Money Mules*, KREBS ON SECURITY (Sept. 30, 2010, 7:46 PM), http://krebsonsecurity.com/2010/09/u-s-charges-37-alleged-money-mules/#more-5470.

135 *Id.*

136 *Id.*

of Homeland Security Investigation, and the U.S. Secret Service.[137] Manhattan U.S. Attorney Preet Bharara was quoted saying that these

> arrests show [that] the modern, high-tech bank heist does not require a gun, a mask, a note, or a getaway car. It requires only the Internet and ingenuity . . . . And it can be accomplished in the blink of an eye, with just a click of the mouse. [However, this] coordinated operation demonstrates that these 21st Century bank robbers are not completely anonymous; they are not invulnerable. Working with our colleagues here and abroad, we will continue to attack this threat, and bring cyber criminals to justice.[138]

It is clear that the United States is taking these online money-laundering schemes very seriously. Hopefully, if virtual world owners become the next target, the techniques used to take down cyber criminals in the above-mentioned plot could easily be employed and effective in virtual worlds.

Even though owners of virtual worlds in the United States have not yet been impacted by money laundering schemes, a variety of countries abroad have been affected. For example, the Seoul Metropolitan Police Agency had to handle a money laundering situation in the virtual world.[139] A group of Chinese and Korean criminals defrauded Korean gamers and laundered funds through a number of business front companies back to mainland China.[140]

2. Recruitment or Communication via Virtual World

There is suspicion that Islamic militants are using or have used Second Life to recruit individuals to engage in terrorist conduct.[141] The head of the Australian government's High Tech Crime Centre, Kevin Zuccato, said that "jihadists may also be using the virtual reality world to master skills such as reconnaissance and surveillance."[142]

The virtual world is being used politically to gather support for different political campaigns. For example, during the most recent elections in Spain, most politicians had established a virtual presence in Second Life.[143] Some politicians had even established their own

---

137 *Id.*

138 *Id.*

139 Marc Goodman, *Crime and Policing in Virtual Worlds*, FREEDOM FROM FEAR MAGAZINE, http://www.freedomfromfearmagazine.org/index.php?option=com_content&view=article&*id*=316:crime-and-policing-in-virtual-worlds&catid=50:issue-7&Itemid= (last visited Feb. 18, 2012).

140 *Id.*

141 Gourlay & Taher, *supra* note 132, at 4.

142 *Id.*

143 Goodman, *supra* note 139.

avatars, which in turn campaigned, held rallies, and put up election posters in virtual spaces.[144] Additionally, during a recent political rally in the virtual world by a far-right French politician, his posters were defaced, he had "exploding [virtual] pigs" hurled at him, and Nazi swastikas were painted on campaign headquarters.[145]

3. Virtual World Terrorism

World of Warcraft has a history of in-game terrorist activity.[146] In the past, players would find a curse in a high-level dungeon that would turn them into living bombs.[147] "They would then teleport to major cities and detonate themselves, killing nearby players. These suicide bombers gradually began to target areas where a large number of players gathered, usually at auction houses or banks."[148] These attacks started to occur with so much frequency that some users began to avoid dangerous cities.[149]

Moreover, a "[v]irtual bioterrorist Allen and his guild, domus fulminata," used a comparable teleportation method to spread an epidemic throughout in-game virtual cities.[150] Allen and his guild used a contagious curse called "Corrupted Blood."[151] This curse had the ability to kill most players in seconds or to purposely infect other players.[152] Allen's conduct displayed telltale signs of terrorism because the group strategically blended in with the general population of the virtual world and preyed on weaknesses in the system in order to carry out an effective attack.[153]

Furthermore, an anonymous intelligence official confirms that some computer users have used their avatars to destroy virtual build-

144 *Id.*

145 Oliver Burkeman, *Exploding Pigs and Volleys of Gunfire as Le Pen Opens HQ in Virtual World*, GUARDIAN, Jan. 19, 2007, http://www.guardian.co.uk/technology/2007/jan/20/news.france (explaining that Marie Le Pen was the first European political party to open headquarters within Second Life, a virtual reality website, and her virtual campaign has incited a remarkable response from protesters).

146 *See* David Thier, *World of Warcraft Shines Light on Terror Tactics*, WIRED (Mar. 20, 2008), http://www.wired.com/gaming/virtualworlds/news/2008/03/wow_terror (describing games that incorporate terrorist themes and actions that serve as "an invaluable tool not only for counterterrorists and epidemiologists but also sociologists and economists").

147 *Id.*

148 *Id.*

149 *Id.*

150 *Id.*

151 *Id.*

152 *Id.*

153 *Id.*

ings,[154] which can be seen in some contexts as an act of terrorism in the virtual world.

C. How to Locate Terrorists in the Virtual World

Is it possible to attribute a real world terrorist attack to an organization that developed in the virtual world? If identification information matches between the avatar and the individual, the virtual plans can be used as evidence to show intent, knowledge, and guilt. However, attribution may be an issue, and this may be easier said than done.[155]

Prosecution of individuals who have committed online offenses requires evidence that a crime was committed and of who committed the crime. A way to prove the identity of an anonymous online offender is to obtain the identity of subscribers, such as name, address, and telephone number, through the records held by service providers located in the real world. Virtual worlds, such as Second Life, require that the information provided by a user to create an account be "accurate, current and complete information about [one]self as prompted by the registration form ('Registration Data') and [that the user] use the account management tools provided to keep . . . Registration Data accurate, current and complete."[156] This information can be obtained through subpoenas, for example to Linden Lab directly if dealing with a situation occurring in Second Life, to ISPs, or to PayPal. This disclosure of information is permissible because individuals who enter the virtual world generally sign an agreement allowing the owners of the online world to provide the government with information about its users under certain circumstances, such as in the case of a lawful investigation. For example, the government retains the power to ensure that networks of Linden Lab, which is the owner of Second Life, are "intercept-capable" and have data retention for a particular period.[157]

---

154 O'Harrow, Jr., *supra* note 101.

155 *See generally* Charles L. Glaser, *Deterrence of Cyber Attacks and U.S. National Security* 3 (George Washington Univ. Cyber Security Policy & Research Inst. Report GW-CSPRI-2011-5, June 1, 2011), *available at* http://www.cspri.seas.gwu.edu/seminar2010_2011.html (describing the various reasons and challenges for erecting government-supported defenses and deterrences to cyber attacks).

156 *See Terms of Service, supra* note 112 (describing the terms under which "Linden Research, Inc. and Linden Research United Kingdom, Ltd. (collectively 'Linden Lab') offer [users] access to Second Life").

157 *See generally* Sara M. Smyth, *Back to the Future: Crime and Punishment in Second Life*, 36 RUTGERS COMPUTER & TECH. L.J. 18, 42 (2009) (referring to Second Life's policy in 2009, but it is important to note that the government was given this authority).

Furthermore, the government can also require that the service agreement between Linden Lab and its users be drafted in such a way as to make it easier for the company to monitor and control illegal conduct by its users.[158] This might include the reporting of illegal content, as is already required with respect to all ISPs in cases of online child pornography.[159] Illegal content may also include terrorist plans. If this is true, then the owner of a virtual world that is being used as a breeding ground for virtual terrorist cells may also be required to report this conduct.

Scientists have proposed another way to identify the user behind an avatar without obtaining a court order or intercepting online communication. Researchers believe that the faces and behavior of avatars could help identify the user, and by "monitoring for signature gestures, movements and other distinguishing characteristics," a behavioral analysis could help determine whether an avatar has been hacked and stolen or is under the control of its owner.[160] This work is very preliminary, but the researchers involved are confident about the results because "[s]o far [they] have been very successful."[161] Therefore, the attribution issue may be closer to being solved.

With that said, finding ways to locate terrorist activity in the virtual world and then reporting it may be challenging. However, "spy avatars" or "undercover avatars" could be used. In the real world, law enforcement agencies use agents to go undercover in online chat rooms to pretend to be underage children as a way to catch adults who are posing as children. These agents go undercover in order to catch adults who are trying to set up meeting times with children to engage in sexual activity and child pornography. Real world law enforcement agents also infiltrate drug rings and terrorist cells by having agents pretend to work for the drug lords or terrorist groups. In actuality, they are working undercover in order to monitor and obtain evidence of illegal conduct. Similarly, in the virtual world, an employee of Linden Lab, an ISP, or the government could make an avatar and go undercover befriending other avatars and possibly becoming part of a virtual terrorist cell in order to obtain evidence that

158 *Id.*

159 *See* 42 U.S.C. § 13031 (2006) (describing the requirement to "make a report of the suspected abuse to the agency designated . . . to take emergency action to protect the child"); *see also* 42 U.S.C. § 13032 (imposing the duty to report any knowledge of facts or circumstances involving child pornography on all who are engaged in providing an electronic communication service or remote computing service to the public).

160 *Virtual People to Get ID Checks*, BBC NEWS (July 28, 2011, 8:12 PM), http://www.bbc.co.uk/news/technology-14277728.

161 *Id.* (quoting Dr. Yampolskiy, a researcher from the University of Louisville).

terrorist activity is occurring in the virtual world. Once the undercover avatar becomes part of a virtual terrorist cell, it would be easier to monitor the cell's current and future conduct. This solution may be costly; however, existing employees can be the ones who make spy avatars, so no extra money would be expended to hire additional personnel.

D. Obtaining Evidence in the Virtual World

As discussed earlier, to obtain a criminal warrant under the Fourth Amendment of the United States Constitution or under the Wiretap Act, a federal agent must prove that under the circumstances known to him or her there is a reasonable belief that a person has committed, is committing, or is about to commit a crime.[162] Also, as previously mentioned, the FISA probable cause standard to obtain a warrant is slightly different. In actuality, the standard for obtaining a FISA wiretap warrant is lower than the standard for getting a criminal wiretap warrant. Under FISA, there needs to be a finding of probable cause that the surveillance target is a foreign power or an agent of a foreign power, irrespective of whether the target is suspected of engaging in criminal activity.[163] There is also an additional element if the target is a United States person.[164] The federal agent then also has to prove that the target knowingly engages in sabotage or international terrorism or is preparing for such activities.[165]

Should the virtual world be subjected to the probable cause standard of the Fourth Amendment of the United States Constitution and the Wiretap Act or FISA probable cause standard? Do you need to have a reasonable belief that an avatar's conduct in the virtual world is going to correlate to a crime being committed in the real world? If a reasonable suspicion standard is followed instead of a reasonable belief standard (due to the arguably reduced privacy in a virtual world because it is a public space), then reasonable suspicion requires specific and articulable facts taken together to form rational inferences from those facts.[166] If a warrant is even necessary to obtain evidence from a virtual world, this standard would be easier to satisfy

---

162 *See* United States v. Puerta, 982 F.2d 1297, 1300 (9th Cir. 1992) (stating the test for probable cause for a warrant).

163 *See supra* Part II.C.

164 *Id.*

165 *See id.*

166 *See* Terry v. Ohio, 392 U.S. 1, 21 (1968) ("[I]n justifying the particular intrusion the police officer must be able to point to specific and articulable facts which, taken together with rational inferences from those facts, reasonably warrant that intrusion.").

because any evidence that an avatar is acting individually or meeting with other avatars to commit a terrorist act could be used to obtain a warrant. Evidence like hosting group meetings in secret locations in the virtual world, speaking a secret language in the virtual world, collecting virtual money, or carrying out terrorist activity within the virtual world itself arguably could be used to form a rational inference that these avatars are organizing to commit or are committing terrorist activities in the real world.

E. Prosecuting Virtual Crimes

1. Elements of a Crime

Criminal activity consists of four elements that must be satisfied beyond a reasonable doubt: (1) prohibited conduct (actus reus); (2) culpable mental state (mens rea); (3) specified attendant circumstances; and (4) a forbidden result or harm.[167] In order for an individual to be prosecuted for a crime, these four elements must be satisfied.

In order to be prosecuted for an activity in the virtual world, the virtual activity must consist of, or involve, conduct that would constitute a crime in the real world. If there are no real world consequences, then the crime is a fantasy crime, which cannot be prosecuted.[168]

Unless the criminal code is modified to accommodate virtual crimes, criminal activity in the virtual world has to satisfy the same four elements as criminal conduct in the real world. First, the actus reus is present when the perpetrator commits an illegal act. This conduct can occur wholly in the real world, wholly in the virtual world, or partially in both worlds.[169] The illegality of the act is what is important, not where the act occurred.[170] Second, the mens rea is present when the perpetrator knew that the illegal conduct was in fact illegal. It is important to note that the mens rea of the perpetra-

---

167 *See generally* Susan W. Brenner, *Is There Such a Thing as "Virtual Crime"?*, 4 CAL. CRIM. L. REV. 1, ¶ 33 (2001), *available at* http://boalt.org/CCLR/v4/v4brenner.htm [hereinafter *Virtual Crime*] ("[W]e define crimes as consisting [of] four elements: prohibited conduct, culpable mental state, specified attendant circumstances and a forbidden result or harm. These elements are the method we use to impose liability for the commission of crimes." (footnote omitted)).

168 *See generally*, Susan W. Brenner, *Fantasy Crime: The Role of Criminal Law in Virtual Worlds*, 11 VAND. J. ENT. & TECH. L. 1, 53–60 (2008) [hereinafter *Fantasy Crime*] (analyzing the propriety of criminalizing fantasy crimes committed in the virtual world).

169 *See Virtual Crime*, *supra* note 167, at ¶ 34.

170 *Id.*

tor will be located in the real world.[171] Third, attendant circumstances will be present when the perpetrator was not legally entitled to engage in the specific conduct at issue.

The element of harm is the most challenging requirement to satisfy because in order for an individual to suffer harm, the virtual conduct must have some real world impact. Real world harm could include financial consequences or emotional consequences. For example, the transfers of money in the real world, the loss of money in the real world, or the destruction of the financial market in the real world are all real world financial consequences. Virtual world conduct that results in real mental pain and suffering for an individual in the real world can also be considered a real world emotional consequence.

There are three types of virtual crimes that have gained some attention in recent years—virtual theft, virtual rape, and virtual harassment. We now discuss examples of each. These examples range in the way they have been handled, and will later be used to suggest how to prosecute virtual money laundering, virtual recruitment and communication, and virtual terrorism.

2. Virtual Theft

Gamers import and export real world money in and out of virtual worlds.[172] This real world money can be used to acquire virtual property,[173] thereby giving virtual property value in the real world. Virtual property can be traded in the real world,[174] and virtual property can also be stolen. Thus, the owner of a virtual perpetrator avatar could be subjected to real world criminal liability for the taking of one's property in the virtual world.

The United States has yet to prosecute a virtual theft; however, such an opportunity arose in 2008 when a user's account in the MMORPG Final Fantasy XI was broken into, and items and currency valued at about $3800 were stolen.[175] The theft occurred to a user liv-

---

171 *Id.* at ¶ 8 (stating that it is not possible to hypothesize difference between real world crimes and cybercrimes pertaining to the element of mental state).

172 *Fantasy Crime*, *supra* note 168, at 65.

173 *Id.* at 70 ("Since the virtual property was purchased with 'real' money, its loss inflicts a harm that resounds in the physical world.").

174 *Id.* In conducting my own investigation, I have discovered that eBay sells Linden Dollars in exchange for United States currency.

175 *See* Earnest Cavalli, *Police Refuse to Aid in Virtual Theft Case*, WIRED (Feb. 4, 2008, 1:25 PM), http://www.wired.com/gamelife/2008/02/police-refuse-t/ ("After the loss of almost $4,000 USD in virtual goods and currency, *Final Fantasy XI* player Geoff Luurs brought his

ing in Blaine, Minnesota, and the local police force found that the user's goods were "devoid of monetary value" and reasoned that no theft had actually occurred.[176] This outcome could have occurred for a variety of reasons. First, it is arguable that the local police force was not familiar with the use of real world money to purchase virtual property.[177] Thus, this virtual theft was not prosecuted, and the wrongdoer went unpunished. Second, it is possible that the amount of money involved in this virtual theft was not enough to prosecute and expend resources on. However, if a well-known company, such as IBM, lost money, then maybe some action by the local police force would have occurred.[178] Either way, the United States is reluctant to consider thefts that occur in the virtual world as crimes.

In contrast, the international community has taken steps to attempt to prosecute and punish users who commit virtual theft. For example, in 2009, a three-year prison sentence was issued to a known gang member for extorting virtual goods.[179] According to Chinese officials, three suspects cornered the victim in a virtual cyber café and noticed he had a particularly large balance of virtual goods in his QQ-Tencent account.[180] A virtual assault ensued and the victim was forced to turn over the equivalent of nearly 100,000 RMB of the virtual currency QQ coins.[181] This case is interesting in that it may show that virtual goods must have value since an arrest and prosecution occurred, and thus could set a precedent in prosecuting virtual theft. In another example, in 2007, the Dutch police force arrested a teenager for stealing nearly $6000 worth of virtual property in the Finland-based MMO Habbo Hotel, but the outcome of this arrest is unclear.[182] In another case in 2005, the Japanese police arrested a Chinese exchange student for stealing virtual property in the Asian

---

case before the Blaine, Minnesota[,] police department only to be refused any kind of aid.").

176 *Id.* (internal quotation marks omitted).

177 *Id.*

178 *Id.*

179 *Four People Sentenced for Virtual Property Theft*, CHINA VIEW (May 24, 2009, 4:41 PM), http://news.xinhuanet.com/english/2009-05/24/content_11427265.htm.

180 *Id.*

181 *Id.*

182 *'Virtual Theft' Leads to Arrest*, BBC NEWS (Nov. 14, 2007, 2:37 PM), http://news.bbc.co.uk/2/hi/technology/7094764.stm; *see also* Wagner James Au, *Why Virtual Theft Should Matter to Real Life Tech Companies*, GIGAOM (Nov. 18, 2007), http://gigaom.com/2007/11/18/why-virtual-theft-should-matter-to-real-life-tech-companies/.

MMORPG, Lineage II, and then reselling it on eBay.[183] Lastly, the South Korean police force has developed a special unit that deals with in-game crimes, which is often inundated with virtual theft reports.[184]

3. Virtual Rape

In order for a perpetrator to be held criminally responsible for rape, there needs to be nonconsensual sexual intercourse with a victim, often through use of physical force.[185] Some critics believe that a rapist in the virtual world may not be prosecuted in the real world because there is no real world harm since an actual person was not raped.[186] However, others claim that the individual behind the avatar being raped can suffer severe trauma that can be similar to what one would experience from actually being raped.[187] In this situation, the harm would be mental instead of physical. However, rape requires a physical assault, placing this criminal conduct solely in the real world and not in the virtual world under our current law.

Nevertheless, "virtual rape", which can occur through text, animation, malicious scripts, or other means instead of by physical force, is a concern of some. In the virtual world LamdaMOO, a text-based multi-user environment,[188] a user, Mr. Bungle, used "voodoo dolls," which are codes represented by objects, to gain control over another user's avatar.[189] Here, voodoo dolls were used by Mr. Bungle to make it appear that other users were participating in explicit, violent sexual acts in an extremely public part of the virtual world, known as the liv-

183 *Student Arrested for Robbing Another Player Inside an Online Game*, INFORMATIONWEEK (Aug. 22, 2005, 2:24 PM), http://www.informationweek.com/news/security/showArticle.jhtml?articleID=169500364.

184 Jeremy Hsu, *Video Game Property Insurance Protects Virtual Goods*, INNOVATIONNEWSDAILY, (July 7, 2011, 12:56 PM), http://www.innovationnewsdaily.com/418-insurance-virtual-items-games.html.

185 18 U.S.C. § 2242 (2006).

186 *Virtual Crime*, *supra* note 167, at ¶ 105.

187 *RCASA's Friday Facts: Avatar Rape in Virtual Reality*, RAPPAHANNOCK COUNCIL AGAINST SEXUAL ASSAULT BLOG (Nov. 5, 2010, 8:00 AM), http://rcasa.wordpress.com/2010/11/05/rcasas-friday-facts-avatar-rape-in-virtual-reality/.

188 Regina Lynn, *Virtual Rape Is Traumatic, but Is It a Crime?*, WIRED (May 4, 2007), http://www.wired.com/culture/lifestyle/commentary/sexdrive/2007/05/sexdrive_0504; *see also* Julian Dibbell, *A Rape in Cyberspace*, VILLAGE VOICE (Oct. 18, 2005), http://www.villagevoice.com/2005-10-18/specials/a-rape-in-cyberspace/.

189 Benjamin Duranske, *Reader Roundtable: "Virtual Rape" Claim Brings Belgian Police to Second Life*, VIRTUALLY BLIND (Apr. 24, 2007), http://virtuallyblind.com/2007/04/24/open-roundtable-allegations-of-virtual-rape-bring-belgian-police-to-second-life/.

ing room.[190] "[T]he victims of Mr. Bungle's [conduct] were shocked and traumatized by how he had manipulated their online characters and by how powerless they had been to stop him."[191] There was a lot of uproar regarding Mr. Bungle's conduct in the virtual world, which resulted in a programmer of LamdaMOO terminating the actual user's existence in this virtual world.[192] Another virtual rape allegation occurred in 2007, which resulted in the Belgium police wanting to patrol Second Life, but it is unclear whether they were given the authority to do so.[193] Neither of these incidents was handled by the real world legal system through the imposition of criminal liability for these activities that occurred in the virtual world.

4. Virtual Harassment

Virtual harassment has become a known problem in MMORPGs and virtual worlds. However, this problem is usually dealt with by the entity that operates the MMORPG or virtual world, typically by suspending offending players or banning them entirely. For example, Second Life allows users to file abuse reports when there is a violation of Linden Lab's Terms of Service or Community Standards.[194] The abuse report is submitted to customer service, and it then takes appropriate action, which ranges from an "official warning to a suspension or permanent termination of the abuser's access to the Second Life world."[195]

5. Application to Virtual Terrorism Conduct

These examples show that there are different classes of virtual crimes, and we have different abilities to prosecute them in the real world. First, there are the virtual world crimes where the harm in the real world can be proven, for example, virtual theft. These types of crimes appear to be the easiest to prosecute in the real world. Like virtual theft, laundering money through the virtual world has real world consequences that can be ascertained. The consequence of laundering money is that one party loses a certain amount of money

190 *Id.*; *see also* Dibbell, *supra* note 188.
191 *Virtual Crime*, *supra* note 167, at ¶ 104.
192 Dibbell, *supra* note 188.
193 Lynn, *supra* note 188.
194 *Linden Lab Official: How to Handle Online Harassment*, SECOND LIFE WIKI, http://community.secondlife.com/t5/English-Knowledge-Base/How-to-deal-with-abuse-and-harassment/ta-p/1339983 (last visited Feb. 20, 2012).
195 *Id.*

while another illegally gains that amount. Therefore, prosecuting terrorists for using virtual worlds to launder money can be prosecuted in the real world.

Second, there are virtual world crimes that have real world consequences but do not necessarily cause the harm that is required under the current United States Criminal Code to amount to a crime, for example virtual rape.[196] Prosecuting virtual terrorist activity, such as communication, recruitment, or collecting virtual weapons, could fall under this category because it would be hard to prove that this conduct in the virtual world would result in harm in the real world. However, if it can be proven that the preparatory conduct actually led to a real world terrorist activity or that the virtual terrorist activity ended up being carried out in the real world, then there is the possibility of prosecuting the user in the real world because the real world harm would be easily ascertained. Therefore, if real world harm is proven, then this virtual world conduct could also fall under the first category.

Finally, there is the category of virtual world crimes that only impact users in the virtual world, for example virtual harassment. Punishing terrorists who use the virtual world to communicate and recruit new terrorists could fall within this category as long as the impact is only felt within the virtual world. If this is so, then punishing users may be better handled by the virtual world itself, by either having the host deactivate the users' accounts temporarily or banishing the users from the virtual world altogether.

F. Who Should Police the Virtual World?

There are at least three different options regarding who should police the virtual world—the virtual world itself, local police, and/or federal authorities. The virtual world can police its users' conduct through User Agreements, "community rules" and "privacy policies," or by holding ISPs responsible for policing user content. First, User Agreements have been used to terminate a user's account if the user has committed an illegal act. The User Agreement can also reference a real world statute through which the offending user can be prosecuted under in the real world. This, for example, has been done in regards to copyright.[197] Second, "community rules" and "privacy poli-

196 *See supra* Part III.E.3.

197 David Assalone, Comment, *Law in the Virtual World: Should the Surreal World of Online Communities Be Brought Back to Earth by Real World Laws?*, 16 VILL. SPORTS & ENT. L.J. 163, 193 (2009) (stating that according to the terms of service agreement, in cases of copy-

cies" can specifically prohibit certain conduct and if a person engages in the prohibited conduct, the virtual world can punish the user. The "community rules" and "privacy polices" can also include mandatory reporting provisions, which mean that other users have a duty to report any illegal conduct that they observe or know about that is taking place in the virtual world. Virtual world operators, such as World of Warcraft's Blizzard Entertainment, try "to foresee vulnerabilities and address them as they become apparent."[198] Third, under § 230 of the Communications Decency Act, which is part of the Telecommunications Act of 1996, an ISP can be held responsible for policing user content. An ISP can restrict access to certain material or give others the technical means to restrict access to that material.[199]

While state laws and local laws could govern conduct in the virtual world for users located in a given region, each region may handle virtual crimes differently, which could result in the unequal punishment among users from different states for the same conduct on the Internet, which is inherently not bound by geopolitical boundaries.

Federal authorities could also police the virtual world. As previously mentioned, the federal government retains the power to ensure that networks are "intercept-capable" and have data retention for a particular period. Additionally, the federal government can also require that the service agreement between Linden Lab and its users be drafted in such a way as to make it easier for the company to monitor and control illegal conduct by its users in the virtual world. For example, the definition of illegal conduct could be expanded to include virtual terrorism and virtual preparatory conduct.

There has been some effort by federal authorities to start looking at ways to monitor virtual worlds, such as World of Warcraft. The United States intelligence community has been trying to develop software that will detect violent extremists infiltrating these multiplayer games.[200] This software is called the "The Reynard Project" and will profile online gaming behavior with the goal of "automatically detecting suspicious behavior and actions in the virtual world."[201] Moreover, some government officials, such as Hillary Clinton, are en-

---

right infringement Second Life adheres to the processes outlined in the Federal Digital Millennium Copyright Act).

198 Thier, *supra* note 146.

199 Communications Decency Act of 1996, 47 U.S.C. § 230 (2006).

200 Ryan Singel, *U.S. Spies Want to Find Terrorists in World of Warcraft*, WIRED: THREAT LEVEL (Feb. 22, 2008, 11:15 AM), http://www.wired.com/threatlevel/2008/02/nations-spies-w/.

201 *Id.*

couraging international cooperation to police the Internet,[202] using "voluntary standards for prosecuting cybercriminals, protecting intellectual property, securing networks, and pursuing terrorists who use cyberspace to plan attacks and woo followers."[203] So steps are being made to address this growing concern about virtual worlds being used to harbor terrorist organizations.

IV. CONCLUSION

Currently, there is no settled method on how to handle the privacy rights of avatars in the virtual world. However, using virtual worlds to carry out terrorist activities, recruit, communicate, and launder money is a growing concern that may require the United States and other countries to either use existing laws or create new legislation that permits the federal government or Internet Service Providers to monitor this type of conduct in the virtual world. Currently, there is existing law that could apply to permit either the government or ISPs to monitor conduct in the virtual world. For example, although the Fourth Amendment reasonable expectation of privacy extends to conduct in the virtual world, it does not extend to conduct that is considered illegal or conduct that falls under a judicially created exception to the Fourth Amendment. Furthermore, the Wiretap Act would protect communication in the virtual world between avatars from government intrusion unless there was an applicable exception, such as the exigent circumstances, consent, or ISP exceptions, which would permit the interception of this communication. Moreover, conduct and communication in the virtual world would fall outside the scope of FISA. However, even if FISA did apply, there are exceptions that could apply, such as when no U.S. person is a party to the communication, which would permit the interception and surveillance of the communication and conduct without a warrant. Additionally, CALEA would apply as long as virtual worlds are considered a provider of wire or electronic communication. Based on the analysis in this Article, virtual worlds would be considered as such.[204] Lastly, information exchanged and conduct engaged in could be monitored or intercepted through NSLs, but as discussed in the Article, this is a contested area of the law that may not be applicable if expanded to virtual worlds. There is some existing federal law that

202 *See U.S. Unveils Global Cyberspace Strategy*, CBS NEWS (May 16, 2011, 10:37 PM), http://www.cbsnews.com/stories/2011/05/16/scitech/main20063445.shtml.

203 *Id.*

204 *See supra* pp. 1056-57.

permits the surveillance of an avatar's conduct in the virtual world under certain circumstances. With that said, virtual worlds, specifically privacy rights in virtual worlds, are not addressed in any of these laws; therefore, a more effective method would be to enact a new law or amend an existing law to include the ability to monitor virtual worlds in order to protect against terrorist organizations using them as breeding grounds for terrorism in the real world.

The issue of prosecuting offending avatars for conduct observed in the virtual world is challenging because attribution may be difficult. Virtual crimes, such as theft, rape, and harassment, have been occurring and still occur in the virtual worlds. Traditional criminal statutes that are relied upon to prosecute a criminal come up short for crimes in the virtual world because there is either no real world harm or the elements necessary to be prosecuted for a crime are not satisfied. This results in virtual wrongdoers going unpunished. This issue could be addressed by tailoring the current criminal statutes to include illegal conduct, such as recruiting, communicating, money laundering, and bombing, done in the virtual worlds by terrorist organizations. The United States, as well as the rest of the world, needs to be prepared when these virtual terrorist acts start to be identified and prosecuted. The ways in which virtual theft, rape, or harassment have been prosecuted can be used as models to help the United States, or the international community as a whole, combat virtual terrorism that results in actual real-world terrorism.

Since developing new laws takes time and effort, the easiest way to permit law enforcement to monitor an avatar's conduct is by including a provision in a privacy statement or terms of service explaining that an individual's conduct in the virtual world is subject to government surveillance and prosecution. Virtual worlds, such as Second Life, have already taken to this, specifically in situations of child pornography. However, these privacy statements or terms of service could be extended to include virtual terrorism.

V. FUTURE WORK

This paper has dealt with the ability to monitor conduct amounting to terrorism in the virtual world through the Fourth Amendment, the Wiretap Act, FISA, CALEA, and NSLs. However, there are a variety of topics that have been left untouched but may have been addressed by earlier authors. One such topic is whether international law and treaties should be applied to the virtual worlds and how foreign governments should handle or have handled illegal conduct that occurs in the virtual world. This is an important topic. Conflicting

laws may result in the wrongdoer engaging in forum shopping and being prosecuted in areas that have tougher laws but avoiding liability in areas with less strict laws. Harmonizing how international laws and treaties are applied will assist in preventing this unwanted outcome. An additional topic that has been left untouched is the role of the free speech rights found in the First Amendment of the United States Constitution, which are implicated by proscribing conduct or speech. It can be argued that this speech is unprotected by the First Amendment because it constitutes fighting words or imminent threats. On the other hand, this speech could be regulated as a time, place, and manner restriction. Another topic of importance is the issue of attribution and making sure the actual wrongdoer is the one being prosecuted and punished. Finally, as mentioned in the Article, another topic that has not been discussed is whether the real world crime of conspiracy is meaningful and applicable in the virtual world.