



SCHOOL VIOLENCE:

L PLAYGROUNDS

VIOLENCE From bullying to cyberstalking to shocking crimes of violence, behaviors in video games are echoing into the classroom.

Sandy Hook. Virginia Tech. Columbine.

These communities are associated with some of the most horrific school shootings our country has witnessed, and reflect the most extreme end of a continuum of school-associated violence and conflict. Online communities, including video games and virtual worlds, have become a focal point of public discourse as we come to grips with the aftermath of these and other school-based tragedies and crimes.

The purpose of this brief is not to propose a connection between violent video games and

acts of violence, but to demonstrate and shed light on how these virtual environments can provide a fertile source of intelligence to school administrators and law enforcement regarding threats and criminal intent that may affect educational environments in the real world.

News media articles chronicle how law enforcement investigators have discovered, sometimes after the fact, the obsessive behavior and online activities of perpetrators of these crimes. On the following pages, we highlight several real-world incidents.







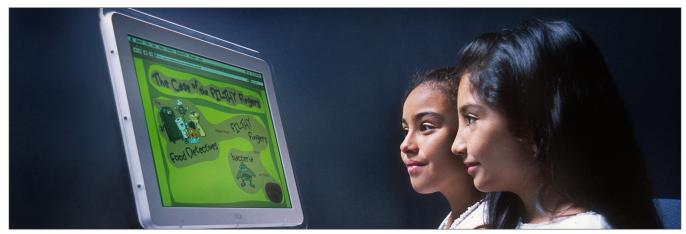
DECEMBER 2013

Following an act of violence, investigators read new meaning into a suspect's online posts in discussion board forums, and may hypothesize a possible connection between the threats made and behaviors exhibited in virtual worlds with the perpetrator's violent act in the real world.

Today, many school resource officers (SROs) and administrators are routinely engaging students about their online interactions and the possible areas of conflict or threats of violence in the same way they have done before for their interactions in the school hallways. In the race to prevent a tragedy, all avenues must be explored, and this policy brief is meant to educate law enforcement personnel, SROs, and school administrators about these digital playgrounds that are playing a larger role in the social lives of students than ever before.

These environments present a new source of conflict for students and, at the same time, a new source of intelligence for those trying to keep them safe. Drakontas LLC and Drexel University have developed this policy brief with funding from the Bureau of Justice Assistance (BJA) at the U.S. Department of Justice as part of a larger program to document and raise awareness regarding the rising incidence of criminal activity within virtual worlds and online gaming communities.

This document is intended to educate law enforcement, SROs, and school administrators about these issues and offer strategies that can be employed to improve school safety. Given the increasing popularity of video games and virtual worlds among school-aged children, coupled with American youths' increasing tendency to cultivate their school experiences with their private lives through social networks and video games, the opportunities for children to use these platforms as conduits to bully, harass, threaten, stalk, and abuse their peers online has increased. The techniques described in this publication offer timely options and suggestions for law enforcement and SROs to consider.

















Hundreds of millions of people – young and old, alike – interact with each other daily in online digital playgrounds. Global revenues for the video game industry reflect this point and are expected to grow from \$67 billion this year to over \$82 billion in 2017. Games like World of Warcraft, Call of Duty, SimCity, and



tens of thousands of other video games offer uniquely crafted entertainment environments that capture the attention of users for hours on any given day. The broad availability of games on smartphones and other handheld electronic devices also ensures a near ubiquity of access for any devoted participant.

A report from the Pew Research Center² highlights the increasing importance and attraction of social media and online communities for children and students in communication with their peers. Consider, for example, the following statistics for this demographic:

- 75% of teens have a cell phone and/or smartphone
- 73% of teens use an online social network site (SNS)
- 37% of SNS users send messages through social networks daily
- 80% of teens have a gaming console
- 51% of teens have a portable gaming device







Two Worlds Collide (Continued)

For many young people, time out of school means time spent online using one or more of these computing and gaming devices so they can keep in touch with and stay connected to their peers around the clock.



Today's virtual worlds and online gaming communities are designed to fuel the need for constant social connections and provide interactive, social features that allow users to communicate with each other and enhance the overall gaming experience. These embedded communications features are built into the software that runs gaming consoles (such as the Microsoft Xbox 360, Sony PlayStation 3, and Nintendo Wii U) and well-known virtual worlds (such as Blizzard Entertainment's World of Warcraft and Riot Games' League of Legends). Examples of these communications options range from text, voice, and video messaging to video game discussion forums, social networking sites, and email.





Drexel

Embedded Communications in Online Games



Virtual worlds and online video games feature different embedded communications options for users who wish to chat or exchange messages (via text, audio, and/or video) and share files. Users can also perform certain financial transactions in these games, either by purchasing virtual goods and services directly from the video game company, or by exchanging them with others in the game using digital currencies or real world funds via credit cards and other platforms. There are also numerous discussion board forums available online for people to discuss various topics relevant to the game or game play, including winning strategies, new software releases, and how to use cheat codes or other game-enhancing technologies. These embedded capabilities offer a wide range of social and economic interaction among players, and, often, players mix together personal information with game-related information. For example, it is not unusual for a young person to post a message in a gaming environment about a relationship breakup, an argument with parents, or some other personal issue, as the environment is often viewed by the player as a safe and comfortable place to express emotions or concerns; however, they can also be used as conduits for abusive and threatening remarks. From this perspective, these communications are a fruitful area of intelligence for educators and school safety professionals regarding emerging threats or conflicts that occur in the school community.

Two Worlds Collide (Continued)



The more common types of criminal behaviors and social harms occurring online among schoolaged children can be categorized as either cyberbullying or cyberthreats:

Cyberbullying: Research indicates that 20% of middle-school students have been affected by cyberbullying.8 Those on the receiving end of this behavior are referred to as victims or targets, while those who witness the behavior are referred to as bystanders. Cyberbullying is a behavior meant to harm someone via verbal means. The bully may use their online presence to attack their victims anonymously through their avatars, or digital personas.

Cyberthreats: Another major type of behavior expressed online are cyberthreats. These can involve direct threats to individuals that may be simple nuisances or not intended as serious, or they may be a valid threat of physical, emotional, or social harm. Regardless of their intention, cyberthreats must be taken seriously in the context in which they are delivered. Some may be made within a virtual world as part of the gameplay, while some are posted outside of a game on a public discussion forum or on a social networking site.

The social aspect of these games – reflected in the embedded communications tools that link players together – keeps users fully immersed in the video game environment by providing social motivation.³ In other words, the games themselves encourage and facilitate peer-topeer interaction. The more time a child spends playing a video game, the more opportunities they have to connect with other gamers and community members. This benefits the videogame creator, as the ever-increasing engagement of and communication among community members through these games can perpetuate the financial success of the game.⁴

The Social Costs and Hidden Dangers of these New Communities

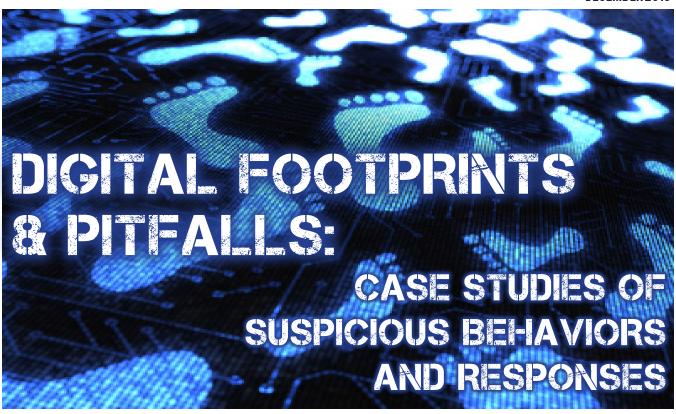
There are resulting social consequences outside the game. Research has demonstrated that youth who do not participate in these communities or use the technology employed by their peers may feel excluded or left out, as the majority of a student's social activity outside of school now occurs online.⁵ There are well-documented examples of students getting into fights over comments made or conflicts and thefts occurring in a virtual world or social network,⁶ even to the point where students have physically assaulted other students.⁷

Daily news headlines highlight the increasing numbers of victims of online crime: social harms, like bullying, intimidation and harassment, and economic harms, like identity theft and fraud. Cyberspace has also provided outlets for users to make threatening comments in video games, chat rooms, or discussion forums about blowing up a school or shooting a fellow student.⁹

The next section offers concrete, real-world examples of how these threats are delivered and the devastating impact they can have on a school community.







To keep children safe in both real-world and online environments, law enforcement and school administrators must become familiar with the virtual worlds and other digital playgrounds in which students spend so much time. Just as we see in the real world, there is a small percentage of individuals in cyberspace with emotional and psychological dysfunctions and malignant tendencies, who vent their frustration and hatred routinely in these communities.

Some of the online postings and messages of these individuals may be idle, non-specific threats. On the other hand, there have been a number of high-profile shootings in which the events required law enforcement to investigate the use of video games and other online communities by the key suspect. These digital footprints and evidence trails can provide law enforcement with valuable intelligence and information regarding the personality and intent of the perpetrator.

For instance, about a week after the Sandy Hook Elementary School shooting in December 2012, a minorin Alaska made a threat online in a video game about his plans to shoot up his school.¹⁰ Another video game player from a different state noticed the threat and told his parents, who reported it to authorities. The authorities deemed it to be credible enough to arrest the suspect and charge him with making a terroristic threat. This example highlights the kind of intelligence collection, analysis, and quick action by law enforcement that results in an added measure of safety for school-aged children in educational environments.

School administrators are also finding themselves increasingly involved in mediating students' online disputes that cross over into the classroom, as digital media usage has become increasingly pervasive among the school community. Take, for example, the case between a 14-year old Georgia girl and two of her peers that involved







Digital Footprints & Pifalls (Continued)

a fake Facebook account.¹¹ The two students purportedly set up a social media profile using distorted pictures and false information to embarrass the girl; after both the school administration and the local police apparently told her they could do nothing due to the fact that the dispute occurred off school grounds and that there was no cyberbullying law in place at the time that they could apply to this case, the victim sued the two students, who were behind the fake Facebook profile, and soon appeared

on CNN as a result of her actions.

Both of these cases highlight the need for collaboration among various stakeholders to resolve online conflicts and disputes before the real-world impacts and ramifications are felt. In the following sections, we discuss some of the reasons that children do not report online conflicts and threats and the ways that school administrators and authorities can engage children in dialogue to resolve disputes and prevent potential threats.

Griefers:

Examples of Cyberbullying Found in Minecraft

Minecraft has become one of the most popular video games in recent years, largely because the game started as an independent, open source project that attracted millions of users with a simple formula: a player gets to build his or her own world, using various tools and resources found in the game by mining for them. The game randomly creates a world filled with different physical features (such as rivers, mountains, animals, etc.) on which a player then can build houses, spaceships, and any number of items.

Many players open accounts on various servers that make the game available for anyone who wishes to join a common virtual environment. Players interact with one another as they build structures and objects within their own "sandbox," and they can travel from location to location and interact with each other using the same server. Players will spend months (literally) building intricate structures, which then become the subject of pride and go on display.



The game's greatest benefit – its openness to multiplayer interaction – also has a significant drawback: players can destroy the work of another. In Minecraft, those kinds of players are referred to as "griefers" because of the grief they cause. 12

Variations on the same theme occur in many popular online games, where a multiplayer framework permits a person to harm the virtual presence of another. Given how seriously young people take these games, it is not surprising that parents have reported fights and even suicide attempts over the loss of objects in virtual worlds.

In other words, some children may think that causing grief in a game like Minecraft is just a bit of fun; in the same way they may think that a sarcastic or cutting remark at school is a harmless joke. However, we have learned that such behaviors often have real ramifications and cause conflict that can escalate and spill over into school hallways and classrooms.







Digital Footprints & Pifalls (Continued)

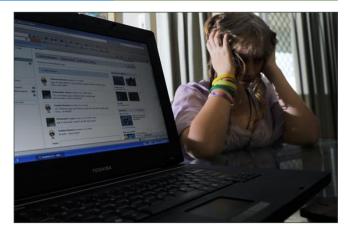
Why Don't Kids Report Online Threats and Behaviors?



For every success story law enforcement experiences in gathering information in time to prevent a violent incident from taking place, there are dozens of examples of threatening behavior that go unreported. Why do some children remain silent when threatening behavior manifests itself, either online or right in front of them during a school day?

A U.S. Secret Service publication sheds light on some of the common characteristics of high-profile shootings and school-based attacks: specifically, the involvement of other students in some fashion of the attack, the behavior of the suspects/attackers prior to the incident that warranted cause for concern, and the knowledge held by other people of the plan of attack.¹³ Sometimes, they fear retaliation or fail to recognize the seriousness of the threat.¹⁴

A recent study of high school students also found that the "dominant attitude toward cyberbullying was indifference, raising alarms about the lack of cyberbullying prevention. Peers, who were the people most teenagers would likely turn to when experiencing cyberbullying, usually took no action because of their tendency to avoid conflicts and to maintain group harmony." 15



There are also concerns among victims and witnesses of being victimized again – after the initial victimization has occurred, children may fear that if they report the incident, the authorities or their parents would not or could not intervene to stop it from occurring again.

What are the strategies that law enforcement and SROs can use to detect cyberbullying and threatening behavior in virtual worlds and online gaming environments and, thereby, increase school safety? The next section talks about the challenges facing the law enforcement community and the successful strategies they can employ to counter this phenomenon.











Given the nature of games and the myriad communication options within them, an automated intelligence collection tool would enhance law enforcement's capacity to intercept or identify threatening exchanges online before an incident is carried out in the real world. However, there are varieties of legal, technical, and consumer privacy hurdles that would have to be overcome first in order to make this a real possibility, and it would also require the active participation and support of the video game industry.

Part of the challenge is that many of today's social activities that take place online in virtual worlds and video games fall outside the regulatory framework that supports the technical capacity for law enforcement surveillance and interception and analysis of archived communications. In response, the FBI¹⁶ in recent years has called for an expansion of the Communications Assistance for Law Enforcement Act (CALEA), which

requires telecommunications providers to produce wiretap-friendly systems, to cover non-traditional telecommunications providers, including virtual worlds and video game platforms that offer Internet protocol chat services, forcing them to design systems that meet the surveillance and interception requests of the law enforcement community.

Online Gaming Communities Policing Themselves

Because the communications channels within video games are most likely not actively monitored by law enforcement, the users of these communities and the companies that manage them are left to police themselves and report anything they may see to authorities.

The process of reporting is complicated by the fact that there is no centralized resource within the video game industry for consumers who run into threatening behavior from fellow gamers. Many of the well-established video game





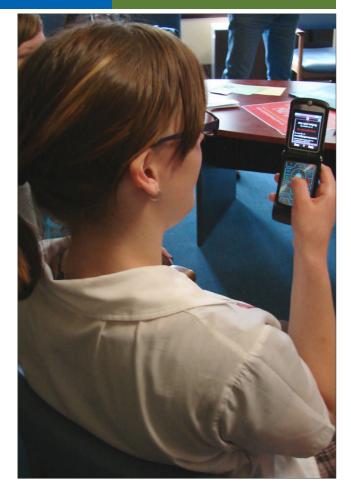


Challenges, Solutions, & Resources (Continued)

companies employ "community managers," whose job it is to oversee behaviors and user exchanges within the game. Oftentimes. community managers become involved in investigations of inappropriate and potentially illegal activity, effectively creating a policing function within the games. Items of concern are elevated to community managers, who, in turn, are responsible for manually analyzing the issue and presenting their findings to upper management depending on the nature of the threat identified. Other companies, meanwhile, use automated processes and realtime computer analyses, in lieu of community managers, to identify threatening language and patterns of interaction within their game brands.

In the absence of technical and legal solutions to combat online threats, awareness about and collaboration on these issues need to be at the forefront of law enforcement and school administration outreach and response efforts, as young people tend to try to "keep the peace" rather than report the issues when they arise. The Mississippi Office of the Attorney General addressed this topic in a recent report and argued that "the most effective school violence prevention programs will result from the collaboration of school board members, administrators, education employees, parents, students, community leaders, emergency response personnel and trained law enforcement liaisons."17

However, for collaboration to work, administrators and students must each share a responsibility to familiarize themselves about the different online environments and digital playgrounds from which violence can originate. They must understand the importance of reporting threats they see that occur in virtual



worlds and online gaming environments to the appropriate authorities. Each step along the way, we should remind everyone that the slogan "If You See Something, Say Something" is not a phrase to be ignored; reporting threatening behavior saves lives and helps to solve crimes, 18 whether it occurs in the real world or virtual world.

We must, therefore, educate and train students about the warning signs and serious nature of threatening messages, and give them viable ways to notify school administrators or SROs about a specific threat they may witness or an abusive incident they may experience online. Conversations about games and behaviors within those games are an essential tool for collecting intelligence about what is going on in the school community.







Challenges, Solutions, & Resources (Continued)

The following page offers a discussion guide that you, as a law enforcement officer, can use with students, parents, and administrators to begin helping them understand the potential impact of virtual worlds and online games in their community.

Law enforcement and the video game industry are also increasingly working together and helping to streamline the investigative and threat response process. Many video game companies publish law enforcement guides that provide information about a game, the types of data the company retains, and the steps law enforcement must take to request this information lawfully from them. As a result of this collaboration, there are examples¹⁹ of law enforcement receiving information from video game companies that have enabled them to arrest individuals suspected of engaging in criminal acts within the gaming environment. However, due to the challenges outlined above, the active engagement of law enforcement, SROs, and school administrators in speaking to children and their parents about this issue still remains a key strategy in detecting brewing conflict within these virtual communities.

How Can Law Enforcement Help?

If you encounter an incident in your school or community and need the help of a video game company, the Internet Crimes Against Children (ICAC)²⁰ task forces located throughout the country are most likely to have relevant contact information for gaming companies and can provide advice on how to proceed. Some gaming companies also make available law enforcement compliance guides, upon request, and list law enforcement points of contact information on their websites.

If You Need to Contact a Video Game Company



Law enforcement can request information through a subpoena or court order during an investigation from video game companies about a specific gamer. Keep in mind that the gaming companies not only will need information about the individual video game user, but also about the individual's account to identify the person in the virtual world. Most of the games allow a user to create a different persona in the virtual world, choosing a unique name or avatar, clothing, physical features, skills, and the like. The company will ask for the individual's "gamer tag," or screen name, as that provides the connection to all of the person's activities and communications within the game. In the event a gaming company cannot assist with a law enforcement inquiry, the resources listed on the following page can be used to report inappropriate behavior.











Law enforcement, SROs, and school administrators should establish a dialogue with students to better understand their use of online video games, virtual worlds, and social networks and what they may see in these environments. Helpful questions include:

- Do you play video games or in virtual worlds? Do you use social networking sites?
- What kinds of games do you play? Role-playing games? Shooter games? Do you play any multiplayer games? Which ones?
- How many hours a week do you play? Do you play at night? During the day?
- Do you talk to people about the games you play? Do you play with friends at their houses (or do they come over to your house to play)?
- Do you talk to your friends or strangers within these games?
- Have you ever seen or heard anything offensive or have you felt threatened while playing a video game online?
- Have you ever reported what you saw or heard to anyone? If you did not report it, why not? If you did report it, how did you report it and what was the outcome?

As part of the dialogue and information collection process and to help mitigate the chances a child falls victim to threats online, school administrators and SROs can educate parents about several preventive measures. Among these include:

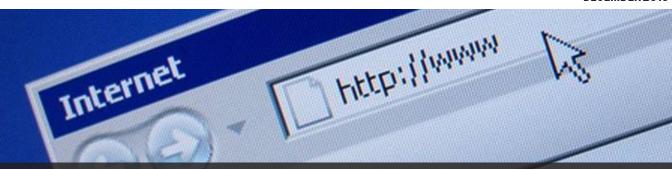
- Understanding the types of applications, video games, and social networks children are using to learn their privacy settings, communications options, and parental control features.
- Limiting a child's social media profile.
- Only allowing children to use virtual worlds that allow for chat/instant messaging to be turned off or set to system-defined phrases.

By educating children and parents about the dangers and risks these online environments can pose to their safety, the likelihood of them being victimized may be reduced.









Below is a partial list of resources that are available to learn more about and report suspicious or threatening online activities:

Reporting Resources

- CyberTipline (http://www.missingkids.com/CyberTipline) is a resource operated by the National Center for Missing & Exploited Children, in partnership with the FBI, ICE, U.S. Postal Inspection Service, U.S. Secret Service, ICAC Task Force Program, and other agencies, that receives leads and tips regarding suspected crimes of sexual exploitation committed against children. More than 1.9 million reports of suspected child sexual exploitation have been made to the CyberTipline between 1998 and June 2013.
- GetNetWise (http://kids.getnetwise.org) is a resource that provides information for parents on online safety, safe websites for children, and links to report criminal behaviors their children may experience, from sexual solicitation and luring to cyberstalking.
- Internet Crime Complaint Center (IC3) (http://www.ic3.gov) is a federal resource from the FBI and the National White Collar Crime Center (NW3C) that provides a centralized means for victims of online crime to report incidents and for law enforcement to search reported events and identify patterns across the Internet.
- School Reach.com (http://www.schoolreach.com) is a system that allows parents to receive notifications from schools via their smart phone. It also manages the CyberBully Hotline (http://www.cyberbullyhotline.com), an anonymous two-way reporting system for administrators, students, and parents.

Educational Resources

- International Association of Chiefs of Police (IACP) (http://www.theiacp.org) is a professional organization that has a variety of online educational resources that address cyberbullying, school violence, and safety issues.
- Internet Keep Safe Coalition (http://www.ikeepsafe.org) is an international nonprofit alliance of
 more than 100 organizations and individuals that tracks global trends and issues surrounding
 digitally connected products and their affect on children. Additionally they assist K-12
 organizations in the development of materials related to online and digital product safety.
- National Crime Prevention Council (NCPC) (http://www.ncpc.org) is a federal resource that provides crime-prevention strategies, including online/Internet safety best practices, for use in communities and schools.
- National Law Enforcement and Corrections Technology Center (NLECTC) (http://www.justnet.org) provides educational and training resources for law enforcement on school safety issues. Their latest publication, entitled "Sharing Ideas and Resources to keep Our Nation's Schools Safe," is available at https://justnet.org/pdf/SharingResources 508.pdf.
- WiredSafety (http://www.wiredsafety.org) is an online safety organization that provides education, awareness, and training on Internet safety, privacy, and security-related issues. They also provide victim assistance for those impacted by cybercrimes and harassment, as well as training and advice for law enforcement professionals on preventing, identifying, and investigating cybercrimes.









As children spend more of their time online in virtual worlds and video game communities, there is an urgent need for the law enforcement community to understand how these environments are being used by children and to educate them about the numerous resources available should they fall victim to or observe suspicious or threatening behaviors online. Moreover, law enforcement needs to encourage children to report anything they see or experience that makes them uncomfortable or that



concerns them, no matter how innocuous it may seem, before people get hurt and it makes front-page headlines. Authorities, working closely with parents, should establish a dialogue with a student or child to help overcome some of the resistance and reluctance they may have to report an online crime or threat and be clear about the process and what will happen after an incident is reported.

Moreover, it is equally important for the law enforcement community to be proactive and vigilant in educating themselves about the types of activities occurring online in these social and entertainment communities and how they can assist children in making sure they navigate these virtual playgrounds safely. Despite the numerous technical, legal, and policy hurdles they presently face, law enforcement can play an active role in working with the public and the video game companies to confront online crime before it crosses over into the real world and claims more school-aged victims.







CONTRIBUTORS:

Dr. Brian Regli, Drakontas LLC Michael Mitkus, Drakontas LLC

Dr. Robert D'Ovidio, Drexel University

Disclaimer

This project was supported by Grant No. 2009-D2-BX-K005 awarded by the Bureau of Justice Assistance. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the Office for Victims of Crime, and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. Points of view or opinions in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

CONTACT INFORMATION:

Drakontas LLC 200 Federal Street, Suite 300 Camden, New Jersey 08103 (215) 887-5570 training@drakontas.com

Drakontas (www.drakontas.com) develops mobile collaboration software and provides training and technical assistance that increase the safety and operational capacity of law enforcement, emergency response, and security personnel. The company was founded in partnership with Drexel University in 2004 to transition technologies developed at the Applied Communications and Information Networking (ACIN) Center for the Department of Defense to commercial, civilian, and homeland security uses.

ENDNOTES:

- Gaudioso, John (2012), "New Reports Forecast Global Video Game Industry Will Reach \$82 Billion by 2017."
- ² Lenhart, A., et al. (2010), "Social Media & Mobile Internet Use Among Teens and Young Adults."
- Nacke, Lennart and Lindley, C. (2008), "Affective Ludology, Flow and Immersion in a First-Person Shooter: Measurement of Player Experience."
- 4 Rodrigues, Lia Carrari and P. Mustaro (2008), "Social Network Analysis of Virtual Communities in Online Games."
- Olson, Cheryl (2010), "Children's Motivations for Video Game Play in the Context of Normal Development."
- KCRG.com (2012), "Online Comments Lead to High School Fight." Retrieved from http://www.kcrg. com/news/local/Online-Comments-Lead-to-High-School-Fight-138840644.html
- BBC News (2005), "'Game theff' led to Fatal Attack." Retrieved from http://news.bbc.co.uk/2/ hi/technology/4397159.stm
- 8 Hoffman, Jan (2010), "Online Bullies Pull Schools Into the Fray," New York Times.
- Ross, Eli (2012), "Online Threat Leads to Oxford Teen's Arrest," ABC24.
- Anderson, Ben (2012), "Anchorage student arrested after alleged shooting threat."

- http://arstechnica.com/business/2012/04/teensues-over-facebook-bullying/
- http://news.jrn.msu.edu/bullying/2012/02/15/ video-game-griefers/
- ¹³ U.S. Secret Service (2008), "Prior Knowledge of Potential School-based Violence."
- ¹⁴ Langman, Peter, Ph.D. (2012), "School Shootings: The Warning Signs."
- Huang, Yun-yin and C. Chien (2010), "An analysis of multiple factors of cyberbullying among junior high school students in Taiwan," Computers in Human Behavior, Volume 26, p. 1589.
- http://news.cnet.com/8301-1009_3-57428067-83/ fbi-we-need-wiretap-ready-web-sites-now/
- Mississippi Office of the Attorney General (2006),"School Violence Prevention Guide," pg. 2.
- Department of Homeland Security, "If You See Something, Say Something" Public Service Announcements.
- ¹⁹ Munsey, Patrick (2009), "Long arm of law reaches into World of Warcraft." Retrieved from http:// kokomoperspective.com/news/local_news/ article_15a0a546-f574-11de-ab22-001cc4c03286.html
- 20 https://www.icactaskforce.org





