Are We Protecting Our Youth Online? An Examination of Programs Keeping Youth Safe and Analysis of Policy Vacuum

Catherine Marcum[1]
Georgia Southern University, USA

Abstract

Gibson's (1984) cyberspace did not become a popular facet in American homes until the 1990s, so in the grand scheme of technology, the Internet is still considered to be in its adolescence. However, despite its young age, approximately 87% of American youth use the Internet on a regular basis (Raine, 2006). While these youth are spending substantial amounts of time online, many of them are becoming victims of criminal activity. The range of crimes committed online, otherwise known as cyber crimes, is quite substantial; however, the particular focus of this study is to examine the preventative programs and policies developed to curb the online victimization of youth (i.e., sexual solicitation, unwanted harassment, and unwanted exposure to sexual material). While several attempts at passing legislation have been unsuccessful, a few attempts by the federal government to protect America's youth have been successfully implemented and will be reviewed. While there are only few evaluations of strategies to prevent online victimization of youth to examine, suggestions of strategies that could be applied to cyberspace based on situational-based crime prevention strategy evaluations of other parallel programs in different arenas are discussed.

Introduction

William Gibson (1984) predicted in his novel, "Neuromancer," that society's increasing fascination and dependence on computer technology would create a completely electronic world he termed "cyberspace." Cyberspace would be composed of millions of different outlets of information that were easily accessible at the click of a button. Gibson also accurately predicted that his new concept would contain dangerous channels leading to sources of vulgarity, criminal activity, and a dangerous hidden world of exploitation.

The range of crimes committed online, otherwise known as cyber crimes, is quite substantial; however, the particular focus of this study is to examine the preventative programs and policies developed to curb the online victimization of youth (i.e., sexual solicitation, unwanted harassment, and unwanted exposure to sexual material). Gibson's (1984) cyberspace did not become a popular facet in American homes until the 1990s, so in the grand scheme of technology, the Internet is still considered to be in its adolescence. However, even though its young age, approximately 87% of American youth use the

[1] Assistant Professor, Georgia Southern University, Department of Political Science, PO Box 8101Statesboro, GA 30460. United States of America. Email: cmarcum@georgiasouthern.edu

Internet on a regular basis (Rainie, 2006). Based on the youthfulness of this new arena of communication and information, preventative programs, legislation, and technology to protect these youth from unwanted harassment and victimization while using the Internet are still in their infancy. The tools that have been developed and utilized as a protection device have been formed under the premonition that reducing the opportunity of online predators to victimize youth will in turn deter them from committing the crime.

Examinations of these policies and programs results in a disappointing finding that methodologically rigorous evaluations to test effectiveness of these protective measures are rare; therefore, it is difficult to confidently preach the effectiveness of any the programs. Since new computer technology is constantly changing, as well as methods to criminally violate the technology, it is difficult to keep preventative measures updated and effective. Possibly best quoted by Frank Andreano (1999) "…dealing with computer crime and the protection of information based technologies is much like the weather in Chicago; wait a few minutes and it is bound to change" (as cited in Lewis, 2004, pp. 1359).

This article will briefly examine the origins of the Internet and how it became a commonality in American households. While several attempts at passing legislation have been unsuccessful, a few attempts by the federal government to protect America's youth have been successfully implemented and will be reviewed. Next, the theoretical basis from which these current prevention programs and policies were developed will be examined. Only a few evaluations of strategies to prevent online victimization of youth are available for examination; therefore, suggestions of situational-based crime prevention strategies that could be applied to cyberspace, based on empirical evidence supporting these types of crime prevention programs, will also be discussed.

Part I. Investigating Cyberspace and Preventive Issues

Origin of the Internet

The first recorded notes birthing the idea of the global information system now known as the Internet were written in 1962 by J.C.R. Licklider of the Massachusetts Institute of Technology (Licklider & Clark, 1962, as cited in Leiner et al., 2003). His "Galactic Network" idea entailed an internationally connected set of computers that allowed for easy accessibility to information. While working at the Defense Advanced Research Projects Agency (DARPA), Licklider's co-worker Lawrence Roberts (1967) published his idea for "ARPANET" while working with DARPA. ARPANET quickly evolved into what is now known as the Internet. A new version of protocol called Transmission Control Protocol/Internet Protocol (TCP/IP) was developed and the general public increased its growing demand for computers. By the 1980s, more vendors were incorporating TCP/IP into their products, because of the increased use of networking by businesses and service providers. This in turn heightened interest among private Internet users (Leiner et al., 2003).

With this amplified popularity for technology, the Internet experienced the perfect environment to thrive, and soon began to do so. The goal of the Internet, originating with ARPANET, was to become a collection of communities that provided useful information to its users. By the early 1990s, use of the Internet became a familiar facet in businesses and homes, and by the year 2001, 75% of the United States population was avid users of the Internet (Sanger, Long, Ritzman, Stofter, & Davis, 2004). Today's Internet

now allows us to shop, make travel arrangements, buy stocks, and most importantly, communicate.

The medium of communication on the Internet, often referred to collectively as social technology (Lamb & Johnson, 2006), has enabled people of all ages (especially youth) to expand their social circles and improve their ability to communicate with friends and family in an inexpensive manner (Roberts, Foeher, Rideout, & Brodie, 1999). Social technology refers generally to computer-mediated communication (CMC) devices that connect people for personal and professional information sharing. The use of CMC methods allows for ease in the workplace, educational setting, or home to communicate effortlessly with others (Simon, 2006). However, since the Internet had become a familiar face in American homes, much like any useful commodity, the beginnings of its corruption started to emerge. Adult users began to prey on younger users in chat rooms, as well as via email and instant messenger. Soon, most Internet users were unable to be online without receiving some type of vulgar email or unwanted approach by a stranger (Mitchell, K., Finkelhor, D. & Wolak, J., 2003; O'Connell, R., Barrow, C., & Sange, S., 2002; Sanger et al., 2004; Wolak, J., Mitchell, K.J., & Finkelhor, D., 2004; Wolak, J., Mitchell, K., & Finkelhor, D., 2006). At that time, protective policies and programs began to emerge as a manner of attempting to protect youth online.

Protective Measures

The federal government has made numerous attempts at passing legislation and instituting protective programs to prevent online victimization of youth. In the mid-1990s, Senator Orrin Hatch authored United States Senate Bill 1237, later known as "The Child Pornography Prevention Act (CPPA) of 1996." The bill amended the definition of child pornography to include the photography, filming, and videoing of sexually explicit conduct of real minor children, as well as digitally-created images of a child involved in pornography. With this amendment, a person could be charged with possession of computer-generated child pornography (Henderson, 2005; Kendall, 1998; McCabe, 2000).

The constitutionality of the CPPA quickly was challenged. In *United States v. Hilton* (1998), the defendant asked that charges of possession of child pornography violating the CPPA be dismissed. Hilton stated that the statute prohibited constitutionally protected speech by banning adult pornography, and that the language in the statute was vague and overbroad. Although the United States Supreme Court found his first claim to be unmeritorious, it did rule that the language of the CPPA was vague and did not clarify the prohibited conduct.

The constitutionality of the CPPA was again challenged by a group of plaintiffs known as the Free Speech Coalition. The United States District Court of the Northern District of California, in *The Free Speech Coalition v. Reno* (1997), ruled that because the CPPA does not require advanced approval for the production of adult pornography that does not include minors, nor does it entail a complete ban on constitutionally protected material, it is not a violation of the First Amendment. However, in 1999 the Court of Appeals for the Ninth Circuit reversed the district court's ruling on the Act. It ruled that the First Amendment does not allow Congress to pass a statute that criminalizes the mere generation of an image, because an actual human being was not involved (Mota, 2002). In 2002, the United States Supreme Court held that since actual children were not used in

the photographs and videos in question, these productions were protected by the First Amendment (Henderson, 2005).

The "Communications Decency Act" (CDA), a part of the "Telecommunications Act of 1996," was enacted to limit the exposure of children to sexually explicit pictures available online (Mota, 2002). Under this Act, any person who knowingly creates, solicits or transmits images to a minor under the age of 18 could be penalized by imprisonment for up to two years and/or a fine of $250,000 per offense. However, on June 26, 1997, the United States Supreme Court decided that the CDA's "indecent transmission" specification violated the First Amendment's guarantee of free speech. Telephone companies and Internet providers were declared not liable for indecency that was beyond their control. In response to the dismissal of the CDA, Congress then passed the "Child Online Protection Act" (COPA) (Henderson, 2005; Hunter, 2000; Mota, 2002).

COPA used contemporary standards based on a test developed in *Miller v. California* (1973). The *Miller* test contains three components that are used to determine if speech is obscene: 1) whether the average person would contend that the material contains prurient value; 2) whether the work depicts sexual acts or excretory functions in an offensive way; and 3) whether the material lacks serious artistic, literary or political value (Virginia Tech, 1997). COPA applied only to material put on the Internet and made for commercial purposes, and it restricted only the documentation harmful to minors. Under this Act, any accused persons must have knowledge of the content of the material, and the material must meet the standard of appealing to the prurient interest of an average person. A violation was classified as a misdemeanor, with the punishment of six months in jail and a $50,000 fine for each violation. The Attorney General also was authorized to collect $50,000 in civil penalties. However, in 2004, the United States Supreme Court ruled in *Ashcroft v. American Civil Liberties Union* (2002) that once again, the tenets of the Act were in violation of the First Amendment (Henderson, 2005; Hunter, 2000; Mota, 2002).

All of above-referenced acts were overturned on the basis of unconstitutionality. Recently, the government has had more success in passing legislation with the objective of protecting adolescents from victimization online in schools, as well as proactive law enforcement efforts to reduce victimization. The Children's Internet Protection Act (CIPA), enacted by Congress in December 2000, addressed access to offensive Internet material on school and library computers. Certain requirements of CIPA were imposed on schools and libraries receiving federal funding for Internet access under the E-rate program; if these regulations were not followed, the E-rate funding could be removed. The CIPA regulations basically required filtering and blocking software, as well as other safety measures, to protect children from accessing obscene and harmful material (Federal Communications Commission, 2006). Building on the concept of CIPA, the Deleting Online Predators Act (DOPA) was introduced to the House of Representatives in spring 2005. DOPA intensifies the regulations of CIPA, as it would require schools and libraries to completely restrict children's access to all Internet sites through which strangers can contact them (Fitzpatrick, 2006). Currently, it has passed the House of Representatives by roll call vote and is awaiting Senate approval.

Besides actual legislation, the federal government has developed various programs to assist law enforcement and parents with the protection of children online. The Internet Crimes against Children (ICAC) Task Force Program, created by the Office of Juvenile Justice and Delinquency Prevention (OJJDP) in 1998, was developed to help state and

local law enforcement construct programs to respond to crimes of online enticement and child pornography. One of the more successful programs, CyberTipline and CyberTipline II (CyberTipline's later enhancement), allows for citizens to report suspicious activity on the Internet, as well as submit unwanted photographs or videos sent to them electronically. In March 2001, the ICAC Task Force reported that because of these citizen reports, more than 550 individuals had been arrested for child sexual exploitation, and 627 search warrants had been served (Medaris & Girouard, 2002).

Also in 1998, the Cyber Division was developed by the Federal Bureau of Investigation to solely investigate computer crimes, such as intellectual property theft and computer security breaches. The Internet Crime Complaint Center (IC3), located in the Cyber Division, received over 200,000 complaints of Internet crimes, 103,509 of which were referred for investigation. However, the Cyber Division also has jurisdiction over crimes involving online child pornography under the Innocent Images National Initiative (IINI). Between 1996 and 2003, 9,366 cases were opened by the IINI, which resulted in 2,569 convictions (Bazelon, Choi, & Conaty, 2006).

In May 2006, Attorney General Alberto Gonzales announced the implementation of Project Safe Childhood, a program designed by the Department of Justice to protect children from online abuse. Gonzales encouraged United States Attorneys across the nation to partner with the ICAC task forces and law enforcement officials to develop educational programs that raise awareness of the dangers of online predators and child pornographers. The goal of the program is to increase public awareness and education of Internet dangers so that residents can protect themselves (United States Department of Justice, 2006).

Part II. Internet and Theories of Crime

Society and its activity patterns are in a constant state of transformation (Madriz, 1996), especially with the development of new technology. For example, the daily and routine activities of children have evolved from bicycles and dolls to video games and the Internet. Raine (2006) reported that 87% of youth currently are using the Internet, and that number likely will continue to grow. However, as innovative technologies emerge, new methods of victimization also accompany these developments (Mitchell, K., Finkelhor, D. & Wolak, J., 2003; O'Connell, R., Barrow, C., & Sange, S., 2002; Sanger et al., 2004; Wolak, J., Mitchell, K.J., & Finkelhor, D., 2004; Wolak, J., Mitchell, K., & Finkelhor, D., 2006).

Early tests of Routine Activities Theory, which often is used to examine different types of victimization, focused on the importance of the environment as a vital component of interaction between criminal offenders and victims (Cohen & Felson, 1979). This is particularly relevant to the current research, as the environment, cyberspace, is a necessary factor that must be present in order to both participate in online activities and become a victim of harassment or other online crime. Cyberspace, which thrives on the possibilities of the unknown, also provides the opportunity for engaging in activities without the presence of a capable guardian. This is true for both the offender and victim, as both parties potentially can participate in deviant behaviors without guardianship being present (Beebe, T., Asche, S., Harrison, P, & Quinlan, K., 1998; Danet, 1998; Jones, 1999). According to Felson (1987), a lack of behavioral controls encourages willingness to participate in criminal activity, and motivated offenders will

place themselves in areas that have an abundance of suitable targets. For example, youth-oriented chat rooms, instant messaging services, and social networking web sites provide a plethora of opportunities for motivated adult predators. As stated by Felson (1987), it is comparable to "how lion look for deer near their watering hole" (p. 912).

Roncek and Maier (1991) suggested that Routine Activities Theory is excellent for use in the examination of predatory or exploitative crimes, which is precisely the type of deviant behavior examined in this article. From the initial assertions of Cohen and Felson, and in conjunction with the works of various other scholars, the currently recognized Routine Activities Theory has been formed. This theory states that there are three components necessary in a situation in order for a crime to occur: a suitable target, a lack of a capable guardian, and a motivated offender (Cohen & Cantor, 1980; Cohen & Felson, 1979; Cohen & Felson, 1981; Felson, 1986; Felson, 1987; Hawdon, 1996; Lasley, 1989; Sampson & Wooldredge, 1987). Moreover, crime is not a random occurrence, but rather follows regular patterns that require these three components.

According to Meier and Miethe (1993), target suitability is based on a person's availability as a victim, as well as his or her attractiveness to the offender. A person who is available for victimization is someone who has not taken certain precautions to protect oneself, such as using blocking software to protect against receipt of unwanted material. The second component necessary for a crime to occur, according to Cohen and Felson (1979), is a lack of capable guardianship. Guardianship is the ability of persons and objects to prevent a crime from occurring (Garofalo & Clark, 1992; Meier & Miethe, 1993; Tseloni, T., Wittebrood, K., Farrell, G., & Pease, K., 2004). The monitoring of a parent or tracking software while a child is using the Internet would be guardianship against victimization. The final component, a motivated offender, is a person who is willing to commit a crime when opportunities are presented through the presence and absence of the other two components (Cohen & Felson, 1979; Mustaine & Tewksbury, 2002). In other words, the theory asserts that if a motivated offender is presented with a suitable target that is not properly guarded against victimization, a crime is likely to occur. For example, a youth providing identifying information to an online predator which would allow for his or her easy location would increase the motivation of the offender to find the youth.

Routine Activities Theory has gained a sizable amount of empirical support in regards to the investigation of illegal behaviors on the macro-level (Cao & Maume, 1993; Cook, 1987; LaGrange, 1999; Roncek & Bell, 1981; Roncek & Maier, 1991; Sampson, 1987; Tseloni, Wittebrod, Farrell, & Pease, 2004), as well as the micro-level, such as property and property crimes (Arnold et al., 2005; Cohen & Cantor, 1980; Cohen et al., 1981; Collins, Cox, & Langan, 1987; Gaetz, 2004; LaGrange, 1994; Lasley, 1989; Lynch, 1987; Moriarty & Williams, 1996; Mustaine & Tewksbury, 1999; Spano & Nagy, 2005; Tewksbury & Mustaine, 2000; Woolredge et al., 1992) and domain-specific models (Ehrhardt-Mustaine & Tewksbury, 1997; Garofalo, Siegel, & Laub, 1987; Lynch, 1987; Madriz, 1996; Wooldredge et al., 1992). Although there have not been any recorded applications of Routine Activities Theory to the online victimization of youth to support its use in cyberspace, the support it has received from other studies would indicate the components could be paralleled in cyberspace to prevent victimization of youth.

Part III. Strategies to prevent online victimization

Very few empirical examinations have been performed on any type of measures instituted to prevent online victimization of youth. Of the few studies that have evaluated these measures, the tenets of the program are mirrored from the components of Routine Activities Theory. Strategies such as proactive measures and filtering and blocking software programs, which will be examined below, have been shown to have some effect on online victimization.

Proactive Measures

Proactive investigations are considered advantageous in several ways, including increasing public safety, economically feasible, and increasing potential of apprehend offenders before harm is caused to innocent children (Girodo, Deck, & Morrison, 2002). This type of investigation makes up at least one-fourth of all investigations of Internet sex crimes against minors and therefore makes a significant contribution to arrests (Mitchell, Wolak, & Finkelhor, 2005). The elimination of the motivated offender through the arrest of offenders reduces the victimization of youth.

A study by Mitchell et al. (2005) utilized data from the National Juvenile Online Victimization Study (NJOVS) to examine the effectiveness of proactive investigations of adults sexually exploiting juveniles on the Internet through child pornography or sexual solicitation. A national sample of state, county, and local law enforcement agencies were surveyed by mail regarding arrests made for these crimes between July 1, 2000 and June 30, 2001. For this particular study, a sub-sample of 644 arrests was examined in which offenders were arrested during proactive investigations on the Internet (Mitchell et al., 2005).

The findings from the analysis of the NVOJS were indicative that proactive investigations were worthwhile for law enforcement. Charges filed against those in proactive investigations varied from an attempted crime, Internet-specific crime, or some form of inducement. Over 90% of arrestees were charged with at least one felony and 91% resulted in guilty pleas. According to Mitchell et al. (2005), this intervention by law enforcement protected many children from the potential of molestation. Second, this active presence of undercover investigators may serve as a deterrent for others who maybe be contemplating the offense.

Filtering and Blocking Software

Many of the statutes passed to criminalize certain materials and activities deemed harmful to minors have been challenged and overturned based on the restriction of free speech provided for in the First Amendment. Courts often have suggested the use of filtering and blocking software as an alternative to legislation, which are assumed to be equally effective, but less restrictive (Volokh, 1997). According to Routine Activities Theory, this capable guardian would monitor and protect children during the use of the Internet, especially when the parent is unable to do so. The Clinton administration also endorsed the use of software, stating that it would do a better job of protecting children from harm on the Internet than any statute (Clinton, 1997). Further federal support came from the chairman of the Federal Communications Commission, William Kennard (1999), who compared the unchaperoned use of the Internet to allowing a child to explore a large city without assistance. Former Vice President Gore (1999) also put forth filtering software as the best tool parents could use to protect their children.

Filtering and blocking software potentially can serve two functions: 1) filtering the receipt of messages, text, or pictures containing certain language, and 2) blocking access to certain sites. According to The Guide (2001), these functions can be further characterized into five different types of software for filtering and blocking certain materials: time-limiting, filtering and blocking, outgoing content blocking, kid-oriented search engines, and monitoring tool. Most family-based Internet safety recommendations endorse the use of filtering and blocking software. However, regulatory advocates have produced studies noting limitations with their use. A study by *Consumer Reports* evaluated six of the mainstream filtering programs and found that all but one, America Online Young Teen Control, blocked at most 20% of sites containing restricted material ("Digital chaperones for kids," 2001). Furthermore, the six programs also blocked a wide range of legitimate content.

Hunter (2000) tested the effectiveness of four popular filtering and blocking software programs: CYBERsitter, Cyber Patrol, Net Nanny, and Surf Watch. He tested the abilities of the programs to block objectionable material, as well as permit non-objectionable material. A website was ranked objectionable or non-objectionable based on its Recreational Software Advisory Council Internet (RSACi) rating, which has five levels of severity based on the content of language, nudity, sex and violence on the website. Websites with a score of two to five were deemed objectionable, and anything below a score of two was non-objectionable. Hunter used three different samples to evaluate the software. The first sample was a set of 50 randomly selected web sites; the second sample was composed of web sites found from a set of 50 popular search terms (i.e., MP3, sex, and Yahoo); and the third sample entailed 100 purposively selected web sites (Hunter, 2000).

Of the four software programs, CYBERsitter was found to do the best job of blocking objectionable material (69%), with Cyber Patrol coming in second with 56% blockage. Surf Watch only blocked 44% of the objectionable material, compared to the 95% blockage claimed in its advertising literature. Finally, Net Nanny did the worst job of blocking material, with only 17% blockage. In regards to blockage of non-objectionable material, CYBERsitter blocked the highest amount with 15%. The other three software packages blocked an average of 6% (Hunter, 2000).

Part IV. Recommendations and Conclusions

Proactive measures serve as a means to curb the activities of the motivated offender (Girodo, Deck, & Morrison, 2002; Mitchell, Wolak, & Finkelhor, 2005). Filtering and blocking software not only serves as a block for motivated offenders, but also as a guardian against victimization (Clinton, 1997; Hunter, 2000; Volokh, 1997). In combination with the other components, these measures decrease target suitability. However, there is still a need for further programs and measures to protect against online victimization and new ideas could come an effective protective measure already in use in the physical world: *target hardening*.

Target Hardening in Cyberspace

Despite the various types of legislation and programs developed to protect children against online victimization, there are only a few scientific evaluations of these programs and policies to determine if they are truly effective. Based on this, it would not be unwise

to examine other types of preventative measures that have been successful in other places and expect them to be successful online.

Situational, or place-based, crime prevention strategies are successful with the same means as hot spot police patrols: they are used when and where they are most needed. Rather than attempting to alter the behavior of the offender, the purpose of situational crime prevention strategies is to block the opportunity of commit criminal behavior in a specific place. According to Eck (2002), place-based tactics could be more influential than offender-based plans because it pays closer attention to immediate situations rather than preparing a person for an uncertain period of time in the future. Referred to as place improvement-processes (Brantingham & Brantingham, 1995), these types of plans are known for reducing crime by reducing the attractiveness of committing a crime in certain areas (Barclay, Buckley, Brantingham, Brantingham, & Whin-Yates, 1996; Brantingham & Brantingham, 1998).

A particular type of situational crime prevention strategy that has been shown to be effective is target hardening, which is providing locks and improved security to access points. In regards to a crime in a physical location, burglary rates have reduced because of target hardening strategies (Bowers, Johnson, & Hirschfield, 2004). This type of strategy could be considered a secondary and tertiary prevention strategy (Pease, 2002) because of its aim to block those at high risk of committing an offense, as well as those who have a criminal history of burglary offenses.

The particular place of this study, cyberspace, is definitely in need of an effective crime prevention strategy. Target hardening in cyberspace could be the security measure needed to protect youth while using the Internet. Situational crime prevention measures that utilize target hardening have an effect of deterring potential offenders away from criminal activity because it tightens security of the particular place (Brantingham & Brantingham, 2005). For example, if a homeowner desires to increase security in his home, he may choose to install an extra lock on all the doors into the home. Increased use of digital locks, such as passwords and controls set by parent or guardian figures, is a potential protective measure that would increase security in cyberspace. Not only would these locks keep motivated offenders out of certain areas used by youth, it would provide a guardianship component to restrict youth from accessing areas inappropriate for their viewing (i.e., adult pornography sites). Content rating sites, such as SafeSurf, allow parents to set passwords and levels for their children during Internet use (Joseph, 2007).

Conclusion

The threat of online victimization for youth has shown to be present and increasing as new technologies emerge on the Internet (Mitchell, K., Finkelhor, D. & Wolak, J., 2003; O'Connell, R., Barrow, C., & Sange, S., 2002; Sanger et al., 2004; Wolak, J., Mitchell, K.J., & Finkelhor, D., 2004; Wolak, J., Mitchell, K., & Finkelhor, D., 2006). The federal government, as well as private organizations, has attempted to decrease the problem with various programs and legislation (Bazelon, Choi, & Conaty, 2006; Clinton, 1997; Girodo, Deck, & Morrison, 2002; Henderson, 2005; Hunter, 2000; Mitchell, Wolak, & Finkelhor, 2005; Mota, 2002; Volokh, 1997). However, very few empirical examinations of these programs demonstrate conclusiveness evidence of what is effective; therefore, we as a society are left with an enormous number of people in our society under the age of 18 who are vulnerable to become a victim online.

Based on the large amount of support found for Routine Activities Theory when exploring crime and preventative measures (Arnold et al., 2005; Cao & Maume, 1993; Cohen & Cantor, 1980; Cohen et al., 1981; Collins, Cox, & Langan, 1987; Cook, 1987; Ehrhardt-Mustaine & Tewksbury, 1997; Gaetz, 2004; Garofalo, Siegel, & Laub, 1987; LaGrange, 1999; Lasley, 1989; Lynch, 1987; Madriz, 1996; Moriarty & Williams, 1996; Mustaine & Tewksbury, 1999; Roncek & Bell, 1981; Roncek & Maier, 1991; Sampson, 1987; Spano & Nagy, 2005; Tewksbury & Mustaine, 2000; Tseloni, Wittebrod, Farrell, & Pease, 2004; Woolredge et al., 1992), new strategic measures that are developed under the same theoretical basis should work. Programs that increase guardianship while decreasing target suitability (i.e., digital locks and protections), as well as deter the motivated offender approaching youth online, would be expected to decrease the likelihood of victimization. Much like initiatives to make parks and playgrounds safe for our children, we need to make our children's cyber-playground a safer place to play.

An important note to remember is that the success of proactive prevention programs and other types of online safety measures is limited. The first and most imperative step to protection of children online is educating them on why it is important to avoid certain behaviors and places on the Internet. We as parents, law enforcement, and policymakers can implement as many programs as possible to keep our children away from dangerous zones online, but if they do not understand why it is dangerous, determination will find a way. Organizations such as the National Center for Missing & Exploited Children (2007) and Prevent Child Abuse America (2007) provide educational literature for children and adults about protecting yourself online. Through the use of these tools like these and other informative measures, we can keep the Internet a safe place for our children, as it was intended.

References

Ashcroft v. American Civil Liberties Union, 535 U.S. 564 (2002), 217 F.3d 162.

Bazelon, D., Choi, Y., & Conaty, J. (2006). Computer crimes. *The American Criminal Law Review, 43(2),* 259-310.

Beebe, T., Asche, S., Harrison, P, & Quinlan, K. (2004). Heightened vulnerability and increased risk-taking among adolescent chat room users: Results from a statewide school survey. *Journal of Adolescent Health,35(2)*, 116-123.

Barclay, P., Buckley, J., Brantingham, P., Brantingham, P.,& Whin-Yates, T. (1996). Preventing auto-theft in suburban Vancouver commuter lots: Effects of a bike patrol. *Crime Prevention Studies, 6,* 133-161.

Bowers, K., Johnson, S., & Hirschfield, A. (2004). The measurement of crime prevention intensity and its impact on levels of crime. *The British Journal of Criminology, 44(3),* 419-439.

Brantingham, P., & Brantingham, P. (1995). Criminality of place: Crime generators and crime attractors. *European Journal on Criminal Policy and Research, 3,* 5-26.

Brantingham, P., & Brantingham, P. (1998). Planning against crime. In M. Felson & R. Peiser (Eds.), *Crime Prevention Through Real Estate Development and Management.* Washington, DC: The Urban Land Institute.

Clinton, W. (1997, July 16). *Remarks by the president at event on the e-chip for the Internet.* Retrieved from The White House Office of the Press Secretary [Online], September 1, 2005, from: http://www.whitehouse.gov/WH/News/Ratings/remarks.html

Cohen, L., & Cantor, D. (1980). The determinants of larceny: An empirical and theoretical study. *Journal of Research in Crime and Delinquency, 17(2),* 140-159.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44,* 588-608.

Cohen, L., & Felson, M. (1981). Modeling crime trends: A criminal opportunity perspective. *Journal of Research in Crime and Delinquency, 18,* 138-164.

Danet, B. (1998). Revisiting computer-mediated communication and community. *Cybersociety 2.0,* 129-158.

Eck, J. (2002). Preventing crime at places. In L. Sherman, D. Farrington, B. Welsh & D. MacKenzie (Eds.), *Evidence-based crime prevention* (pp. 241-294). New York: Routledge.

Ehrhardt-Mustaine, E., & Tewksbury, R. (1997). The risk of victimization in the workplace for men and women: An analysis using routine activities/lifestyle theory. *Humanity and Society, 21(1),* 17-38.

Federal Communications Commission (2006).

Felson, M. (1986). Linking criminal choices, routine activities, informal social control, and criminal outcomes. In D. Cornish and R. Clarke (Eds.), *The Reasoning Criminal* (pp. 119-128). New York: Springer-Verlag.

Felson, M. (1987). Routine activities and crime prevention in the developing metropolis. *Criminology, 25,* 911-932.

Fitzpatrick, M. (2006, June 10). Testimony before house energy and commerce subcommittee on oversight and investigations.

Garofalo, J., Siegel, L., & Laub, J. (1987). School-related victimizations among adolescents: An analysis of national crime survey narratives. *Journal of Quantitative Criminology, 3(4),* 321-338.

Gibson, W. (1984). *Neuromancer.* New York: Ace Books.

Girodo, M., Deck, T., & Morrison, M. (2002). Dissociative-type identity disturbances in undercover agents: Socio-cognitive factors behind false-identity appearances and reenactments. *Social Behavior and Personality, 30(7),* 631-644.

Gore, A. (1999, May 5). *Remarks on the Internet.* Retrieved from The White House Office of the Press Secretary [Online], September 1, 2005, from: http://www.whitehouse.gov/WH/News/html/19990505-4219.html

Hawdon, J. (1996). Deviant lifestyles: The social control of routine activities. *Youth and Society, 28,* 162-188.

Henderson, H. (2005). *Internet predators.* New York: Facts On File.

Hunter, C. (2000). Social impacts: Internet filter effectiveness testing - over- and under inclusive blocking decisions of four popular web filters. *Social Science Computer Review, 18(2), 214-223.*

Jones, S. (1999). *Doing Internet research.* London: Sage.

Joseph, L. (2007). Keeping safe in cyberspace. *MultiMedia & Internet @Schools, 14(1),* 17-20.

Kendall, V. (1998). The lost child: Congress's inability to protect our teenagers. *Northwestern University Law Review, 92(4),* 1307-1315.

Kennard, W. (1999, May 4). *Remarks of William Kennard at the Annenberg Public Policy Center conference on Internet and the family [Online].* Retrieved September 1, 2005, from: http://www.fcc.gov/Speeches/Kennard/spwek916.html

Lamb, A. & Johnson, L. (2006). Want to be my friend? What you need to know about social technologies. *Teacher Librarian, 34(1), 55-57.*

Lasley, J. (1989). Drinking routines/lifestyles and predatory victimization: A causal analysis. *Justice Quarterly, 6(4),* 529-542.

Leiner, B., Cerf, V., Clark, D., Kahn, R., Kleinrock, L., Lynch, D., Postel, J., Roberts, L. & Wolff, S. (2003). A brief history of the Internet. *Internet Society.* Retrieved September 24, 2006, from http://www.isoc.org/internet/history/brief.shtml

Lewis, B. (2004). Prevention of computer crime and amidst international anarchy. *The American Criminal Law Review, 41(3),* 1353-1372.

Lynch, J. (1987). Routine activity and victimization at work. *Journal of Quantitative*

Criminology, 3(4), 283-300.

Madriz, E. (1996). The perception of risk in the workplace: A test of routine activity theory. *Journal of Criminal Justice, 24(5),* 407-412.

McCabe, K. (2000). Child pornography and the Internet. *Social Science Computer Review, 18(1),* 73-76.

Medaris, M. & Girouard, C. (2002). *Protecting children in cyberspace: The ICAC task force program.* Washington, DC: National Center for Missing & Exploited Children.

Meier, R. & Miethe, T. (1993). Understanding theories of criminal victimization. In M. Tonry (Ed.), *Crime and Justice: An Annual Review of Research* (pp. 459-499). Chicago: University of Chicago Press.

Miller v. California, 413 U.S. 15; 93 S. Ct. 2607; 37 L. Ed. 2d 419

Mitchell, K., Finkelhor, D. & Wolak, J. (2003). The exposure of youth to unwanted sexual material on the Internet: A national survey of risk, impact and prevention. *Youth & Society, 34(3),* 3300-3358.

Mitchell, K., Wolak, J., & Finkelhor, D. (2005). Police posting as juveniles to catch sex offenders: Is it working? *Sexual Abuse: A Journal of Research and Treatment, 17,* 241-267.

Mota, S. (2002). The U.S. Supreme Court addresses the Child Pornography Prevention Act and Child Online Protection Act in *Ashcroft v. Free Speech Coalition* and *Ashcroft v. American Civil Liberties Union. Federal Communications Law Journal, 55,* 85-98.

Mustaine, E., & Tewksbury, R. (2002). Sexual assault of college women: A feminist interpretation of a routine activities analysis. *Criminal Justice Review, 27(1),* 89-123.

National Center for Missing & Exploited Children. (2007). *June is National Internet Safety Month.* Retrieved June 13, 2007, from http://www.missingkids.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=3207

O'Connell, R., Barrow, C., & Sange, S. (2002). *Young peoples use of chat rooms: Implications for policy strategies and programs of education.* Retrieved November 1, 2005, from http://www.uclan.ac.uk/host/cru/publications.htm

Pease, K. (2002). Crime reduction. *Oxford Handbook of Criminology,* 947-979.

Prevent Child Abuse America. (2007). *Prevent Child Abuse America.* Retrieved June 13, 2007, from http://www.preventchildabuse.org/index.shtml

Raine, L. (2006). *Life online: Teens and technology and the world to come*. Speech to the annual conference of the Public Library Association, Boston. Retrieved October 1, 2006, from www.pewinternet.org/ppt/Teens%20and%20technology.pdf

Roberts, D., Foehr, U., Rideout, V., & Brodie, M. (1999). Kids & media @ the new millennium: A comprehensive analysis of children's media use. *The Henry J. Kaiser Family Foundation*.

Roncek, D., & Maier, P. (1991). Bars, blocks, and crimes revisited: Linking the theory of routine activities to the empiricism of "hot spots." *Criminology, 29(4),* 725-753.

Sampson, R., & Wooldredge, J. (1987). Linking the micro- and macro-dimension of lifestyle-routine activity and opportunity models of predatory victimization. *Journal of Quantitative Criminology, 3,* 371-393.

Sanger, D., Long, A., Ritzman, M., Stofer, K. & Davis, C. (2004). Opinions of female juvenile delinquents about their interactions in chat rooms. *Journal of Correctional Education, 55(2),* 120-131.

Simon, J. (2006). Computer-mediated communication: Task performance and satisfaction. *Journal of Social Psychology, 146(3)*, 349-379.

The Free Speech Coalition v. Reno, No. C 97-0281 VSC, 1997 WL 487758, at *7 (N.D. Cal. Aug. 12, 1997).

The guide. (2001). *On Magazine, 6(6).* Retrieved October 1, 2006, from: http://www.GetNetWise.com

Tseloni, T., Wittebrood, K., Farrell, G., & Pease, K. (2004). Burglary victimization in England and Wales, the United States and the Netherlands. *The British Journal of Criminology, 44(1),* 66-91.

United States Department of Justice. (2006, May 17). (FINISH CITE)

United States v. Hilton, 999 F. Supp. 131, 134 (D. Me. 1998)

Virginia Tech. (1997, July 21). *"Three-prong obscenity test."* Retrieved November 12, 2006, from the Virginia Tech website: http://courses.cs.vt.edu/~cs3604/lib/Censorship/3-prong-test.html

Volokh, E. (1997). Freedom of speech, shielding children, and transcending balancing. *Supreme Court Review, 141*, 141-197 [Online]. Retrieved September 1, 2005, from: http://www.law.ucla.edu/faculty/volokh/shield.htm

Wolak, J., Mitchell, K.J., & Finkelhor, D. (2004). Internet-initiated sex crimes against minors: Implications for prevention based on findings from a national study. *Journal of Adolescent Health, 35(5),* 11-20.

Wolak, J., Mitchell, K.J., & Finkelhor, D. (2006). *Online victimization of children: Five years later.* Washington, DC: National Center for Missing & Exploited Children.