Policing possession of child pornography online: investigating the training and resources dedicated to the investigation of cyber crime

Catherine D. Marcum†, George E. Higgins§, Tina L. Freiburger¥ and Melissa L. Ricketts‡

†(Corresponding author) Department of Political Science, Georgia Southern University, Campus Box 8101, Statesboro, GA. 30460 Tel: +1 912 478 7098; Fax: +1 912 478 5348; email: cmarcum@georgiasouthern.edu
§Department of Justice Administration, 208 Brigman Hall, College of Arts and Sciences, University of Louisville, Louisville, KY 40292. Tel: +1 502 852 0331; email: gehigg01@gwise.louisville.edu
¥University of Wisconsin of Milwaukee, Department of Criminal Justice, University of Wisconsin—Milwaukee, PO Box 786, 1139 Enderis Hall, Milwaukee, WI 53201, Tel: 414-229-6134; Fax: 414-229-5311; Email: freiburg@uwm.edu
‡Shippensburg University Shippen Hall, 1871 Old Main Drive, Shippensburg, PA 17257-2299. Tel: 717-477-1550; Fax: 717-477-4087; Email:@ mlricketts@ship.edu

Submitted 16 March 2010; revision submitted 29 May 2010; accepted 10 June 2010

Keywords: cyber crime, child pornography, policing, task forces

Catherine D. Marcum *is an assistant professor of justice studies in the Political Science Department at Georgia Southern University. She received her PhD in criminology from Indiana University of Pennsylvania. Her most recent publications are in Deviant Behavior; Criminal Justice Studies: A Critical Journal of Crime, Law, and Society; International Journal of Cyber Criminology; and Journal of Child Sexual Abuse.*

George E. Higgins *is an associate professor in the Department of Justice Administration at the University of Louisville. He received his PhD in criminology from Indiana University of Pennsylvania in 2001. His most recent publications appear in Criminal Justice Studies; Deviant Behavior; Criminal Justice and Behavior; and American Journal of Criminal Justice.*

Tina Freiburger *is an assistant professor in the Department of Criminal Justice at the University of Wisconsin-Milwaukee. Her current research interests include gender and racial disparities in sentencing, criminological theory, and online victimisations and offending. Her recent publications have appeared in American Journal of Criminal Justice; Behavioral Sciences and the Law; Crime and Delinquency; and Criminal Justice Policy Review.*

Melissa L. Ricketts *is an assistant professor in the Criminal Justice Department at Shippensburg University. She received her PhD in Criminology from Indiana University of Pennsylvania. Her most recent publications appear in Journal of School Violence; Western Criminology Review; and Criminal Justice Studies. Her research focuses on criminological theory testing.*

International Journal of Police Science and Management, Vol. 12 No. 4, 2010, pp. 516–525. DOI: 10.1350/ijps.2010.12.4.201

Abstract

The internet is not a single network, limited to one specific type of information or restrictive of the

types of users who can access its information. Conversely, the internet is an intercontinental information highway that has enabled people of all ages to communicate with family and friends with lightning-fast speed, share and collect information, and connect with people and companies thousands of miles from their computer (Roberts, Foehr, Rideout, & Brodie, 1999; Rosenbaum et al., 2000; Smith & Rupp, 2002). However, this growth of information technology has introduced a new form of criminality to the criminal justice system: cyber crime (Denning, 1998). The purpose of this research study is to investigate the prevalence of cyber criminality, specifically possession of child pornography, in law enforcement jurisdictions and the types of training which local and State law enforcement agencies currently offer to effectively combat these technological crimes.

INTRODUCTION

The internet is not a single network, limited to one specific type of information or restrictive of the types of users who can access its information. Conversely, the internet is an intercontinental information highway that has enabled people of all ages to communicate with family and friends with lightning-fast speed, share and collect information, and connect with people and companies thousands of miles from their computer (Roberts, Foehr, Rideout, & Brodie, 1999; Rosenbaum et al., 2000; Smith & Rupp, 2002). However, this growth of information technology has introduced a new form of criminality to the criminal justice system: cyber crime (Denning, 1998).

Multiple forms of innovative cyber crime have emerged in the recent years. This type of criminality can include, but is not limited to, the following: digital piracy, identity theft, financial theft, computer hacking, embezzlement, and espionage (Rosoff, Pontell, & Tillman, 2002). Moreover, cyber crime can also include the production and possession of child pornography (Quayle & Taylor, 2003). Due to increasing concerns in the criminal justice community about the prevalence of cyber crime, some law enforcement agencies are making a concerted effort to target this behaviour with additional resources (Broadhurst, 2006; Hinduja, 2004). This can include general cyber crime task forces, or specialised task forces to target certain types of cyber crime (such as child pornography). Currently, there is a gap in the literature investigating the efforts made nationally by law enforcement agencies to target resources towards cyber crime investigation and arrest. The purpose of this research study is to specifically investigate the prevalence of online child pornography possession in law enforcement jurisdictions and the types of training which local and State law enforcement agencies currently offer to effectively combat all cyber crime (including possession of child pornography).

Policing cyber crime

A large percentage of unreported cyber crimes are a result of the difficulty in detecting these high-tech crimes and the lack of training which police officers generally receive at the academy (Leibowitz, 1999). Policing cyber crime is significantly different from policing crimes involving a physical crime scene in a neighbourhood or office building. The digital crime scene cannot be marked with yellow crime-scene tape that contains a specific physical area where the crime occurred, as it may extend beyond a home, city, State, or even a continent (Katos & Bednar, 2008). A digital crime scene includes all involved or infected computers, the location of which can range from different states to different continents; therefore, it makes it difficult for police to confine their investigation to a smaller identified area known as the 'crime scene', when policing the internet often involves

exploring unknown territory. For example, when investigating possession of child pornography crimes, law enforcement agencies can seize hardware and software from multiple users, as well as perform investigations to determine the online locations where the pornography was purchased and downloaded (Taylor & Quayle, 2006). Due to the sophistication of the technology used by expert collectors of this material, bulletin boards and websites often appear for only minutes to allow active users and traders to obtain the material. Once the limited time-period is over, the website 'disappears' and tracking its original location is difficult for the untrained law enforcement officer.

In order to investigate effectively and make arrests for these offences, sophisticated technology for communication and investigation is required, and law enforcement officers need specialised training in investigation tactics (Wells, Finkelhor, Wolak, & Mitchell, 2007). Only within the past decade have police departments developed cyber crime task forces to investigate better and eventually prosecute these crimes (Broadhurst, 2006; Hinduja, 2004). The goal of these task forces, often called CERTs (computer emergency response teams) is to follow up on tips from the public, as well as to explore the internet service providers which are providing offensive material and allowing illegal activities to occur on their sites. Cyber task forces and law enforcement efforts specifically aimed at investigating possession of child pornography are often responsible for disbanding a range of criminal figureheads, from dealers of only a few photographs up to elite international traffickers. For example, in 1998 the federal government disbanded 'The Wonderland' group, whose membership involved traffickers in over 40 countries. One of the defendants, Antoni Skinner, was found to have over 750,000 pornographic images of minors on his computer (McAuliffe, 2001 as cited in Marcum, 2007). More recently, the Department of Justice arrested over 500 individuals globally in 'Operation Nest Egg'. This investigation originated in the southern district of Indiana and grew to an international investigation of possession of child pornography (CNN.com, 2010).

As a result of these specialised task forces, more departmental funds are dedicated to training officers for cyber crime investigation (Broadhurst, 2006). However, the resources dedicated to cyber crime investigation and prosecution are still minimal and local law enforcement agencies recognise the need for these task forces. For example, Hinduja (2004) found that an overwhelming 75 per cent of law enforcement agencies in the State of Michigan believe better training was their biggest need in order to investigate these types of crimes better. This continues to emphasise the need for better cyber crime investigation training, especially dedicating resources toward crimes that violate children. The next section will explain the difficulty often encountered when investigating these types of crimes.

Child pornography

There is often confusion in the general public about what constitutes a cyber crime, especially when the crime existed before the emergence of the internet (eg, possession of child pornography). According to Wall (2007), there are three different groups of cyber crimes that can be identified. First, there are 'traditional' crimes in which computers were used to communicate or gather information to assist with a crime. However, if the use of the computer was removed, the criminal behaviour would still commence. On the other end of the spectrum are 'true' cyber crimes, which are crimes committed only in cyberspace and

are the product of the opportunities available on the internet: an example is spamming. Finally, there are the 'hybrid' crimes, which are crimes that fall between traditional and true cyber crimes. These are traditional crimes already in existence, but expanded through the use of the internet. Possession of child pornography is a classic example of this type of crime.

Although States vary on the definition of child pornography, it is generally defined as sexually explicit pictures or films involving young people under the age of 18 (Klain, Davies, & Hicks, 2001). There is a continuum of different types of child pornography, ranging from non-erotic pictures of children to sadistic images (Taylor, Quayle, & Holland, 2001). According to Seigfried, Lovely, and Rogers (2008), persons who possess this material are more likely to be manipulative, exploitative and have lower levels of morality. Moreover, Quayle and Taylor (2003) have argued that many adult predators are motivated to possess child pornography to use as a seduction tool.

Rather than risking exposure through the receipt of magazine and mail-order pictures, collectors can now access images with the click of a mouse (Jenkins, 2001; Taylor, Quayle, & Holland, 2001). These images can be bought and traded much like baseball cards or comic books. Wolak, Mitchell, and Finkelhor (2003) found that from July 2000 to July 2001, over 1,700 offenders were arrested for possession of child pornography. 80 per cent of these images involved graphic sexual images, while 83 per cent contained prepubescent children. Furthermore, Hinduja (2004) discovered that Michigan law enforcement agencies encountered a sizable amount of internet child pornography cases (31.9 per cent of their total case load). Only online harassment/stalking (39.5 per cent) were encountered more in their cyber crime investigations. As the evidence in these cases is electronic and easily erased or moved, this makes it more difficult for law enforcement agencies to investigate these cases using traditional methods (Wells et al., 2007). Obviously, there is a need for law enforcement agencies to better dedicate resources toward training officers to investigate these high-tech crimes.

THE PRESENT STUDY

The purpose of this paper is to add to the small amount of literature investigating law enforcement agency reaction to the growing occurrence of cyber crime. This study will investigate the prevalence of online child pornography possession investigations and arrests by law enforcement agencies in the United States, as well as the training and resources dedicated to investigating cyber crimes in general. More specifically, the current research examines whether the presence of a specialised task force and training programmes focused on the investigation of cyber crimes increases the number of investigations and arrests for cyber crime. It is expected that the additional use of a special task force and specialised training will increase departments' abilities to detect incidences of child porn violations, leading to a higher number of investigations and arrests.

METHODOLOGY

Research design

The study involved mailing a one-page, double-sided survey to law enforcement agencies for cities with a population of 50,000 or more. Our original population was chosen from the listing of cities in the United States provided by the 2000 United States Census. The letters were directed to the head law enforcement agent of the department, such as the chief or sheriff. Although an online survey would be less expensive, they generally have a much

lower response rate than surveys that are mailed or administered in a group setting (Dillman, 2007). In order to get our desired sample size, we felt a mailed survey would best reach this goal. Three waves of mailings were sent between November 2009 and January 2010 to retrieve the optimal response rate. Of the 625 surveys mailed, 168 were returned which equated to a 26.9 per cent response rate.

Measures

The survey requested information from law enforcement agencies on several different measures. First, agencies were requested to report data from 2007 and 2008 regarding the number of investigations of and arrests for several different forms of cyber crime. This particular study only examines one of the forms of cyber crime noted on the survey: possession of child pornography. Next, agencies were asked to provide information on the types of training and amount of resources, if any, dedicated to the investigation of cyber crime. Finally, demographic information was requested regarding the jurisdiction of the agency and the department.

Dependent measures

The present study uses four dependent measures. Each of the dependent measures concerns the possession of child pornography. In addition, the measures concern the occurrences investigated and the arrests that were made for the possession of child pornography. Specifically, the first item is: 'Please mark the column that best indicates the total number of cyber crime occurrences investigated by your department in the years 2007 and 2008: possession of child pornography'. The second item is: 'Please mark the column that best indicates the total number of cyber crime arrests made by your department in the years 2007 and 2008: possession of child pornography'. Because the items cover 2007 and 2008 the two items result into four items. The respondents indicated the number of occurrences investigated and arrests made, for each year, using a 3-point Likert-type indicator (i.e., 0 = 0–5, 1 = 6–10, and 2 = 11+). We dichotomised these measures so that we might be able to capture better whether an investigation or an incident took place.

Independent measures

The present study uses five independent measures. The first independent measure is: 'Do you have a designated task force/departmental unit that solely investigates cyber crime?' The answer choices were 0 = no and 1 = yes. The second measure is: 'Does your department in general receive training for cyber crime investigations?' The answer choices were 0 = no and 1 = yes. The third measure is the region of the country where the respondent is located. Specifically, the item is: 'What region of the country are you located?' The answer choices were as follows: 1 = Northwest, 2 = Southwest, 3 = Midwest, 4 = Northeast and 5 = Southeast. The fourth measure was the respondents' indication of the number of sworn officers. The respondents addressed the following item: 'How many sworn officers are employed in your department?' The respondents indicated the number using an open-ended response. The respondents were asked about whether their department had an education requirement. The item is: 'Do police officers in your department have an education requirement?' The answer choices were 0 = no and 1 = yes.

Analysis plan

The analysis plan takes place in a series of steps. The first step is a presentation of the

descriptive statistics. This takes place to provide an indication of the distribution of the measures. The second step is a series of regression analyses that compare 2007 with 2008 correlates. In cross-sectional data, regression analysis (ie, Ordinary Least Squares Regression (OLS)) is a statistical technique that indicates the change in a dependent measure based on a series of independent measures. Given that we used dichotomous dependent variables, the proper form of regression analysis is logistic regression (Menard, 2002). One important assumption in OLS is multicollinearity. Multicollinearity occurs when multiple independent measures are highly correlated to a point where they are indicating the same concept. Freund and Wilson (1999) argued that tolerance levels of 0.20 and below are an indication of multicollinearity. This remains true when using dichotomous dependent measures (Menard). Our focus is not to directly compare the differences in the coefficients between the years. Thus, we refrained from using a coefficient difference test: see Paternoster, Brame, Mazerolle, and Piquero (1998).

RESULTS

Step 1

Table 1 presents the descriptive statistics for this sample. This table shows that 30 per cent of the sample has a designated cyber crime task force and that 41 per cent of the sample has departmental training on cyber crimes. The average department was in the Southwest region of the country and 93 per cent of the departments have an educational requirement. In 2007, 48 per cent of the departments conducted possession of child pornography investigations, and that rose to 51 per cent in 2008. In 2007, 31 per cent of the departments arrested for possession of child pornography, and the percentage rose to 34 per cent in 2008.

Table 1 also shows that two of the items are non-normally distributed. The open-ended response to the item that addresses the number of sworn officers is non-normal. We would expect this item to be non-normal given that the answer choice is open-ended. To avoid cumbersome interpretations based on transformations, we retained the item as the respondents

Table 1: Descriptive statistics for the measures in the present study

Measure	*Mean*	*Standard deviation*	*Skew*	*Kurtosis*	*Min*	*Max*
Designated task force	0.30	–	0.86	–1.27	0	1
Department training	0.41	–	0.38	–1.88	0	1
Region	2.58	1.30	–0.33	–1.07	0	4
Sworn officers	292.07	911.56	8.37	81.75	12	10,000
Education requirement	0.93	–	–3.55	10.69	0	1
Possession of child pornography investigations 2007	0.48	–	0.08	–2.02	0	1
Possession of child pornography investigations 2008	0.51	–	–0.06	–2.03	0	1
Possession of child pornography arrests 2007	0.31	–	0.83	–1.33	0	1
Possession of child pornography arrests 2008	0.34	–	0.67	–1.58	0	1

N = 168

indicated. In addition, the responses to the educational requirement are non-normal as well. Today, most police agencies have an educational requirement; thus, we would expect nearly the non-normality as the responses are over 90 per cent. We retained this item in its current form.

Step 2

Table 2 presents two logistic regression analyses that explore the correlates of conducting an investigation for child pornography in 2007 and 2008. In 2007, the number of sworn officers (b = 0.01, Exp(b) = 1.01) and police departments that have designated task forces (b = 1.23, Exp(b) = 3.43) increase the likelihood of performing a child pornography possession investigation. The region of the country (ie, the departments in the South) were less likely to perform child pornography investigations (b = -0.39, Exp(b) = 0.68). In 2008, as the number of sworn officers (b = 0.01, Exp(b) = 1.01) and police departments with designated task forces (b = 1.56, Exp(b) = 4.76) increased, so did the likelihood of performing a child pornography investigation. Following Menard (2002), we used tolerance as a measure of multicollinearity. For both years, the tolerance figures were above the 0.20 cut-off suggesting that multicollinearity was not a problem.

Table 3 presents the logistic regression analysis for the child pornography arrests in 2007 and 2008. In 2007, child pornography arrests were more likely when the number of sworn officers increased (b = 0.00, Exp(b) = 1.00), and when the police department had a designated task force (b = 1.58, Exp(b) = 2.30). Having departmental training also led to increased odds of arrests (b = 0.05, Exp(b) = 0.83). In 2008, increases in the number of sworn officers (b = 0.00, Exp(b) = 1.00) and police departments that have a designated task force (b = 1.71, Exp(b) = 5.53) are more likely to have child pornography arrests. Following Menard (2002), we used tolerance as our measure of multicollinearity. Our results show that multicollinearity was not an issue with these data.

Table 2: Regression analysis for child pornography possession 2007 and 2008 investigations

	2007				*2008*			
Measure	*B*	*S.E.*	*Exp(b)*	*Tolerance*	*b*	*S.E.*	*Exp(b)*	*Tolerance*
1. Region of country	–0.39★	0.15	0.68	0.93	–0.27	0.15	0.77	0.93
2. Sworn officers	0.01★★	0.00	1.01	0.990	.01★★	0.00	1.01	0.99
3. Education requirement	1.63	1.13	5.11	0.97	1.72	1.13	5.58	0.96
4. Designated task force	1.23★★	0.44	3.43	0.93	1.56★★	0.46	4.76	0.93
5. Department training	0.66	0.40	1.93	0.99	0.64	0.41	1.89	0.99
Chi-Square	53.39				49.09			
–2 Log likelihood	154.31				147.51			
Cox & Snell *R*-Square	0.30				0.29			
Nagelkerke *R*-Square	0.40				0.39			
	N = 168				*N* = 168			

Note:
★ $p<0.05$, ★★ $p<0.01$

Table 3: Regression analysis for child pornography arrests for 2007 and 2008

	2007				*2008*			
Measure	*b*	*S.E.*	*Exp(b)*	*Tolerance*	*b*	*S.E.*	*Exp(b)*	*Tolerance*
1. Region of country	–0.30	0.16	0.74	0.92	–0.15	0.16	0.86	0.93
2. Sworn officers	0.00**	0.00	1.00	0.97	0.00**	0.00	1.00	0.97
3. Education requirement	0.20	0.90	1.22	0.98	0.47	0.95	1.59	0.96
4. Designated task force	1.58***	4.86	0.95	1.71**	0.44	5.53	0.94	
5. Department training	0.83*	0.42	2.30	0.99	0.49	0.43	1.64	0.98
Chi-Square	43.79				33.96			
–2 Log likelihood	142.74				135.85			
Cox & Snell *R*-Square	0.25				0.23			
Nagelkerke *R*-Square	0.36				0.31			
	N = 168				*N* = 168			

Note:
* $p<0.05$, ** $p<0.01$, *** $p<0.001$

DISCUSSION

In addition to the communication advantages brought about by the internet, several problematic issues have also been presented. Specifically, traditional crimes such as child pornography have found a new and efficient outlet by which to be distributed. This new outlet has made these crimes harder to detect and increased their prevalence. The current study examined variations in police departments' investigations and arrests in child pornography cases to determine if having a specialised task force and training specific to cyber crime investigation increases law enforcement agencies' abilities to detect these crimes.

The results showed that having a specialised task force did increase the number of child pornography investigations and the number of arrests for child pornography. It does appear, therefore, that the addition of a specialised task force enables police departments to detect cases of child pornography, leading to an increase in investigations and arrests. The addition of training for cyber crimes, however, was only significantly related to child pornography arrests in 2007. It was not significantly related to investigations in 2007 or 2008 nor was it significantly related to arrests in 2008. While this finding was contrary to arguments in prior research and what was initially expected (Leibowitz, 1999; Wells et al., 2007), a few possible explanations exist.

It is possible that the addition of cyber crime training is not indicative of sufficient resources to investigate and carry out arrests for child pornography crimes. Even with cyber crime training, some departments may still lack the personnel actually to police such crimes. It also is possible that the addition of cyber crime training results in more investigations and arrests for other types of cyber crimes. Although the current study specifically examined child pornography cases, police departments were asked if they had programmes specific to cyber crime. Child pornography is just one such crime. It is possible, therefore, that training has been effective at increasing the investigation and arrest of cyber crimes other than child pornography.

Lastly, the inability of training programmes to significantly increase the number of investigations and arrests might be

due to the quality of the training programme being utilised. The current data are limited to the determination of whether a training programme is used by each department. No information is currently available as to the information provided in the training, whether officers receive training specific to child pornography, the length of the training provided, or the qualifications of the individuals administering the training. It is possible, therefore, that the training programmes are inadequate in preparing officers to deal with these types of crimes.

LIMITATIONS AND IMPLICATIONS

Although the current study offers insight into the impact of different police organisations on the investigation and arrest of online child pornography, it suffers from a couple of limitations. First, several of the departments surveyed did not respond. This can introduce non-response error if the departments who did not respond handle online pornography cases differently from those that did respond. This is, however, a common limitation when organisations are surveyed (see Dillman, 2007). Finally, as briefly mentioned above, detailed information regarding the content of the training was not collected. It is possible that some training programmes are more effective than others. Given the data collected for the current study, however, this could not be determined.

Despite the above limitations, the current results suggest important policy and future research recommendations. The increased ability of police departments with specialised task forces to investigate and make arrests for child pornography, indicates the importance of police departments to allocate necessary resources to the investigation of cyber crimes. As discussed earlier, cyber crimes such as child pornography are often undetected and under-reported (Kabay, 2000). Increasing the certainty of apprehension and punishment could potentially decrease the prevalence of these crimes.

Future research should also more closely examine the training programmes being used by various police departments. It is possible that some training programmes actually are effective. More detailed information regarding the content and manner in which training programmes are delivered could lead to a deeper understanding of why these programmes do not consistently increase investigations and arrests. Outcome evaluations of these specific programmes can then aid in determining which types of training have the potential to significantly affect the policing of cyber crimes. These findings can then be used to develop a 'best practices programme' that can be utilised by other departments to increase the effectiveness of cyber crime training.

References

Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. *Policing: An International Journal of Police Strategies & Management, 29*(3), 408–433.

CNN.com. (2010). *Feds shut child porn social networking site.* Retrieved May 29, 2010, from http://news.blogs.cnn.com/2010/05/27/feds-shut-child-porn-social-networking-site/?iref=allsearch

Denning, D. (1998). *Information warfare and security.* Reading, MA: Addison-Wesley.

Dillman, D. (2007). *Mail and internet surveys: a tailored design method*. Hoboken, NJ: John Wiley.

Freund, R. & Wilson, W. (1998). *Regression analysis: Statistical modeling of a response variable.* San Diego, CA: Academic Press

Hinduja, S. (2004). Perceptions of local and state law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies & Management, 27*(3), 341–357.

Jenkins, P. (2001). *Beyond tolerance: child*

pornography on the internet. New York University Press.

Kabay, M. E. (2000). *Studies and surveys of computer crime.* Retrieved March 1, 2010, from http://www.security portal.com/cover/coverstory20001211.html

Katos, V., & Bednar, P. (2008). A cyber-crime investigation framework. *Computer Standards and Interfaces, 30*(4), 223–228.

Klain, E., Davies, H., & Hicks, M. (2001). *Child pornography: the criminal justice system response.* Alexandria, VA: American Bar Association Center on Children and the Law for the National Center for Missing & Exploited Children.

Leibowitz, W. R. (1999). How law enforcement cracks cyber crimes. *New York Law Journal,* 5.

Marcum, C. D. (2007). Interpreting the intentions of internet predators: an analysis of online chat room transcripts. *Journal of Child Sexual Abuse, 16*(4), 99–114.

Menard, S. (2002). *Logistic regression.* Thousand Oaks, CA: Sage.

Paternoster, R., Brame, R., Mazerolle, P., & Piquero, A. (1998). Using the correct statistical test for the equality of regression coefficients. *Criminology, 36*, 859–866.

Quayle, E., & Taylor, M. (2003). Model of problematic internet use in people with a sexual interest in children. *CyberPsychology & Behavior, 6*, 93–106.

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

Rosenbaum, M., Altman, D., Brodie, M., Flournoy, R., Blendon, R., & Benson, J. (2000). *NPR/Kaiser/Kennedy School Kids and Technology Survey.* Retrieved September 24, 2006, from http://www.npr.org/programs/specials/pool/technology/technology.kids.html

Rosoff, S., Pontell, H., & Tillman, R. (2002). *Profit without honor: white-collar crime and the looting of America.* Upper Saddle River, NJ: Prentice Hall.

Seigfried, K., Lovely, R., & Rogers, M. (2008). Self-reported online child pornography behavior: a psychological analysis. *International Journal of Cyber Criminology, 2*(1), 286–297.

Smith, A., & Rupp, W. (2002). Issues in cybersecurity: understanding the potential risks associated with hackers/crackers. *Information Management & Computer Security, 10*(4), 178–183.

Taylor, M. & Quayle, E. (2006). The Internet and abuse images of children: Search, precriminal situations and opportunity. In R. Wortley and S. Smallbone (Eds.) *Crime prevention studies: Vol. 19 Situational prevention of child sexual abuse* (pp. 169–195). Monsey, N.Y: Criminal Justice Press/Willan Publishing.

Taylor, M., Quayle, E., & Holland, G. (2001). Child pornography, the internet and offending. *Canadian Journal of Policy Research, 2*(2), 94–100.

Wall, D. (2007). *Cybercrime: the transformation of crime in the information age.* Cambridge: Polity.

Wells, M., Finkelhor, D., Wolak, J., & Mitchell, K. (2007). Defining child pornography: law enforcement dilemmas in investigations of internet child pornography possession. *Police Practice & Research, 8*(3), 269–282.

Wolak, J., Mitchell, K., & Finkelhor, D. (2003). *Internet sex crimes against minors: the response of law enforcement.* Washington, DC: National Center for Missing & Exploited Children.