Winter 2003

Law enforcement dilemmas in the investigation of Internet sex crimes against minors

Melissa Wells
University of New Hampshire, Durham

Recommended Citation
Wells, Melissa, "Law enforcement dilemmas in the investigation of Internet sex crimes against minors" (2003). *Doctoral Dissertations*. 200.
https://scholars.unh.edu/dissertation/200

LAW ENFORCEMENT DILEMMAS IN THE INVESTIGATION OF INTERNET SEX CRIMES AGAINST MINORS

BY

MELISSA WELLS

BA University of New Hampshire, 1991

MSW University of Minnesota Duluth, 1995

DISSERTATION

Submitted to the University of New Hampshire
in Partial Fulfillment of
the Requirements for the Degree of

Doctor of Philosophy
in
Sociology

December, 2003

ProQuest Information and Learning Company
300 North Zeeb Road
P.O. Box 1346
Ann Arbor, MI 48106-1346

This dissertation has been examined and approved.

Dissertation Director, David Finkelhor, Ph.D., Professor of Sociology

Michele Dillon

Michele Dillon, Ph.D., Associate Professor of Sociology

James Tucker, Ph.D., Associate Professor of Sociology

Robert Jolley, Ph.D., Chair and Associate Professor of Social Work

Kimberly Mitchell

Kimberly Mitchell, Ph.D. Research Assistant Professor of Psychology

JWolak

Janis Wolak, J.D., Research Assistant Professor of Family Research

11/25/13

Date

DEDICATION

To my father, David C. Wells, who always believed that attitude and hard work make all the difference.

ACKNOWLEDGEMENTS

I would first like to thank David Finkelhor for his sincere commitment to his role as mentor to graduate students. As the chair of this dissertation committee, David provided comprehensive feedback and constant encouragement. I am grateful that David, Janis Wolak and Kimberly Mitchell allowed me to extend my work as a research assistant in the Crimes Against Children Research Center to include this project. I cannot thank David, Janis and Kim enough for providing this opportunity. It has been an honor to work as a member of this outstanding research team. Janis willingly shared her office space, time and extensive knowledge of this subject. Kim provided many hours of ready assistance with data entry and statistical analysis.

This research would not have been possible without sponsorship from the National Center for Missing & Exploited Children and funding from the U.S. Department of Justice. Their support is just one example of the commitment of these two agencies to the empirical study of crimes against children.

The other members of my dissertation committee consistently provided timely and substantive feedback on all phases of this dissertation. Jim Tucker shared resources and offered crucial insight on Donald Black's theories and the sociology of law. Michele Dillon's passion for qualitative research, initial encouragement, and suggestions during the development of my proposal helped to shape this research. Bob Jolley's observations and thorough editorial comments provided focus and clarification at many stages of this project.

My family deserves special recognition, as this accomplishment is a testament to their love and support. First, I thank Karl for his belief in my professional goals, his eternal optimism, his patience and so much more. In addition, thanks to Mom, Chris, Jen, Nancy, Steve, Elli and all who agreed that this was a goal worth pursuing. Thanks also to the many friends who encouraged me all along to "finish the paper" and who keep me connected to the world outside of graduate school.

There are so many others who have shaped my professional career and who have been helpful throughout my graduate years. The Social Work faculty at the University of Minnesota Duluth instilled a passion for research and encouraged me to continue my graduate education. Graduate students here and at other institutions were willing providers of support and perspective. Weekly runs with Liz Caffrey allowed for deep discussions of this project and served as the ideal dissertation support group. In addition, I would like to thank Erika Gebo, Nena Stracuzzi, Derek Bowen, Wendy Walsh, Kathy Kopiac, Paul Muller, Luiz Rodriquez and other graduate students past and present for sharing their knowledge and experiences.

Finally, I would like to acknowledge the many law enforcement investigators who shared these cases and their experiences. Their commitment to the protection of children and their passion for law enforcement are an inspiration.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

LAW ENFORCEMENT DILEMMAS IN THE INVESTIGATION OF INTERNET SEX CRIMES AGAINST MINORS

by

Melissa Wells

University of New Hampshire, December, 2003

This study examines dilemmas associated with the investigation of Internet sex crimes against minors. Data collected from a national sample of law enforcement agents provide insights into complications of three types of cases: (1) Internet crimes against identified victims, (2) Internet solicitations to undercover law enforcement, and (3) Internet child pornography crimes.

A mail survey of United States law enforcement agencies identified two samples of Internet sex crimes against minors. The first sample consisted of 464 investigations in which an arrest was made, and the second sample included 68 cases in which no arrest was made. Telephone surveys were used to collect case-specific data on both samples, and in addition, data were collected on dilemmas in the investigations in which law enforcement made no arrest.

An exploratory analysis found that law enforcement investigators reported challenges related to defining child pornography, identifying offenders, determining the criminality of preparatory acts (including online grooming of minors), some victim characteristics (such as victim cooperation), and collaboration between law enforcement agencies. Remedies exist for some of these dilemmas, and others may require innovative efforts, policy development, or additional research.

To examine predictors of legal action taken in these cases, a second analysis compared the sample of cases in which an offender was arrested to those in which law enforcement made no arrest. Those findings provide some support for sociological theories that social structural characteristics predict law enforcement action if legal context factors are held constant, but also suggest some contradictions.

Logistic regression was used to test the relationship between social and legal structure of cases and law enforcement action taken in these Internet sex crimes against minors. These findings suggest that when the legal context of cases was controlled, cases were most likely to receive legal attention if they involved adult offenders and if the parties had a relationship prior to any Internet communication. The latter finding is not consistent with sociological theories, which suggest that cases between strangers are more likely to attract legal attention. However, these findings may be related to gaps in social information, which present significant challenges in these investigations.

STATEMENT OF PROBLEM

Although child sex crimes have been a recognized social problem for more than two decades (Finkelhor 1984), recent policy and media attention has focused on the commission of these crimes via the Internet. The emergence of Internet-facilitated sex crimes, including Internet sex crimes against identified victims and online child pornography, has raised crucial questions regarding the use of the Internet by offenders, the safety of children online, and the ability of law enforcement to address these offenses.

This study explores two general categories of Internet Sex Crimes Against Minors, online sexual abuse and online child pornography. Online sexual abuse crimes could include incidents in which the Internet is used to sexually solicit juvenile victims online, crimes between family members with an Internet component, as well as crimes in which these online meetings may lead to actual meetings and sexual assaults. Online child pornography crimes involve an offender's use of the Internet or computer technology to possess, distribute, and/or collect electronic images of child pornography.

All of these crimes involve some form of Internet nexus. In some instances, such as online solicitations of minors, the Internet is directly used in the commission of a crime, and in others (including email communications following a sexual assault by a family member) it plays a peripheral role. Computer crimes are relatively new phenomena, and there is little empirical evidence regarding how or if these Internet sex crimes against minors differ from their conventional counterparts. Recent media reports feature prominent cases of Internet sex crimes against identified minors. In August of

2001 a 15-year old girl from Massachusetts agreed to meet an adult she met online, and was subsequently taken to New York, held hostage, and sexually abused for a week (The Associated Press 2002). A corrections officer was found to have a collection of child pornography images on his computer. Some of the images featured this corrections officer nude and engaging in what appeared to be sexual acts with children (Messing, Allen, and Connor 2001).

As is suggested by these media accounts, the Internet is a central element in these crimes. Several features of Internet communication, including the relative anonymity and privacy of Internet use, electronic transmission speed, and the elimination of geographic barriers to communication distinguish online interactions. However, there is little empirical evidence regarding the overall impact of the Internet-nexus on either the commission of sex crimes against juveniles or law enforcement investigations of these crimes. It is clear that the Internet may facilitate some criminal offenses, by providing offenders mass access to child victims, for example, or by linking geographically distant child pornography dealers. On the other hand, the Internet may deter the commission of some criminal offenses, by limiting initial physical vulnerability and potentially providing some measure of anonymity online.

Impact of the Internet on Law Enforcement

It is also difficult to gauge the impact of the Internet on law enforcement effectiveness. While investigating computer crimes can pose specific challenges for law enforcement, the Internet has also opened up new avenues for investigation and evidence collection in child sex crimes. Investigations of Internet sex crimes against minors generally require specific technical expertise, which is not available to all law enforcement agencies.

However, computer technology can provide law enforcement with powerful weapons and forensic evidence often lacking in child sex crimes (Norland and Bartholet 2001:49). Since much of what takes place on the Internet leaves a digital trail, it is possible that this social change may actually facilitate police investigations of some child sex crimes, and allow law enforcement agencies with access to computer forensic equipment to collect valuable digital evidence.

Sociology of Law

The sociology of law recognizes that law varies according to "the social environment within which legal events occur" (Baumgartner 1999:2). Sociologists of law have found that similar acts may elicit various law enforcement responses, depending upon the social characteristics of the individuals involved in specific incidents. In terms of arrest for instance, the sociology of law suggests that even within the same jurisdiction and with similar amounts of evidence, police may arrest one suspect, let another go with a warning, and choose never to investigate others (Baumgartner 2001).

Much of the existing literature regarding Internet sex crimes against minors enumerates the ways in which legal context factors including digital evidence and case severity impact law enforcement efforts (U.S. Department of Justice 2000). Sociologists like Baumgartner (2001) and Black (1980) suggest that while these factors can impact arrest, sociological factors account for much of the variation in law when legal factors are held constant.

This analysis will draw upon the sociology of law, with particular emphasis on theories of law presented by Donald Black (1976). Black (1976; 1980) provides a compelling framework for examining legal involvement in general and arrest more specifically. His theories of law, first presented in *The Behavior of Law* (Black 1976), were developed prior to the emergence of computer crime. This study presents an opportunity to investigate the applicability of Black's theories of law and arrest to crimes committed with a computer nexus.

What literature exists on this topic provides unclear evidence regarding the ability of Black's theories to explain arrest likelihood and legal involvement in these crimes. The sociology of law suggests that legal and resource factors may vary from case to case, and that the social structure of crimes, including victim and offender characteristics, are strong predictors of arrest (Baumgartner 2001). According to this theory, legally similar crimes may result in different outcomes, according to the social structure of the crime, which may include the social status of the parties involved, the relationship between victims and offenders, and other social aspects of the crime.

Crimes with a computer nexus present unique cases for examining this theory. It may be that there is variation in social characteristics of victims and offenders in Internet sex crimes against minors, and that this social variation impacts arrest. If this is the case, for example, we may find that arrest is less likely in cases where victims and offenders are family members than in cases in which they are strangers. However, we would expect legal and resource factors to be stronger predictors of arrest in these crimes under two conditions. First, it may be that there is little variation in the social structure of these cases. For instance, it is possible that the socioeconomic status of victims and offenders in these crimes is similar. If the social structure of these crimes is the same, then we predict that legal and resource variables will predict arrest.

There is a second condition under which Black's theory would suggest that legal and resource variables are stronger predictors of arrest in Internet sex crimes against minors. The social structure of cases cannot predict arrest if such structure is not visible to law enforcement agents (Black 1989). Black suggests that there are settings in which law enforcement encounter "socially invisible" offenders, such as when ticketing parking offenders (1989:63). When police ticket vehicles for parking violations, the social characteristics of offenders are largely invisible. As a result, we would not expect that social characteristics of parking violators would predict arrest likelihood. Given this lack of social information, we would anticipate that legal factors and evidence, such as parking ordinances or an expired meter, would impact police response to these offenses. If the social characteristics of an offender are unknown, such as in cases in which law enforcement agents cannot ascertain the identify of an offender, Black suggests that legal context is a stronger predictor of arrest (1989).

The nature of the Internet can allow individuals to conceal identities, to be deceptive about social characteristics, and even to assume alternate identities. Offenders in these crimes may be "socially invisible" if investigators are never able to definitively identify offenders online. This leaves two crucial questions. First, does the social structure of Internet sex crimes against minors predict arrest? And second, do investigators have knowledge of the social structure of these cases? This study explores variations in arrest in cases of Internet sex crimes against minors using Black's theoretical formulations regarding the social structure of cases and the relation between victims and offenders.

If there are variations in the social structure of these cases (such as offender and victim characteristics) these social characteristics will be predictors of arrest and other law enforcement involvement if cases occurred in a similar legal context. However, the amount of social information available to law enforcement may vary independently across cases. For example, there may be cases in which the social status of the victim is known to law enforcement, but no offender information is available. As noted previously, Black suggests that legal and resource variables may also be more predictive of arrest than social factors if offenders are "socially invisible," (1989:63).

Current Study

The current study examines the impact of the Internet on law enforcement investigations of two specific child sex crimes: (1) sexual abuse and (2) child pornography. This study seeks to accomplish two primary goals. First, using a sample of cases in which law enforcement was unable to make an arrest, it identifies general categories of dilemmas, or problems encountered in these investigations. While the study does not provide an opportunity for comparisons between Internet sex crimes against minors and their conventional counterparts, it provides some context for examining both types of crime, with a focus on those committed using an Internet-nexus.

A second goal of the study is to present a sociological analysis of arrest and other legal action in Internet sex crimes against minors. This analysis compares online child sex crime cases in which law enforcement agents made no arrest to cases in which an arrest was made. In addition, cases in which law enforcement conducted searches, seized computers, involved multiple jurisdictions, and generally had higher amounts of legal involvement are compared to cases without such legal action.

This study of law enforcement dilemmas in Internet sex crimes against minors provides valuable and currently unavailable insights. Police, child advocates, and policy makers can benefit from the results of this study. In addition, the investigation of obstacles to arrest in Internet sex crimes against minors using Black's theories makes a substantive contribution to the sociology of law.

The primary focus of this exploratory study is a sample of 68 Internet sex crimes against minors in which law enforcement agents were unable to make an arrest. The study categorizes various dilemmas in law enforcement investigations of these crimes. An analysis of these dilemmas provides a context for exploring the impact of the Internet on child sex crimes. The study also makes comparisons between cases in which no arrest was made and a larger data set (464) of Internet sex crimes against minors cases in which law enforcement was able to make an arrest. Using theories suggested by Black, the impact of sociological factors on law enforcement arrests and other legal involvement, such as searches and computer seizures, is investigated.

CHAPTER 1

LITERATURE REVIEW

Internet sex crimes against minors have only recently received attention as a social problem, and therefore, little literature exists on this subject. As there has been minimal previous research how the Internet-nexus impacts law enforcement investigation of sex crimes against minors, this literature review will draw on previous research in three areas.

First, the review will explore existing literature on conventional child sexual abuse and child pornography crimes to assess crime characteristics and challenges in law enforcement investigations of these crimes. Second, the study examines literature developed primarily for the criminal justice field, which suggests new aspects of sex crimes against minors created by the Internet. Third, using Black's sociology of law theories, the literature review will present the primary questions to be examined in this study of online child sexual abuse and child pornography crimes.

There is little empirical evidence regarding whether or not Internet sex crimes against minors can be considered computer-mediated versions of their conventional counterparts. In order to understand the dilemmas inherent in Internet sex crimes against minors, a review of the dilemmas in conventional child sex crimes is warranted.

Conventional Child Sexual Abuse Crimes: Law Enforcement Dilemmas

There may be child sexual abuse crimes in which law enforcement agents are able to conduct straightforward investigations with minimal complications. For example, imagine a hypothetical case where a woman enters her home, finds her 45-year old husband sexually assaulting the neighbor's 10-year old daughter, and calls the police. Imagine that the crime occurred in a state where the age of consent is 16 and that the key investigator in the case had received extensive training in child sexual abuse intervention.

In that scenario, law enforcement investigators have an investigative advantage. The age difference between the victim and offender, the setting in which the crime occurred, the legal statutes, and the key investigator's specialized training could all be assets in building the case. In reality, law enforcement investigators rarely have all of these investigative advantages in child sexual abuse investigations.

This is due to the nature of these investigations and these specific crimes. Crimes that are considered child sexual abuse involve two key features. Accepted definitions of child sex abuse require "sexual activities involving a child" and an abusive condition; such as a significant age difference, a power differential, or coercion (Finkelhor 1994:33). These two features, sexual activity and the presence of an abusive condition cover a wide range of child sex crimes. For example, a stranger may sexually assault a child once or a family member could lower the inhibitions of several children (grooming) to engage in sexual acts over an extended period of time.

In his overview of research examining the overall prevalence of child sexual abuse, Finkelhor finds that estimates of child sexual abuse vary according to sampling methods, definitions used, sample size and other factors (1994). There is evidence that not all child sexual abuse cases come to the attention of law enforcement (Finkelhor and Ormrod 2001) either due to variations in reporting mandates or underreporting of these crimes. In addition, although some attention has been given to the role of law enforcement in child sexual abuse cases (Humphreys 1996; Maguire 1993) there is little empirical evidence regarding law enforcement dilemmas in these investigations.

The sociology of law would suggest that factors including victim and offender characteristics might impact legal outcomes in these crimes. In addition to these social factors, the legal context of the case may affect law enforcement's ability to investigate these crimes.

Victim and offender characteristics

Victim and offender characteristics can be expected to vary significantly in child sexual abuse crimes, but there is little evidence regarding the impact of those differences on law enforcement investigations. It can be assumed that although all child sexual abuse involves a juvenile victim and an adult offender, specific victim and offender characteristics, as well as the nature of the offender/victim relationship vary.

Victim characteristics. Victims of child sexual abuse who come to law enforcement attention are likely to reflect those reported in the general child sexual abuse literature. Children between the ages of seven and twelve are most vulnerable in these crimes, and girls are more likely to be victimized than boys (Finkelhor 1993). The age of victims can create dilemmas for law enforcement investigations, since specific investigative techniques, such as child sexual abuse interviews, may be more challenging with very young victims. Likewise, law enforcement investigations could be complicated if there is a suspicion that a male victim has experienced child sexual abuse, but the child is hesitant to disclose the abuse. There is some evidence that a significant number of young children and male victims experience child sexual abuse, but that these crimes are not as apt to be reported (Barnett, Miller-Perrin, and Perrin 1997).

Offender characteristics. Law enforcement investigations of child sexual abuse can also be influenced by offender characteristics. For example, although the majority of child sexual abuse perpetrators are adult males (Barnett et al. 1997), there is growing recognition that these offenders can also be juveniles (Ryan and Lane 1991).

Victim/offender relationships. In investigating these crimes, law enforcement must also evaluate the relationship between the victim and offender. Existing research on child sexual abuse suggests that offenders are generally known to child victims (Barnett et al. 1997). Offenders in these crimes may be family members, friends, or acquaintances of child victims. This may lead to dilemmas in investigation of these crimes, if for example, a child sexually abused by a family member has been threatened and warned not to talk to police. In cases where victims and offenders are strangers prior to a child sex crime, investigators must identify and locate the perpetrator.

Law enforcement investigations may be complicated by the dynamics of these victim/offender relationships as well. Some child victims of sexual assault who have been groomed by offenders could be convinced that what is happening to them must be kept secret (Barnett et al. 1997). In some child sexual abuse crimes, there may be power or authority differentials between victims and offenders that could impact children's willingness to disclose abuse to law enforcement investigators.

Legal context factors

Training and Collaboration. In light of these challenges, specific skills and resources may be required for investigating child sexual abuse crimes. Identifying offenders, interviewing child victims, and collecting evidence in these crimes can be challenging, and specialized child sex crime training of law enforcement investigators is becoming routine (Lanning 1992). The emergence of multidisciplinary child sexual abuse investigation teams can mitigate some of these challenges. Teams consisting of law enforcement agents, child protective service workers, and other professionals have been developed in an effort to streamline investigations of child sexual abuse (Smith 1989). One key feature of these multidisciplinary teams is that they attempt to avoid revictimization of children through the re-living of the event, by coordinating child interviews and investigative efforts.

Evidence. This multi-agency coordination can be crucial, in particular if the child victim is the only witness to the crime. The general absence of witnesses in child sexual abuse crimes contributes to an overarching dilemma, which is that there is often little evidence available to law enforcement. Since these crimes generally occur in private, sexual abuse investigations typically involve the word of a child against the word of an adult. There may be little evidence to corroborate a child's report, and relying on a child's testimony can raise additional challenges. For instance, Lanning suggests that some children may or may not sense that certain types of touch or contact are "wrong," and that children are not always believed when they report being sexually abused (1992).

Statutes and legal history. Even in cases where children provide “credible” accounts of sexual abuse, legal definitions of child sexual abuse vary widely. Determining what constitutes sexual activity, as well as whether or not there was an abusive aspect to the crime can prove a difficult task for law enforcement (Lanning 1992). Hugging, kissing, and other forms of contact can be appropriate expressions of affection between adults and children. Law enforcement must be able to determine whether or not such contact is “sexual” or “abusive” on a case-by-case basis.

In conclusion, when a child sexual abuse crime is reported to police, the ensuing process can be complicated. While there is little literature available on this topic, there is some indication that victim and offender characteristics, legal issues, and the availability of resources can create dilemmas in law enforcement investigations of these crimes. Child pornography crimes, discussed in the following section, share many features of child sexual abuse, but may also present unique dilemmas.

Conventional Child Pornography Crimes: Law Enforcement Dilemmas

The problem of child pornography was thought to have been minimized prior to the emergence of the Internet. The availability of child pornography had declined due to legal actions and statutory revisions (Jenkins 2001). Nevertheless, dilemmas exist in conventional child pornography investigations, and therefore law enforcement investigations of conventional child pornography may or may not progress smoothly.

Imagine a scenario in which a police officer pulls an adult male over for a traffic violation and notices child pornography on the front seat of the car. The image depicts the same adult, sexually abusing a female child who appears to be six years old. Law enforcement investigators learn that this individual had already sold copies of this image to others and that the child depicted in the image was the offender's niece.

Several features of this hypothetical crime would facilitate law enforcement investigation. First, the image clearly depicted a minor, who police were able to identify and contact. Second, the offender was an adult with an existing relationship with the victim. Finally, the responding officer found the offender in possession of the produced images. While there is little evidence regarding dilemmas in child pornography investigations by law enforcement, there is reason to believe that this hypothetical example is not the norm. This is likely due in part to the nature of these crimes, as well as characteristics of victim and offenders, legal factors, and resources available to law enforcement agencies.

A primary similarity between child sexual abuse and child pornography crimes is that both involve a child victim and an aversive sexual act. In some situations, sexual abusers of children photograph or videotape this sexual abuse. Although images recording child sexual abuse are considered child pornography crimes, these images may not always feature sexual abuse of children by adults. They may depict actual or simulated sexual activities or sexually graphic images of children (Klain, Davies, and Hicks 2001).

In any discussion of child pornography, a key legal distinction is between two general categories of child-related material, child pornography and child erotica. Child pornography includes photographs and films of conduct that is sexually explicit (Klain et al. 2001) and that "requires a child to be victimized" (Lanning 1992:25). These images may depict graphic sexual abuses of children, or they may be sexually suggestive and not show any specific sexual activity (Schuijer and Rossen 1992).

Child erotica does not depict graphic sexual images of children, and unlike child pornography, the production, possession and distribution of child erotica is not generally considered criminal behavior (Lanning 1992). For example, images of teen models wearing revealing outfits and posed in sexually suggestive positions do not generally fall under child pornography laws (Brunker 2002). An ongoing debate involves whether or not child erotica should be considered illegal material. Lanning suggests that child erotica encompasses a broader range of interest in children, and may include games, books, and other material about children (1992).

This literature review will focus on child pornography rather than child erotica. Child pornography crimes can be generally organized into three categories: 1) production, 2) possession, and 3) distribution of child pornography. Offenders in child pornography *production* crimes take indecent photos of or videotape children being sexually abused or in sexually suggestive poses (Edwards 2000; Klain et al. 2001). Producers of child pornography may create images for private collections, to trade with other offenders, or for commercial distribution (Klain et al.). Production of child pornography most closely reflects child sexual abuse, in that an offender interacts with a minor victim and produces a graphic image.

Possession of child pornography does not necessarily involve producing these images. Child pornography possessors may possess images they produce or images they obtain from others. These individuals may use this child pornography to validate their sexual interest in children, to groom children and lower their inhibitions, or to blackmail victims or other offenders (Klain et al. 2001; Tyler and Stone 1983). Others may be motivated to collect child pornography out of curiosity, for sexual arousal, or for other reasons.

Distribution of child pornography involves the dissemination or trading of child pornography images (Klain et al. 2001). As with collectors, distributors of child pornography may or may not be producers. An individual may distribute images produced using actual victims, or may trade images collected from others. These images may be distributed to other offenders or to child victims. Individuals involved in distributing child pornography may or may not be interested in profiting financially from distribution of these images (Klain et al.).

Production, possession, and distribution of child pornography crimes all involve unique components. A primary challenge for law enforcement is that investigations of child pornography may involve one, two, or all three of these child pornography crimes. A suspect may be found with a collection of illegal indecent images of children, with no evidence of production or distribution of child pornography. Another offender may sexually abuse a child, create a permanent record of that sexual abuse by videotaping the crime, and exchange the video with other offenders in exchange for additional videos. A number of features impact law enforcement investigations of these crimes and may present dilemmas.

Victim and offender characteristics

Victim characteristics. Identifying and locating victims in child pornography crimes can be difficult for law enforcement agencies (Whitcomb and Eastin 1998). In 1992, Schuijer & Rossen suggested several dilemmas involved in identifying child pornography victims . For example, the victims may be unrecognizable due to the passage of time or the content of the images (such as the absence of the face) (Schuijer and Rossen). Even if identifying features can be noted in child pornography, the child victims may or may not live in the United States (Tyler and Stone 1983). It may also be difficult to ascertain the age of child victims in images.

Offender characteristics. Characteristics of child pornography offenders can also pose challenges to law enforcement. There is little empirical evidence regarding distinctions between child pornography producers, distributors, and collectors. Some suggest that offenders who sexually abuse children often produce images of the child victims (Klain et al. 2001). Other offenders may have a specific sexual interest in children, be motivated by curiosity, or have an interest in making a profit from the images (Klain et al.). It is also possible that offenders who do not produce child pornography, but who are involved in possession or distribution of child pornography crimes may be more difficult to identify.

Victim/offender relationships. The range of offender motivations in child pornography crimes may lead to greater variation in the relationships between victims and offenders than is generally present in child sexual abuse crimes. In child sexual abuse crimes, victims and offenders must have some relationship or come into physical contact. This is true in child pornography production crimes, where there may be a close relationship between the victim and the offender. In distribution and possession of child pornography crimes, however, offenders may not actually interact with the child victims depicted in the images. It seems probable that this would complicate law enforcement investigations, since it may not be possible to link a specific offender with a child victim.

Whitcomb and Eastin suggest that there is a misconception, perhaps as a result of this ambiguous victim/offender relationship, that these crimes are "victimless" (1998:3). While child pornography production crimes generally involve an act of child sexual abuse, it could be contended that possession and distribution crimes involve more of a "secondary viewing" than actual commission of a crime. From that perspective, the distribution and possession of graphic images of many types of crime is a frequent if not banal reality of American life.

Law enforcement agencies, United States federal law, and many international organizations reject this perspective. Child pornography is generally recognized as a permanent record of child sexual abuse, and distribution of produced images is considered as a source of ongoing harm for child victims (Grasz and Pfaltzgraff 1998) This harm could result from at least two factors. First, each viewing of a child pornography image could be considered a victimization (Grasz and Pfaltzgraff), and second, often just the knowledge that an image has been produced is traumatic for victims (Itzin 1994) .

Legal context factors

Evidence and Training. Detection of child pornography crimes, especially crimes involving possession and distribution of images, can be difficult using traditional investigative techniques (Perez 1991). If a child victim reports that an offender took pictures during a child sexual abuse, for example, specialized training may assist law enforcement agents in collecting crime evidence including information on that offender. To investigate distribution and possession child pornography crimes, police may rely on undercover, or proactive investigations.

Undercover investigations of conventional child pornography crimes have been the topic of much debate (Perez 1991). Law enforcement agencies have used undercover operations to identify offenders who would otherwise not come to the attention of police. Some have objected to child pornography undercover "sting" operations, challenging that "they raise serious concerns about entrapment and protection of individual due process rights" (Perez 1991:237). The rationale behind these objections is that offenders would not purchase child pornography if law enforcement officials did not advertise or offer child pornography for sale. In general terms, entrapment occurs when an individual commits a criminal act as a direct result of law enforcement inducement (Perez). More specifically, it requires that an offender commit a crime that he or she was not predisposed to commit (United States Court of Appeals for the First Circuit 1998).

Historically, the United States Postal Inspection Service, the enforcement division of the U.S. Postal Service, has coordinated undercover child pornography investigations

(Klain et al. 2001). This method has not generally targeted producers of child pornography, but it has allowed Postal Inspectors to identify offenders who purchase child pornography (Perez 1991). In general, undercover investigators tend to be carefully selected and highly trained (Marx 1982). Being selected as a member of an undercover unit can bring "increased prestige and professional recognition" (Marx 1982:166). Marx notes that while undercover investigators used to work alone on highly classified assignments, contemporary undercover work is often done by task forces and specialized units.

Statutes and legal history. Regardless of whether offenders produce, distribute, or collect child pornography, law enforcement investigations must prove that images identified fit definitions of child pornography. This is not always an easy task, as there are variations in statute and ongoing legal debates regarding definitions of child pornography that can impact arrest and other legal actions.

Elements of child pornography can lead to challenges in defining these crimes. For example, there is little disagreement that a produced image of an adult sexually penetrating a six-year-old child should be considered a "crime" of child pornography. It is also clear that one family photo album image of an infant bathing in the sink is not child pornography. However, the range of images between these two extremes has generated widespread debate (Grasz and Pfaltzgraff 1998) and even images of bathing infants could be considered child pornography in the context of an entire collection.

United States federal law includes in its definition of child pornography photographs and films of conduct that are sexually explicit (Klain et al. 2001). The clearest legal guides for defining child pornography are based on the premise that child pornography images present a "lascivious exhibition of the genitals" (Grasz and Pfaltzgraff 1998:621). A more specific legal definition requires consideration of five factors: whether the image 1) focuses on the child's genital area, 2) is sexually suggestive, 3) depicts the child in an unnatural pose, 4) includes an unclothed child, and 5) is designed to elicit a sexual response (Grasz and Pfaltzgraff). These factors need not all be present in order for an image to be classified as child pornography, but some contend that they should be taken into consideration (Grasz and Pfaltzgraff).

Grasz & Pfaltzgraff (1998) suggest that the legal history of child pornography can be divided into two periods, pre and post 1982. Prior to 1982, the major concern of the United States Supreme Court was children's access to obscene material. The Supreme Court ruled that children's access to obscene material could be restricted and developed guidelines for such material. These guidelines, known as the *Miller* test, focused in part on community standards for obscene materials, and did not directly address the issue of child pornography (Grasz and Pfaltzgraff).

During the 1982 United States Supreme Court case *New York v. Ferber,* it was ruled that the *Miller* test needed modification in order to apply to cases of child pornography (Grasz and Pfaltzgraff 1998). This ruling was based on a number of issues, and perhaps the most frequently cited of these was a ruling that child pornography depicts an image of child sexual exploitation and abuse (Grasz and Pfaltzgraff). The Supreme Court action made it clear that distribution or possession of child pornography was not constitutionally protected under the First Amendment (Grasz and Pfaltzgraff; Whitcomb and Eastin 1998).

A range of factors can impact law enforcement investigations of conventional child pornography crimes, as well as child sexual abuse crimes. Victims and offenders in these investigations may be difficult to identify or locate. Both types of child sex crimes have been confronted with legal and resource challenges. With the emergence of the Internet, online variations of these two crimes have come to law enforcement attention.

New Aspects of Internet Sex Crimes Against Minors

It is clear that child sexual abuse and child pornography are crimes, regardless of whether they occur with or without a computer nexus. However, there are some clear distinctions regarding the commission of Internet sex crimes against minors. The relative anonymity and privacy of Internet use, the speed of electronic transmissions, the elimination of geographic barriers to communication, and other specific qualities distinguish online interactions. In addition, youth currently use the Internet more than any other age group (U.S. Department of Commerce 2002). The United States Department of Commerce (2002) estimates that three-quarters of 14 to 17 year olds and 65% of 10-13 year olds use the Internet.

Therefore, this examination of conventional child sexual abuse and child pornography crimes raises at least three questions regarding the similarities and differences between on and offline sex crimes against minors. First, in what ways are minors victimized online? Second, how has an Internet-nexus impacted law enforcement effectiveness? And finally, do existing sociological theories apply to the legal response to these crimes?

Internet victimization of minors

In terms of Internet sex crimes against minors, the impact of the computer nexus on children has been largely overlooked. On and off line, children are generally vulnerable to the same crimes as adults, but are also victimized in ways that are related to their childhood status (Finkelhor and Hashima 2001). For example, both child and adult victims may have property stolen or destroyed. However, research over the past twenty years has demonstrated that children are also victimized in ways that are related to their age and dependent status (Finkelhor and Hashima). Child sexual abuse, for example, is a criminal victimization related to childhood status. Both children and adults can be victims of sex crimes; non-consensual sexual contact between adults is generally considered a criminal sexual assault. However, child sexual abuse is specific to childhood. Due to the minor status of children, all sexual contact between children and adults is a crime, regardless of perceptions of whether or not such contact was "consensual."

Children as well as adults can be victims of computer-related crimes, such as exposure to computer viruses and harassment. However, there is increasing law enforcement concern regarding the two categories of online child victimization addressed in this study. First, there are concerns that children are vulnerable to sexual exploitation initiated or facilitated by the Internet (Aftab 2000). Second, there are indications, such as reports of increased availability of child pornography via the Internet, which suggest that this technology has created new opportunities for criminal activity and has generally led to a resurgence in child pornography trade (Jenkins 2001; Stanley 2001).

Impact on law enforcement effectiveness

Discussions regarding whether or not online child sexual abuse and online child pornography crimes are "different" from their conventional counterparts reflects a larger debate regarding computer crime in general. A key question is whether the emergence of computers and the Internet as tools for social interaction have opened up new avenues for child and adult victimization. Some suggest that the Internet provides offenders with increased opportunities to commit crime (Stanley 2001) and that many computer crimes go undetected (Collier and Spaul 1992). According to this perspective, a computer-nexus may allow some people to offend who might never have offended without the Internet. Alternatively, others claim that a computer nexus does not necessarily mean increased opportunity, since many "computer crimes," could have been committed with or without computer (Wasik 1991).

Law enforcement agencies investigate Internet sex crimes against minors using both traditional and undercover investigations. Police are generally involved in one of these two types of work, either *reactive* police work initiated by citizens, or *proactive* police work, in which police "initiate encounters on their own authority" (Black 1980:86). Most of the existing literature regarding arrest and other outcomes of law enforcement actions deals with reactive, or citizen-initiated cases. Online child sexual abuse and child pornography crimes may come to the attention of police through citizen reports, or can be initiated by police themselves.

Reactive, or citizen-initiated criminal investigations are brought to police attention in a number of ways. Police may respond to the site of a robbery, be dispatched to a domestic assault, or receive a call from a hospital about a stabbing victim. In reactive cases, an investigation could come to the attention of law enforcement by the victim, a suspect, or by a witness or other third party to the crime.

In Internet sex crimes against minors, a citizen-initiated case may be called in to police when a parent notifies law enforcement that a person met on the Internet sexually abused a child. Family members might notice child pornography on a computer and report seeing the images to law enforcement. In these citizen-initiated cases, an investigation begins once the public brings a case to police attention. In some citizen-initiated cases, such as those in which an adult sexually solicits a child online, law enforcement agents may take on some undercover persona (such as the child who received the sexual solicitation).

Alternatively, law enforcement agencies may elect to conduct proactive investigations of certain crimes. In Internet sex crimes against minors investigated using proactive, police-initiated methods, law enforcement agents generally use two distinct approaches (Klain et al. 2001). First, as a modification of conventional undercover child pornography investigations, law enforcement investigators may literally go "undercover," impersonating either juvenile victims or consumers interested in child pornography (Douglas 2002). Online child pornography investigations may involve an investigator taking on the role of a child pornography collector interested in trading images, or infiltrating a child pornography bulletin board service. Second, law enforcement investigators may actively patrol the Internet, posing as juveniles in online chat rooms (Douglas).

Law enforcement's ability to conduct proactive investigations of sex crimes against minors deserves note. While undercover work in child pornography crimes has been relatively common, undercover investigations of child sexual abuse appear to have emerged only as a result of computer technology. Prior to the emergence of the Internet, it was not possible for law enforcement agents to "go undercover" as children in an effort to identify child sexual abuse offenders.

These undercover investigations of Internet sex crimes against minors may require specific resources, including computers for electronic communication, personnel to work online, training in online investigations, and digital technology for tracking suspects. Whether or not these online undercover investigations differ from conventional undercover work is difficult to ascertain. While law enforcement agencies are understandably cautious about exposing specific undercover approaches, the available literature suggests that in most ways, investigative skills used in these cases are similar to conventional undercover work (Perez 1991). Police officers involved in both undercover narcotics and child pornography investigations, for example, may identify a suspect who is suspected of purchasing illegal substances, and use a sting operation to develop a case against that suspect.

On the other hand, offenders in Internet sex crimes against minors may not be organized in the same way as organized crime or drug offenders, which may pose dilemmas for law enforcement agencies. In undercover investigations of organized crime and drugs, law enforcement often focuses attention on low-level offenders tied in with a larger criminal structure (Jenkins 2001). The same may not be true for online child sex crime offenders. For example, child pornography offenders do not typically work in such large networks (Jenkins). While there have been numerous crackdowns on large circles of child pornography dealers (the Wonderland Club and others), some believe that these groups do not include the majority of offenders (Jenkins).

Media reports suggest that a growing number of law enforcement agencies are initiating undercover investigations of Internet sex crimes against minors. Undercover investigations of Internet sex crimes against minors can be highly technical, and often require specialized training and computer expertise. The Office of Juvenile Justice and Delinquency Prevention has awarded a number of grants to support the development of Internet Crimes Against Children (ICAC) Task Forces across the United States (Douglas

2002). These ICAC Task Forces were developed to coordinate investigations of Internet sex crimes against minors, as well as to provide resources including training for other agencies and community education (Medaris and Girouard 2002).

Law enforcement agencies' ability to make arrests vary, whether online child sex crime investigations are police-initiated or initiated by citizens. Media accounts highlight cases in which offenders are arrested for large online child pornography collections, some of which contain images of the offenders engaged in sexual acts with children (Messing et al. 2001). At the same time, publications by the U.S. Department of Justice imply that making these arrests is not always as clear-cut as these media accounts suggest (U.S. Department of Justice 2000).

Crimes involving online child sexual abuse and online child pornography are relatively new phenomena, and there is little research examining law enforcement dilemmas in these crimes. What literature does exist is primarily in the form of government documents and manuals for law enforcement professionals. The majority of this literature focuses on the legal and resource dilemmas in online child sex crime investigations, with little emphasis on dilemmas related to sociological variables in these crimes.

Applicability of sociological theories

Internet sex crimes against minors have yet to be investigated using any specific sociological theory, and Donald Black's sociology of law provides a compelling context for this examination. As noted previously, the sociology of law assumes that social factors lead to variation in response to crime (Baumgartner 2001). The sociology of law contends that any crime is impacted by legal factors, but that if those legal factors are held constant, social variables are more likely to predict arrest and other responses to crime. The relatively recent emergence of these crimes, the lack of information regarding arrest in Internet sex crimes against minors, and Black's sociological questions call for an initial exploration of the relationship between social and legal variables in these investigations. Black suggests that the relation between victim and offender social characteristics can lead to variation in legal response (1989). At least six types of relations between victim and offender social characteristics addressed may impact Internet sex crimes against minors.

Victim/offender age. Black's propositions suggest that children have less law than adults, and that crimes between minors are less likely to lead to legal action (1976). This view contends that since children and young people are more often subject to social control by families, they would be subject to less law enforcement effort (Howerton 2002).

If Black's propositions hold in Internet sex crimes against minors, we would expect less police involvement in cases between minors. Such cases would be seen as less legally serious, and therefore less apt to attract legal attention. Alternatively, police may assume that there are limits to parental control on the Internet, and take cases between minors as seriously as those involving adult offenders and minor victims.

Victim/offender race: Black finds that law enforcement involvement ranks from high to low according to the relation between victim and offender race (1976). Legal involvement in cases are expected to rank from high to low in the following order: 1) cases in which the victim is White and the offender is some other race, 2) cases involving White victims and White offenders, 3) cases in which both the offender and victim were non-White, and 4) cases in which the victim was non-White and the offender was White. In short, police are most likely to be involved in cases in which the victim is White and the offender is another race and are least likely to be involved in cases in which the offender is White and the victim is another race.

Victim/offender gender. While Black's theories do not explicitly address the relation between legal actions and victim or offender gender, others have examined gender and social structure and found gender differences in criminal court outcomes (Daly 1999). If more legal attention is directed at female victims, gender may be related to outcomes in Internet sex crimes against minors. Alternatively, it may be that victim gender does not predict legal actions in these cases.

Victim-Offender Respectability. The application of Black's theories regarding victim and offender respectability to Internet sex crimes against minors is unclear. Offenders and victims with prior criminal histories may be less socially integrated, or respectable, than individuals without such history (Black 1976). Black hypothesizes that "Law varies inversely with the respectability of the offender" (1976:117). It appears that an offender's criminal history, including prior offenses, can create a "self-fulfilling prophesy" (Farrell and Swigert 1999:389). If this theory holds true in Internet sex crimes against minors, we would expect that arrest is *more* likely if the suspect has a prior record or criminal history and *less* likely if there is no evidence of any previous criminal charges.

Victim respectability, including victim prior arrest record and history of running away may also impact law enforcement response to crime. If victims are found to have prior criminal records, police are less likely to investigate cases very thoroughly (Cooney

1999). According to this perspective, victims' claims can be impacted by deviant behaviors on the part of the victim (Cooney 1999).

This may make overall police involvement as well as arrest less likely. In fact it may be that in online child sex crime investigation, arrest likelihood actually decreases with diminished victim respectability, such as in cases where victims have criminal records or a history of running away.

Alternatively, it may be that respectability is not a predictor of arrest in these crimes. Internet sex crimes against minors may lead to such ambiguities that offender and victim respectability is unclear. If law enforcement agents are unable to narrow down the identity of an individual distributing child pornography, for example, prior arrest records and other measures of respectability will be unavailable.

Victim-Offender Relationship (Relational Distance). The victim/offender relationship, or relational distance, has also been noted as a predictor of legal response. Black (1989) suggests that cases involving intimates will be subject to less law than those involving strangers and that "the greater the relational distance between a complainant and a suspect, the greater the likelihood of arrest" (1980:104). If victims and offenders are intimate, this suggests that law enforcement is less likely to get involved than in cases where the parties are strangers. Relational distance can impact case outcome not only at arrest, but also at other stages in the criminal justice process. In his analysis of homicides, Lundsgaarde (1999) found that individual found to have killed strangers were more likely to receive severe punishment than those who killed family members.

Relational distance in Internet sex crimes against minors may impact arrest in at least three ways. First, if Black's theory holds true in Internet sex crimes against minors, we could expect, for example, that arrest is *most* likely in sexual abuse crimes with a computer nexus if victims and offenders have no prior relationship, and therefore are at a great relational distance. In other words, we would expect that cases in which a victim and offender are not intimates or family members would be *more* likely to end in arrest than cases in which a family member uses the Internet during the commission of an online child sex crime.

A second possibility, however, is that Black's theory will not apply in these crimes, and that arrest is actually *less* likely if victims and offenders have no prior relationship. It is conceivable that in some Internet crimes, the victim and offender may have no offline relationship, have one meeting at which a sexual assault occurs, and have no future contact. In this scenario, the offender may be a literal stranger to the child victim, making future identification and arrest unlikely. As noted previously, "strangers" is used here to describe victims and offenders with no prior offline relationship, although minors may not consider people met online as "strangers."

A third option is that the nature of the Internet results in missing social information, and therefore, the social structure of a crime, including "relational distance" is impossible to ascertain. This is likely the case, for example, in some online child pornography crimes. It is likely that identifying an actual "victim/offender relationship" is only possible in child pornography production crimes. Any "relationship" between offenders and child victims in the images is more likely to be ambiguous in online child pornography possession or distribution crimes.

Victim/offender income (Vertical direction). Black (1976) suggests that vertical direction (the relation between victim and offender social status) can impact law. This view contends that law is applied according to a predictable hierarchy of victim/offender social status combinations and results in a specific pattern of law enforcement involvement from high to low legal activity. Black (1989) predicts that legal response varies in the following order: (1) most likely in crimes involving high status victims and low status offenders (*upward* crimes), (2) followed by crimes in which both parties are high status (*lateral* crimes), (3) then low status victims and low status offenders (*lateral* crimes), and (4) the least amount of law enforcement involvement is predicted in crimes with high status offenders and low status victims (*downward* crimes). In short, if a homeless individual is accused of a crime against high-income business executive, the crime is more likely to result in legal intervention than if the same high status individual commits a crime against a person of lower social standing. Reports are more likely to be given law enforcement attention if they are what Cooney calls "big cases" (1999:188). Cases with high status victims may be given higher priority than other cases.

If Black's theory applies in Internet sex crimes against minors, we would expect that Internet sex crimes against minors involving victims of high social status and offenders of low social status are more likely to end in arrest than those involving high status offenders and low status victims. Alternatively, it may be there is little variability among victims and offenders in these crimes. The computer nexus may essentially level the vertical direction playing field. Finally, there may also be ambiguity in terms of vertical direction in Internet sex crimes against minors. It is possible that social status information is missing in these crimes, perhaps because victims and offenders are deceptive about education, occupation, income, or other measures of social status.

This analysis will explore possible views of Black's propositions regarding the social context of Internet sex crimes against minors. Each of the preceding social measures (*victim/offender age, race, gender, respectability, relational distance, and vertical direction)* will be assessed as potential predictors of legal involvement in these cases. Primarily, the study explores the relationship between the social structure of these cases and arrest in Internet sex crimes against minors. In addition to arrest, the study examines four other measures of legal involvement: (1) law enforcement search, (2) computer seizure, (3) multiple agency involvement, and (4) overall legal involvement.

At this time, it is unclear how these social characteristics impact legal involvement in Internet sex crimes against minors. As noted earlier, Black's frame predicts that social factors will only predict law enforcement involvement in these crimes if the legal context is held constant. Three potential legal context factors are the strength of evidence in these cases, investigator training, and whether or not an offender can be identified.

Much of the evidence in Internet sex crimes against minors is collected through a computer forensic lab (Hames 1994). In addition, investigations of Internet-related crimes involving juvenile victims require specific training (U.S. Department of Justice 2000) and a "careful and systematic analysis of the forensic evidence" (Hames 1994:201). Forensic science has been defined as "the application of science to law-any scientific principle or technique that can be applied to identifying, recovering, reconstruction, or analyzing evidence during a criminal investigation" (Casey 2000:3). In Internet-facilitated crimes involving juvenile online sexual victimization, computer forensics may be used to produce evidence including recovered email messages, a duplicate copy of a website containing illegal material, a replica of a file of collected images, or a summary of a suspect's Internet browsing history.

It is important to note that the collection and examination of evidence is only useful to law enforcement agents if there are specific state and Federal statutes criminalizing Internet sex crimes against minors. Statutes related to Internet child pornography, online solicitation, and other online offenses vary from state to state. Laws regarding child sex crimes have changed in some ways as a result of the Internet.

Historically, legal systems have adapted to address changing social relations, which are influenced by technological advances (Bartlett 1981). A primary example of these shifts occurred in response to the development of the railroad in the United States. As railroad development progressed, law evolved to regulate the technology. While some existing laws applied to the railroad, new laws were needed for newly created problems, such as assigning fault in cases of injury (Bartlett) and protecting railroad passengers from vandalism, assault, and other crimes (Schulz 1987). Specialized "railroad police" were trained to address safety issues resulting from this technological advancement (Schulz).

Specialized Internet crimes against children investigators generally have basic training in computer forensic examinations, working with digital evidence, and other Internet-specific factors. Law enforcement interest in Internet sex crimes against minors crimes may be reflective of a more general public concern regarding the use of the Internet by child molesters and pedophiles (Whitcomb and Eastin 1998). Police departments often create specialized units to address emerging social problems as a "way to signify that a department is doing something about those problems" (Mastrofski

2000:433). The “railroad police” emerged in a time when there was increasing societal concern regarding railroad safety. Internet Crimes Against Children Task Forces evolved to address concerns regarding online child sex crime.

Legal scholars have opened a debate regarding whether or not existing laws and traditional police interventions can address these changes. Some reviews of existing state and federal statutes suggest that existing law sufficiently addresses these crimes (Cobb 1996; Grasz and Pfaltzgraff 1998). Others suggest that there are serious limitations to the coverage of the law (Brown 2002). This is a debate that is likely to continue for some time.

Internet Crimes Against Identified Victims: Law Enforcement Dilemmas

Whether or not there are significant differences between online child sexual abuse and conventional child sexual abuse is difficult to determine (Brown 2001a). For example, a *Newsweek* story in March 2001 warned that using the Internet, sexual predators "could enter a home, introduce themselves to a teenage child, and carry on a long process of seduction" (Norland and Bartholet 2001:46). This type of scenario may or may not occur in conventional child sexual abuse crimes. It is conceivable that a stranger could enter an adolescent's life in this way, although it seems less likely to occur offline.

Few clear definitions exist regarding the categories of crimes committed against juveniles using the Internet. A range of crimes including child sexual abuse could be included in this discussion. Crimes in which offenders lure and victimize minors met online, those in which the Internet is used to lower children's inhibitions (grooming), and online solicitation crimes may fall into this general category.

To reflect this wide range of online sex crimes, Wolak, Mitchell and Finkelhor (2003a) characterize these crimes as Internet Crimes Against Identified Victims (I-CIV). Clear estimates regarding how often Internet crimes against identified victims crimes occur are currently emerging (Wolak et al. 2003a). Research suggests that approximately one in five youth (10-17 years) experience a sexual solicitation while online in a one year timeframe (Finkelhor, Mitchell, and Wolak 2000) and media accounts imply that some of these online sexual solicitations lead to real-world sexual abuse. However, how often these online solicitations develop into actual meetings between children and adults or criminal sexual acts is uncertain.

As in conventional child sexual abuse crimes, there may be some Internet crimes against identified victims in which law enforcement investigators face relatively few dilemmas. Again, imagine a hypothetical scenario in which a fourteen-year-old girl tells her mother that a 56-year-old man she met on the Internet sexually assaulted her earlier in the day. Assume that the girl met the man in a teen oriented chat room, and that he told her he wanted to be friends. The offender picked the girl up from school, took her to his house in a nearby town, and sexually abused her. The girl agrees to cooperate with the investigation and remembers where the man lives. Imagine that the mother calls the police, and an investigator who is a member of the State's Internet Crimes Against Children Task Force is one of the initial responders. This investigator searches the offender's computer for evidence and is able to retrieve email communication between the victim and offender that corroborates the victim's account.

Under these circumstances, law enforcement could potentially develop a strong case against the 56-year-old suspect. The victim's age and cooperation, the Internet communication as evidence, the lack of jurisdictional complications, and the responding officer's training could all facilitate the law enforcement investigation and ultimate arrest of the offender.

Given the nature of these investigations and the characteristics of these crimes, however, law enforcement may not always have these investigative advantages. The outcome of the case above could have been different if the victim in the crime described above was 17, was in love with the offender, or refused to cooperate with law enforcement investigators. Similarly, if law enforcement was unable to identify the offender, or if the investigator had no training in computer forensics, there may have been significant dilemmas.

First, victim and offender actions, such as consensual sexual activity and deceptions by offenders and/or victims can pose problems. Second, legal factors, perhaps most notably jurisdictional issues in cases where victims and offenders live in different states or countries, can be challenging. Finally, not all law enforcement agencies have the resources required to capitalize on digital evidence or to engage in undercover investigations of these crimes.

The sociology of law assumes that although all of these factors lead to variation in law enforcement response to Internet crimes against identified victims, the sociological features may be most salient. While Black's theories, in particular those related to arrest, were developed well before the emergence of Internet crimes against identified victims (1980), they provide a context for examining these and other dilemmas associated with arrest in these crimes.

Victim and offender characteristics

There is no clear evidence at this time that victims or offenders of Internet crimes against identified victims crimes differ from those involved in conventional crimes. In fact, there is little empirical evidence regarding the characteristics of victims or offenders in online juvenile sexual exploitation. Mitchell, Finkelhor, and Wolak (2001) interviewed fifteen hundred youth and identified "vulnerable" victims (composite of negative life events scale, physical and sexual assault history, and depression) who were more likely to receive a sexual solicitation online. However, no child in that study had actually been sexually assaulted as a result of the online sexual solicitation (Mitchell et al.).

What literature exists regarding law enforcement dilemmas in these crimes addresses legal and resource issues, and makes little note of the impact of victim and/or offender social characteristics (U.S. Department of Justice 2000). Given this reality, this review will highlight what seem to be the most likely law enforcement dilemmas regarding Internet crimes against identified victims, with particular emphasis on dilemmas related to social characteristics. Black's theories regarding relational distance, respectability, and vertical direction provide a useful context for examining victim and offender characteristics in these crimes.

Relational distance. Issues of relational distance may present dilemmas for law enforcement investigators in these crimes. Due to the nature of the Internet, it may be that Internet crimes against identified victims are more likely to involve individuals who are initially strangers than conventional child sexual abuse crimes, which may create some challenges during investigation. It is possible that in offline child sexual abuse cases, children are more likely to be victimized by family members, acquaintances, and adults who live in their own community and are perhaps easier to identify and contact. Media reports suggest that the Internet provides a forum for initial child/adult meetings that would not have occurred in the offline world (Norland and Bartholet 2001), and so online crimes may involve victims and offenders who are relative strangers. This could present problems, for example, if victims of Internet crimes against identified victims are unable to provide investigators with offender's names or true identities.

There may be additional differences between on and offline child sexual abuse crimes. Online crimes may be less likely to involve the use of physical intimidation, or issues of power or authority over their child victims. In offline child sexual abuse crimes, offenders may be teachers, religious leaders, or older family members. Relationships that child victims develop with adults online may not have these same power or authority differentials. In some ways, this may actually facilitate investigations, if child victims are less fearful about the consequences of disclosing sexual abuse.

A notable feature of victim/offender "relationships" in both on and offline child sexual abuse crimes is grooming. Adults may use grooming, or attempts to lower children's inhibitions, in on and offline sexual exploitation crimes. Grooming may include efforts to build trust, deceiving children, providing gifts, or fulfilling children's needs (Brown 2001a). It is difficult to say whether online grooming poses specific investigative challenges for law enforcement agencies. Both on and offline child sexual abuse involve some form of interaction between a child victim and an adult offender and typically involve a seduction or grooming process (Brown 2001a). Internet crimes against identified victims crimes generally involve the same grooming rituals and methods of reducing children's inhibitions prior to sexual exploitation as conventional child sexual abuse crimes (Brown 2001a).

Some suggest that the Internet has changed the nature of the grooming process by shortening the amount of time it takes for offenders to build trust with children (Brown 2001a). While no empirical evidence currently exists to investigate this claim, anecdotal evidence suggests that there is significant variation in the amount of time involved in grooming children for sexual abuse on and offline. Offenders in offline child sexual abuse cases may groom children for years or may entice children at an initial meeting. In a similar fashion, it is likely that the online grooming process may involve long-term electronic communication in some cases and almost none in others.

The issue of online grooming ties into the ambiguous nature of relationships in Internet crimes against identified victims. A child may meet an adult online, develop a relationship, and agree to meet the person, only to be sexually abused at the meeting. Are the victim and offender relationally close or distant? On one hand, we may be able to assume that most offenders develop these online relationships as a form of grooming toward future sexual exploitation. From this perspective, the relationship itself is a criminal act. On the other hand, Lanning (1998:17) states "By no reasonable definition can an individual with whom a child has regularly communicated online for months be called a 'stranger.'" It may be that although juveniles view these adults as intimates, law enforcement investigators see these relationships as criminal.

Respectability of victims and offenders. The nature of these online relationships may tie into respectability of victims and offenders. It may be that law enforcement investigators view child sexual predators, particularly those who seek out children online, with little respect. Additionally, it may be that issues such as prior arrest history, particularly for sexual offences, impact perceptions of respect.

The Internet can allow opportunities for offenders to be deceptive about intentions, personal history, and even their true identities. Turkle (1995) suggests that the Internet allows individuals to try out multiple identities and selves. Some offenders may be exploring alternative identities online, and others modify personal information in an effort to deceive juvenile victims. In either case, it may be difficult for law enforcement agencies to determine who offenders are, and whether or not they have prior criminal records. In an undercover investigation, for example, a law enforcement investigator may pose online as a female child and receive a sexual solicitation in a chat room. If the suspect in the investigation suggests an immediate face-to-face meeting, investigators may only know the information posted on the suspect's Internet Service Provider (ISP) profile, which may or may not be accurate. In other words, police may not know the name or any other information about the person that they hope to arrest.

There is little evidence regarding "respectability" of child victims, although it may be that as with offenders, victim characteristics, including prior arrest record influence case outcomes. It may also be possible that victims' acknowledgement of consensual sexual activity affects police evaluations of a crime. The possibility that some child sex crimes involve *"compliant victims"* has recently received attention in the child abuse literature and is likely to be the subject of much debate and policy analysis (Berliner 2002:3). Child victims in Internet crimes against identified victims may or may not be different from conventional child sexual abuse victims in terms of consensual activity. Lanning (1998:18) states that victims in Internet crimes against identified victims crimes can be "curious, rebellious, or troubled adolescents seeking sexual information or contact." In these crimes, it may be that victims refuse to cooperate or present evidence, perhaps because they are in love with offenders, or feel compelled to protect their identity.

This perspective seems to imply that consensual behavior by victims makes statutory criminal activity less serious, and perhaps less likely to lead to arrest or other legal consequences. As noted earlier, law enforcement agents may interpret legal statutes literally, and disregard whether or not these juveniles, who are minors according to state law, consented to sexual activity with adults.

Vertical direction. In addition to issues of relational distance and respectability, the sociology of law suggests that arrest varies with vertical direction. Although there is little evidence regarding vertical direction in Internet crimes against identified victims crimes, it is likely that Internet crimes against identified victims crimes involve victims and offenders at higher levels of socioeconomic status than conventional child sexual abuse crimes. This may create dilemmas for law enforcement investigators, such as if offenders have top of the line computer equipment, have an education in computer science, or are able to use high social standing to their advantage.

Legal context factors

Evidence & Training. A primary dilemma in these crimes relates to evidence collection. Strength of evidence consistently appears as a strong predictor of arrest in general (Mastrofski 2000; Mastrofski, Worden, and Snipes 1995) and cases with stronger evidence are more likely to end in arrest than cases with limited evidence (Black 1980). Many online child sex crime investigations rely on digital information, which can provide valuable evidence (Hardy and Kreston 2002). Digital evidence may include email communications, information provided by Internet Service Providers, and evidence obtained during computer forensic examinations. This evidence may be easily accessible to law enforcement, or it may be deleted, hidden, or encrypted (scrambled) and need to be retrieved using computer forensics (Hardy and Kreston). It is likely that in some cases, this digital evidence provides concrete evidence, such as pictures or explicit requests often lacking in conventional child sexual abuse investigations.

This digital evidence can also create challenges for law enforcement, since collection of such evidence requires specific training, and the interpretation of digital evidence can be complicated and generally involves technical terms and sophisticated computer experience (Hardy and Kreston 2002). Evidence collected using computer forensics needs to be clearly explained to prosecutors, a jury, or others who will assess its value (Hardy and Kreston).

Statutes and legal history. Internet sex crimes against minors are generally seen as a threat to children's safety, although there are debates regarding what constitutes an online sex crime against a minor. For example, is it a crime to ask a child to engage in sexual acts online? Is it criminal to talk about sex, have Cybersex, or sexually harass minors on the Internet? While sexually assaulting a child met online is clearly a crime, there is currently no consensus regarding which of these other online actions can be considered criminal. In some jurisdictions, it is illegal for an adult to have sexually explicit communications with minors, and in others, the same act is not a crime.

This statutory diversity is just one factor that creates dilemmas in multi-jurisdictional investigations of Internet sex crimes against minors. Investigators may need to assess whether one state's statute applies in a case, or whether some federal jurisdiction could more appropriately address the specific act. It may be, for example, that a state's statute prohibits interstate travel to sexually solicit a minor, but online sexual solicitation is not considered criminal. Obviously, arrest is more likely if specific acts are considered criminal by one or more jurisdictions involved in a case.

Some existing child sex crime legislation applies in online investigations, and other laws have evolved to address unique features of these crimes. For example, investigators can generally determine where a crime took place in conventional sex crimes against minors. The nature of the Internet may make it more difficult to establish venue, such as in cases in which an offender sexually solicited a minor victim online, and then traveled to meet the minor for sex. In such a case, it may not be clear "where" the sex crimes occurred, which can complicate legislation regarding and prosecution of Internet crimes against identified victims (Cobb 1996). Cobb suggests that these crimes can be considered using two federal statutes that apply to other sexual abuse crimes that involve crossing state lines. The White Slave Traffic Act addresses issues of coercion and enticement of minors and the Continuing Offense Statute provides for establishing case venue in multi-jurisdictional cases (Cobb). In 1996, Cobb suggested that in terms of existing federal laws, "old law is still good law" (p. 553).

Some new law has also evolved to address this issue. In 1994, it became a federal crime to cross state/national borders to "engage in a sexual act with a juvenile" (Whitcomb and Eastin 1998:1). This law more specifically targets features of Internet sex crimes against minors in that it makes it illegal to induce children under the age of consent (which varies by state) to cross state or national lines for sexual acts. In 1998, the Protection of Children from Sexual Predators Act was passed, which prohibited the use of a computer to transmit sexual information about a minor (under age 16) .

Entrapment. Undercover, or proactive online investigations of child sexual abuse investigations have raised legal dilemmas about entrapment. For instance, an offender charged with indecent solicitation of a child claimed that since he was actually communicating with an undercover officer, he did not actually solicit a minor (Chicago Daily Law Bulletin 2002).

Proactive investigations of Internet crimes against identified victims generally involve undercover investigators posing as child victims online in sexually explicit chat rooms, communicating with potential suspects, and waiting to see if suspects suggest a meeting. Should a meeting be arranged, law enforcement agents may arrest the offender at the pre-determined meeting place. Law enforcement officials note that suspects are typically "found" located in chat rooms or bulletin boards dedicated to sexual exploitation of children (Douglas 2002). Investigators who work these crimes contend that these cases should not be considered as cases of entrapment. Online undercover investigators must wait to see if a suspect sexually solicits the "child" or attempts to set up a meeting.

Douglas quotes undercover investigator Jim McLaughlin as stating that entrapment requires that as a police officer, "you have to urge or persuade someone to do something they're not otherwise predisposed to do to create an interest that wouldn't otherwise be there" (2002:82) . McLaughlin suggests that in proactive undercover investigations, an offender's sexual interest in children exists prior to law enforcement involvement (Douglas).

Victim and offender characteristics, as well as legal and resource issues present dilemmas in law enforcement investigations of Internet crimes against identified victims crimes. Online child pornography investigations share some of these dilemmas, and others are unique to those crimes.

Internet Child Pornography Crimes: Law Enforcement Dilemmas

Law enforcement agencies have been investigating child pornography crimes since the mid-seventies and until the emergence of the Internet, it was believed that police were a step ahead of child pornography offenders (Jenkins 2001). While there have been few empirical attempts to quantify the amount of child pornography on the Internet, there is a general consensus that the Internet has increased the accessibility and availability of this material (Biegel 2001; Jenkins; Wolak, Mitchell, and Wells 2002).

Online sources for child pornography include UseNet Newsgroups, Bulletin Board Systems (BBS), Internet Relay Chat (ICR), and the World Wide Web (www) (Taylor, Quayle, and Holland 2001). These sources provide opportunities for posting produced images of child pornography, downloading images for collections, and distributing images to others. Some suggest that posting images online is basically the same as distributing, since others can easily retrieve images and save them (Biegel 2001).

Some law enforcement investigations of online child pornography may proceed with few complications. For example, imagine that a computer repair shop notifies law enforcement that they have found child pornography on a computer under repair. Law enforcement investigators seize the computer and do a complete forensic examination. They learn that the owner of the computer is a 56-year-old male and interview the suspect. During the forensic examination, over 1,000 images of child pornography are found, including several images of the suspect sexually abusing a seven-year-old child. These images have been saved on the suspect's hard drive. During the investigation, police learn that the seven-year-old child lives next door to the suspect.

Law enforcement investigators' ability to identify a victim, to seize and search the offender's computer, and to perform a forensic examination would likely facilitate this investigation. Obviously, other online child pornography cases may present significant dilemmas. First, it may be difficult for law enforcement investigators to identify children depicted in electronic child pornography images. These children may be physically located anywhere in the United States or across the globe. Second, it may not always be clear who the offender truly is, especially if multiple users share a computer. Even if offenders are identified, variations in state statutes may make it difficult to move ahead with these cases. Finally, seizing and searching computers generally requires specific investigatory skills and expertise.

Victim and offender characteristics

Victim characteristic. Researchers involved with the Combating Paedophile Information Networks in Europe have provided some evidence regarding the characteristics of children appearing in online child pornography (Taylor et al. 2001). Their database of 800,000 still images and more than 400 video clips consisted of close to equal numbers of male and female victims (Taylor et al.). Taylor and colleagues found that most of the online child pornography in their database consisted of a series of children in a specific narrative or theme. Once an image of a child is found online, law enforcement investigators may attempt to locate and identify child victims, but as with offline child pornography, finding victims can be challenging. However, as noted previously, victims are rarely contacted in child pornography possession crimes (Schuijer and Rossen 1992; Whitcomb and Eastin 1998).

Offenders. There is some agreement that the Internet has made child pornography available to a wider range of offenders (Jenkins 2001; Norland and Bartholet 2001). There are no definite estimates regarding how many people use the Internet to look at images of child pornography, but there is evidence that the Internet has led to a growth in "collectors" of child pornography (Taylor et al. 2001). Challenges related to identifying offenders in online child pornography crimes may vary according to the type of crime. For example, offenders in production crimes may appear in the images, facilitating identification and subsequent arrest. However, it is likely that law enforcement investigators could run into challenges when attempting to identify distributors and collectors of online child pornography. Clearly, initial detection of these crimes is complicated by the fact that individuals can post, access, download, and save images of child pornography from a private computer.

Victim/offender relationship. The nature of victim and offender relationships can also complicate online investigations of these crimes. If a law enforcement agency finds a collection of images on a suspect's home computer, they may or may not be able to determine where the images came from. Images found by law enforcement may have been produced by the individual under investigation, obtained electronically from another person, or scanned into electronic form from existing photographs. In some production crimes, offenders may appear in images with child victims, but without an actual image of the offender, it is likely difficult to ascertain who produced the images. In terms of possession and distribution crimes, the concept of *relational distance* could be ambiguous. If an offender downloads a large number of child pornography images and saves them to his hard drive, does he have any specific "relationship" with those victims?

As is the case with conventional child pornography crimes, offenders could possess graphic photos of children they have never met.

Respectability of offenders. Once law enforcement agents are able to identify suspects in online child pornography crimes, issues of respectability may come into play. For example, it may be that an offender suspected of distributing child pornography over the Internet has a prior conviction for child sexual abuse. However, until an offender is identified, these issues cannot be considered.

Vertical direction between victims and offenders. There is no evidence to suggest that social status, or vertical direction between victims and offenders, is a predictor of law enforcement involvement in online child pornography crimes. In part, this could be due to the inherent difficulty in identifying children depicted in these images. If investigators cannot locate child victims, differences in social status of parties involved cannot be ascertained. In this sense, it is possible that the Internet minimizes the impact of vertical direction.

Legal context factors

Although these victim and offender characteristics may present dilemmas for law enforcement, it is likely that legal and resource factors also present significant obstacles. For instance, whether or not a law enforcement agency has the resources to collect forensic computer evidence or has anyone trained in computer crime investigation could impact arrest likelihood.

Evidence & Training. Collecting evidence in online child pornography crimes can require specific skills and technology. As with conventional child pornography crimes, computer investigations of child pornography cases often yield graphic sexual images of children. Some suggest that although online child pornography is "indecent and obscene material," it provides tangible evidence for law enforcement (Hames 1994:200). Hames (1994:200) suggests that the images should be seen as "high-grade forensic evidence of crime," which "offers the opportunity to identify the victims as well as the perpetrator(s)."

In cases in which offenders are reported to "possess" images of child pornography on a computer, images may be deleted by the time law enforcement investigators examine the computer. Computer forensics experts with specific training may be able to locate files that have been deleted, and in most cases deleted information can be retrieved and used as evidence (Hardy and Kreston 2002). Once images are located, investigators must be able to identify the age of victims in the photos, which may require expert testimony by medical experts.

The United States government has only recently begun work on a centralized national database of child pornography images (Caruso 2003), and Hames (1994) suggests that this can be problematic for law enforcement. Hames states that the lack of a centralized database in the United States leads to a situation with "literally thousands of images of children in abusive situations stored away in police files," with no possibility for further action or identification (p. 203).

Statutes and legal history: Legal rulings and statutes can also present dilemmas for law enforcement agencies. Two major legislative modifications for regarding the legal definitions of online child pornography occurred in 1996 and 2002. In 1996, the Child Pornography Prevention Act (CPPA) modified existing law to include, among other things, child pornography stored, or *produced* using electronic means (Whitcomb and Eastin 1998). Prior to this time, there was no federal statute that applied directly to Internet-facilitated child pornography.

Brown suggests that legislation is lacking when it comes to "virtual," or computer generated child pornography (2002). Computer technology makes it possible to create images that look like child pornography, but that are actually computer generated or composite images. For example, computer technology can be used to superimpose children's faces on adult bodies. Whether or not it is legal to produce, possess, or distribute virtual child pornography has raised First Amendment issues and legal battles (Norland and Bartholet 2001).

In a landmark 2002 case, the Supreme Court ruled that "virtual" images of child pornography could not be considered criminal under the CPPA (Brown 2002). The ruling in this case, Ashcroft v. the Free Speech, stated that "virtual" images of child pornography were a "legal and logical alternative to actual child pornography" (Brown 2002:1). This Supreme Court decision in 2002 ruled that virtual child pornography created entirely using computer graphics, with no actual children, is protected under the First Amendment (Brown 2002).

This ruling had major implications for law enforcement and prosecutors, who are responsible for proving that children in child pornography images are "real." It may be that with advances in computer technology, police and prosecutors may not be able to discern which images are real and which are 'virtual' (Taylor 2001). This ruling is still under debate (McCullagh 2003).

Taken individually, the challenges to law enforcement investigations of online child pornography crimes presented here may seem inconsequential. However, it is possible, if not probable, that these problems create serious limitations in law enforcement investigations of these crimes. The proposed study will provide an opportunity to examine law enforcement challenges in online child sex crime investigations.

CHAPTER 2

METHODOLOGY

The primary goal of this study is to examine specific law enforcement dilemmas in 68 Internet Sex Crimes Against Minors (ISCAM) cases in which no offender was arrested. In addition, the study compares this sample of 68 cases in which no arrest was made to a larger sample of 464 cases in which law enforcement agents made an arrest. This analysis is in two sections. First, qualitative case summaries are examined to identify sub-samples of cases and specific categories of dilemmas in Internet sex crimes against minors. Second, using propositions suggested by Donald Black (1976; 1998) the study explores a series of hypotheses regarding the impact of social and legal factors on arrest in these cases. As has been done in previous studies of arrest, offender characteristics, victim characteristics and other factors are be compared for cases in which there was an arrest and cases in which no arrest was made (Felson and Ackerman 2001; Howerton 2002; Novak, Frank, Smith, and Engel 2002).

Research Design

The research project involves analysis of data collected as a component of the Crimes against Children Research Center's National Juvenile Online Victimization Study (N-JOV). N-JOV was sponsored by the National Center for Missing and Exploited Children (NCMEC) and the United States Department of Justice, and was administered by the Crimes against Children Research Center at the University of New Hampshire. The primary objective of the N-JOV study was to capture incident estimates of Internet sex crimes against minors coming to the attention of law enforcement in a one-year time frame. A secondary goal of N-JOV was to identify dilemmas in law enforcement investigations of these crimes. Please see the National Juvenile Online Victimization Study Methodology Report for a more detailed summary of N-JOV methodology (Wolak, Mitchell, and Finkelhor 2003b).

N-JOV collected detailed case information regarding Internet sex crimes against minors in which an arrest was made by a law enforcement agency, as well as in cases in which no arrest was made by any law enforcement agency. Cases in which an offender was arrested between July 1, 2000 and June 30, 2000 are classified here as N-JOV cases. Cases in which no law enforcement agency made an arrest are identified here as OBSTACLES cases.

By definition, cases in the OBSTACLES sample did not end in an arrest. Therefore, those cases may not have involved substantiated criminal activities or "offenders" in a criminal sense. For convenience, both N-JOV and OBSTACLES cases may be called "crimes" instead of "investigations" in this analysis and the term "offender" may be used instead of "suspect" in some analyses.

Data Collection and Procedures

The N-JOV project used a two-phase data collection process. In Phase 1, a mail survey was sent to a national sample of county, state and federal law enforcement agencies asking if they had investigated cases of Internet-related child pornography or sexual exploitation cases between July 1, 2000 and June 30, 2001. Agency directors or chiefs of police from the sample of law enforcement agencies were asked to provide case numbers and investigator names for three types of cases:

- ANY ARRESTS in cases involving the attempted or completed sexual exploitation of a minor and at least one of the following:
  a) the offender and the victim first met on the Internet
  b) the offender committed a sexual offense against the victim on the Internet, regardless of whether or not they first met online.
- ANY ARREST in cases involving the possession, distribution, or production of child pornography and at least one of the following:
  a) Illegal images were found on the hard drive of a computer or on removable media (e.g., CDs or disks) possessed by the offender
  b) The offender used the Internet to order or sell child pornography
  c) There was other evidence that illegal images were downloaded from the Internet or distributed by the offender over the Internet
- Any significant Internet-related child pornography or sexual exploitation cases in which you were unable to make an arrest because of technical, legal, evidentiary or other obstacles? (By significant cases, we mean investigations in which your agency invested considerable energy and resources.)

In Phase 2 of the data collection process, interviewers conducted telephone interviews with law enforcement investigators about a sample of the cases reported in the mail survey. Six trained interviewers telephoned specified investigators at agencies with cases and collected data using a standardized instrument. Interviewers recorded answers on paper copies of the survey instrument and typed case summaries in Microsoft Word for each case. Rather than using Computer Assisted Telephone interviewing, the interviewers used pencil and paper data collection so that they could use discretion in determining which sections of the survey to use and the order in which questions were asked. The N-JOV data collection instrument included nine sections and the OBSTACLES study used an additional section (see Appendix A). The telephone survey sections are as follows:

- The *Preliminary* section was used to determine whether cases were eligible for the study. In addition, this section collected initial case, offender, and victim characteristics. Victim data were only collected if a case involved an "identified" victim, or a victim who law enforcement agents located and contacted. Offender data were collected in all cases. In cases with multiple victims or multiple offenders, this section was used to determine a primary offender and a primary victim. For additional information on how interviewers identified primary victims and offenders see the N-JOV methodology report (Wolak et al. 2003b).
- The *Sexual Exploitation: Online Meeting* section was only used in cases where a victim identified by law enforcement met an offender on the Internet. It includes questions regarding online correspondence, meetings, and any illegal sexual activity (ranging from non-contact activities to sexual intercourse or penetration).
- The *Sexual Exploitation: Prior Face-to-Face Relationship* section was used if a case involved identified victim and the victim and offender did not meet on the Internet. These cases will be referred to as "family and prior acquaintance" cases. This section also collected information about

online correspondence, actual meetings, and illegal sexual activities between the victim and offender. If a case involved an identified victim, interviewers either used this section or the previous section.

- The *Production of Child Pornography* section was used when an identified victim was a victim of child pornography production. This section was used if the law enforcement investigator stated that an offender created images of an identified victim in a sexually suggestive or explicit pose. This section collected information including the number of images produced, the format of those images, and any distribution of the produced child pornography.
- The *Possession of Child Pornography* section was used if the law enforcement investigator said that the offender possessed child pornography. This section also collected information including the number of images produced, the format of those images, and any distribution of the produced child pornography.
- The *Undercover Investigation* section was used if law enforcement investigators 1) posed online as minors or adults with access to minors, 2) took over identities of identified victims, or 3) posed as distributors or consumers of child pornography. The questions in this section address online correspondence between undercover investigators and offenders, the nature of the online investigation, and collect information about face-to-face meetings between offenders and investigators, if such a meeting occurred.

- The *Offender* section captured a range of offender information, including family, employment, mental health, criminal history, and other characteristics of offenders. In the N-JOV cases, this section also collected information on arrests, charges and outcomes of criminal cases.
- The *Victim* section was used if law enforcement investigators were able to identify (locate and contact) a specific minor victim. The section includes questions related to family, employment, mental health, criminal history, and other characteristics of victims. If information was collected about a victim using this survey section, that case was considered to have an *identified* victim in an Internet-related investigation.
- The *Interview Conclusion* was used at the end of every interview. This section collected information about the law enforcement investigators' training, and provided an opportunity for investigators to share any other case information not covered in the survey.
- The *OBSTACLES* section (Appendix A) collected information on specific problems encountered during law enforcement investigations of these cases.

Maintaining confidentiality was a priority in this project. All interviewers and others involved in the project signed agreements to comply with Federal data collection protocols. Names of agencies or investigators collected during the interview process will not appear in any published or presented material. The University of New Hampshire's Institutional Review Board has approved confidentiality procedures for this project and access to data for this investigator (see attached approval letter in Appendix B).

This dissertation will primarily focus on the third category of cases noted previously, cases in which no arrest was made by any law enforcement agency. The author was one of the six interviewers on the initial N-JOV project and developed the OBSTACLES survey section. The author completed 57% of the OBSTACLES interviews, and two research assistants from the N-JOV project completed the remaining 43%. The author and one of the N-JOV principal research investigators reviewed all completed OBSTACLES interviews.

Study Population and Sample

Sample Selection

The Phase 1 mail survey was sent to a national sample of 2,574 law enforcement agencies. The initial stratified sample included three frames in order to collect information from agencies specializing in these crimes, those with training in these investigations, and from a random sample of all United States law enforcement agencies.

The first frame consisted of 79 specialized agencies charged with investigating Internet sex crimes against minors, including 30* federally funded Internet Crimes Against Children (ICAC) Task Forces and 43 federally funded ICAC satellites that were in operation when the sample was developed. Eighty-three percent of the 75 ICAC Task Forces and satellite agencies completed and returned

* One of the ICAC Task Forces included three agencies from three different states. Each agency was surveyed individually.

surveys and 64% reported one or more cases involving Internet sex crimes against minors.

The second frame consisted of law enforcement agencies in which some staff attended training in Internet sex crimes against minors. Those trained agencies were identified using lists of agencies participating in training conducted by two training organizations, SEARCH and the National Center for Missing and Exploited Children. Half of the 1,668 agencies identified in the second frame were randomly selected to participate in the study. One additional agency in a large metropolitan area was added to the sample; this assured that agencies from all major metropolitan areas in the United States were included in the sample. Ninety-three percent of the eligible trained agencies returned mail surveys, and 27% reported one or more cases involving Internet sex crimes against minors.

The third frame consisted of 13,586 other local, county and state law enforcement agencies across the United States. This sample was drawn using a database available through the National Directory of Criminal Justice Data (National Directory of Law Enforcement Administrators 2001). First and second frame agencies were cross-referenced with those in the third frame to avoid duplication in the final sample. Twelve percent of the third frame agencies were selected to participate. Of the eligible agencies, 86% completed and returned mail surveys, and 7% reported one or more Internet sex crimes against minors cases.

sampling strategy may mean that cases involving identified victims are over-represented in the OBSTACLES sample.

Second, some cases were considered ineligible if they did not fit within the study parameters. These cases were excluded if the investigation in the original mail survey did not have an Internet-nexus, if the case ended in an arrest by some other jurisdiction, if the case was not within the specified timeline, or if the reporting agency did not do any actual investigation (21%).

A third issue is that once the final sample was selected some interviews could not be completed. As a result, no information could be collected 52% (n=74) of the cases in the OBSTACLES sample. No interview was completed in cases in which law enforcement investigators were unable to complete an interview, law enforcement investigators could not be contacted, or no case could be identified. Some of the original mail surveys did not provide case numbers for law enforcement investigations in which no arrest was made, and identifying cases was problematic in many of those instances. Time restraints of some respondents limited their ability to complete more than one interview. Law enforcement investigators were not interviewed more than once if they were unable to complete a second interview. Eight agents were interviewed on two cases in which they were key law enforcement investigators. In addition, some cases reported here were duplicates (8%). Five cases were reported twice in the OBSTACLES section of the original mail survey, and six cases were duplicates from the N-JOV study.

As a result of these factors, it is possible that the cases included here may not be representative of the entire sample of OBSTACLES cases reported by law enforcement investigators. This study makes no attempt to develop incidence estimates of cases in which no arrest is made in an Internet sex crime against a minor. Despite these case selection issues, there is no reason to expect that the dilemmas reported by these investigators are different than those presented by the cases excluded from this study.

The initial N-JOV sample included 1, 115 cases in which the law enforcement agency reported a case in which an arrest was made in the study's timeframe. About 55% of those cases were included in the sample (n=615). Interviews were completed in 480 (78%) of those initial 615 cases. The N-JOV sample included sixteen duplicate interviews, leaving a final total of 464 completed interviews (Table 1).

Table 1: Responses to OBSTACLES and N-JOV Telephone Interviews

Number of...	OBSTACLES	N-JOV	Total
Cases reported in mail surveys	**200[a] (100%)**	**1,115**	**1,315**
- Cases not selected for sample	16 (8%)	264 (24%)	280
- Ineligible cases*	42 (21%)	236 (21%)	278
Number of cases in sample	142	615	757
Cases in sample but not completed			
- Non-responders** and refusals	63 (31%)	108 (18%)	171
- Other (duplicate *** and invalid cases)	11 (6%)	27 (4%)	38
Completed Interviews (percent of cases in sample)	68 (34%)	480 (78%)	548
Duplicate cases deleted****	0	16	16
Final Number	68	464[b]	532

Note: Percentages may not add to 100 because of rounding

* Cases did not meet eligibility requirements of the study. (Includes cases in which arrest did not occur in the timeframe of the study, no Internet-nexus, and arrests made by some other jurisdiction)

** Could not schedule interviews for various reasons

*** Interviewers realized these were duplicate cases and did not conduct interviews

**** Cases were determined to be duplicates after interviews were completed.

[a] Includes N-JOV cases which did not end in an arrest

[b] The N-JOV methodology also included data collected from two participating federal law enforcement agencies. Those federal cases are not included in the analyses presented here, as the two federal agencies were not asked to provide data on cases in which no arrest was made. Therefore, all subsequent analyses reflect a sub-sample of N-JOV cases excluding those identified by the two federal agencies. For additional information on those cases see the National Juvenile Online Victimization Study Methodology Report (Wolak et al. 2003b).

Measurement

The unit of analysis for this research is the individual law enforcement case. It is possible that some agencies reported more than one case in the study time frame. Therefore, individual cases may be nested within departmental units.

Whether or not victim and offender characteristics are available for analysis varied by case type. For example, child pornography possession cases did not typically involve *identified* victims (victims identified and contacted by law enforcement) and so characteristics of the victim were generally not available for analysis. Therefore, social information may be minimal in many cases. In addition, the dilemmas in some of these cases may make it difficult for law enforcement agents to ascertain age, race, and other social characteristics of some offenders.

Treatment of missing data was a consideration in these analyses, since law enforcement investigators did not always have comprehensive information on cases in which no arrest was made. In fact, no case record was available on some of these OBSTACLES cases, and therefore some law enforcement investigators relied upon memory and case recall in some of these interviews. Missing data was also a problem in some N-JOV cases. Data were either missing because law enforcement agents did not know the answer to a question or because interviewers should have, but did not ask some specific question.

Missing data were treated using the following approach:

- Frequencies were run for all variables to assess the percentage of missing data for N-JOV and OBSTACLES cases. Particular attention was directed at the

OBSTACLES cases, which were generally missing data due to the nature of those investigations.

- If more than five percent of data were missing on any one OBSTACLES variable, dummy variables were created to compare missing data with known responses. The dummy variables were included in subsequent bivariate analyses to check for statistically significant differences between the missing and known data.
- Missing data relationships that were found to be statistically significant in bivariate analyses were included in multivariate analyses to control for the influence of missing data.

Dependent variables

Five dependent variables were examined here. Each of these factors was expected to measure the amount of legal action in a case. Those variables included arrest, search, seizure, multiple agency involvement, and overall police involvement. There were no missing data in any of the dependent variables.

Arrest. Arrest was measured using the final case outcome. If no arrest was made by any law enforcement agency, the case was coded as 0, and if an arrest was made, the case was coded as 1. As a note, this coding corresponds with the study in which the interview was completed. Data on cases in which an arrest was made were collected in the N-JOV study, and data on the non-arrest cases were collected in the OBSTACLES study.

Search. Whether or not law enforcement investigators conducted a search was measured using the question "Was a search conducted?" with yes coded as 1 and no coded as 0.

Seizure. Whether or not any computer equipment was seized was measured using the question "Was any computer equipment seized or handed over?" with yes coded as 1 and no coded as 0.

Multiple jurisdictions involved. Whether or not multiple law enforcement jurisdictions were involved was measured using the question "Were any other law enforcement agencies involved with this case?" with yes coded as 1 and no coded as 0.

Law enforcement involvement. Exploratory factor analyses were conducted to assess whether a latent construct, law enforcement involvement, emerged from the data. Based on this data, it appears that arrest, search, and seizure of a computer are all measures of the amount of police involvement in a case. Therefore, it is not surprising to find moderate to high correlations between arrest and both search (Pearson Correlation =.54, p=. 000) and seizure (Pearson Correlation .460, p= .000) in these cases. The number of law enforcement agencies involved does not appear to contribute to the total police involvement. The involvement of multiple jurisdictions was not related to arrest, but was weakly correlated with both search (Pearson Correlation = .156, p= .000) and seizure (Pearson Correlation =.174, p= .000).

Arrest, search, and computer seizure all contributed to a factor score for law enforcement involvement. The resulting component explains 72% of the combined variance between these variables. Including the measures of multiple agency involvement into the factor analysis lowered the variance explained to 54%. Therefore, the multiple agency variable was not included in the final factor score exploration.

The distribution of this factor score variable (*legal involvement*) had a severe negative skew (skew = -2.21). The minimum factor score for legal involvement was minus 3.1 and the maximum was positive .45. Approximately 79% of the scores (N=422) were positive. Sixty of the 68 OBSTACLES cases appear as outliers in this distribution, as they uniformly involved less police involvement (mean of -2.00) than the N-JOV cases in which an arrest was made (mean of .2947). As expected, this difference in mean police involvement between OBSTACLES and N-JOV cases was statistically significant (t=16.35, df=71, p= .000).

Attempts to normalize the *legal involvement* variable were unsuccessful. Therefore, the original police involvement score was dichotomized for use in the subsequent analyses into cases with high and low police involvement. Cases with negative factor scores were coded as low police involvement and those with positive factor scores were coded as high legal involvement. Twenty-one percent (N=110) of the cases received low legal involvement, and 79% (N=422) received high involvement.

Law enforcement involvement may be a misnomer in that police may have been heavily "involved" in an investigation, but still may be unable to conduct a search, seize a computer, or make an arrest. This may be particularly true in undercover investigations, in which investigators may track offenders for significant amounts of time, but never have enough evidence to make offline contact with the suspect.

Independent variables

The primary independent variables examined here will be drawn from the sociology of law, with emphasis on Black's (1976) frame.

Victim-Offender Age. The variable *Victim/offender age* was recoded from continuous measures of age to identify cases with adult offenders. Cases with an offender over 18 were coded as 1, and all other cases were coded as 0. All victims in these cases were minors, and therefore this variable is labeled *Offender Age* for the remainder of this analysis. Offender age was unknown in 32% of the OBSTACLES cases, and therefore dummy comparison variables will be examined in all analyses. It is hypothesized here that cases with minor offenders are less likely to attract legal attention.

Victim-Offender Race. The variable *victim/offender race* was recoded from initial victim and offender race variables to identify cases with white victims. Initially, investigators were asked whether victims and offenders were White, African-American, Asian, Native American, or some other race because of the small percentage of victims and offenders from minority groups. First, those variables were recoded into dichotomous variables: White and other race. Using those recoded variables, combinations of victim/offender race were collapsed into one variable. To examine race within Black's frame, cases were coded as follows: 1) the offender was other race and the victim was White, 2) if both offender and victim were White, 3) if both offender and victim were other race, and 4) if the offender was White and the victim was another race.

Due to the small number of cases with White victims and other race offenders (N=10), the race variable was dichotomized. The four categories noted above were collapsed, with 1 being those cases where the victim was White and 0 being those cases in which the victim was another race. Offenders may be white or some other race in either of these categories. For the remainder of this analysis, this variable is labeled *Victim race.* Victim race data were missing on less than 5% of cases. It is hypothesized here that cases with White victims are more likely to end in arrest or result in other legal involvement than cases in which the victim is not White.

Victim-Offender Gender. Those cases with female victims were coded as 1 and cases with male victims were coded as 0. This variable is labeled as *victim gender* for the remainder of this analysis. Victim gender data were available on all OBSTACLES cases. It is hypothesized here that police effort is greater with female victims.

Victim-Offender Respectability. The relation between victim and offender respectability was measured using four initial variables. Measures of victim respectability included whether or not the victim had run away from home in the past and whether or not the victim had a prior arrest history. According to Black's propositions (1976) law enforcement involvement of all types should be ranked from high to low in the following order: 1) the offender had a criminal history and the victim did not, 2) neither had any criminal history, 3) both had a criminal history, or 4) the offender had no criminal history and the victim did have a criminal history.

These categories were collapsed into a dichotomous variable, with 1 being those cases where the victims had no criminal or run away history and 0 being those cases in which the victim did have a criminal or run away history. In both categories, offenders may or may not have had a criminal history.

This variable is labeled *Victim Respectability* for the remainder of this analysis. Missing data for victim prior criminal history and victim history of running away exceeded 5%, and therefore dummy comparison variables were examined in subsequent analyses of victim respectability. Cases involving victims who could be seen as less socially respectable are expected to receive less law enforcement attention than those cases involving more legally respected victims (Black 1976).

Victim-Offender Relationship. A measure of relational distance was constructed using two measures of victim-offender relationship from the original instrument. No data were missing on these variables. In cases in which victims and offenders had a prior face-to-face relationship, investigators reported whether they were family members or acquaintances. Cases involving victims and offenders with a prior relationship were coded as "family/acquaintance relationships" (1). Cases involving online meetings in which victims had met offenders online were coded as "strangers" (0). Offenders in a few other cases in which identified victims were sent adult pornographic material, child pornography, or sexual solicitations (but did not meet in person) were also coded as "strangers" (0). In short, all cases in which the victim had no prior offline relationship with the offender were coded as "stranger" cases. This variable is labeled *relational distance* in the subsequent analyses. Although some of these victims may have developed relationships with the offenders online, the parties were "strangers" prior to the crime. It is hypothesized here that cases involving strangers are more likely to receive legal attention than cases in which victims and offenders had a prior relationship.

Vertical direction (Income of Victim and Offender). The relation between the income of the victim and the offender, or the vertical direction of the crime, was determined using measures of victim and offender income. Originally these questions asked law enforcement investigators to estimate victim/offender income using the following categories; 1) less than $20,000, 2) Over $20,000 to $50,000, 3) Over $50,000 to $80,000, 4) Over $80,000. Using initial income codes, a comparative variable was created. The categories are as follows: 1) cases in which the victim's household income was greater than that of the offender were coded as *upward* crimes; 2) those involving offenders with incomes higher than victims were coded as *downward* crimes; 3) and cases in which victim household and offender income were the same were coded as *lateral* crimes. Law enforcement effort in these cases is expected to rank from high to low in the order above, with the greatest amount of law in upward crimes. Therefore, this variable was dichotomized into upward crimes (1) and other crimes (0).

Data were missing on offender income in almost 65% of OBSTACLES cases, and therefore a missing income dummy variable will be included in subsequent statistical analyses.

Legal Context/Control Variables

Legal responses to Internet Sex Crimes Against Minors are expected to vary according to the social structural variables noted above. However, the data presented here may allow for limited exploration of Black's (1976) propositions. Black states that these social structural variables only predict arrest if incidents occur within similar legal environments and if other aspects of the social structure of the case are the same. Ideally, these propositions would be tested given cases with similar amounts of evidence, identical legal statutes, or uniformity in terms of witnesses or other third parties involved in the cases. In an effort to control for some variation in the legal context of these cases, several variables are examined as possible, but clearly imperfect substitutes. Four legal context factors: 1) proof that a crime occurred, 2) limited offender information, 3) reluctant or uncooperative victims, and 4) training in investigations of Internet sex crimes against minors were derived from the qualitative analysis of case summaries. Measures for these legal context factors are presented here and discussed in more detail in Chapter 4.

Proof issues. Law enforcement investigators identified several issues related to proving that a crime occurred, and measures for two of those factors are presented here. First, investigators noted difficulties related to defining child pornography, both in terms of the nature of images and the age of children depicted in those images.

Graphic nature of images. As a measure of the graphic nature of images, investigators were asked whether child pornography in both the production and possession cases included graphic sexual images, "images that focused on genitals or showed explicit sexual activity." Less than five percent of data were missing on these measures. Those cases involving any graphic images were coded as 1 and cases in which no graphic images were identified were coded as 0.

Age of children in images. The subsequent qualitative analysis finds that challenges related to the age of children in child pornography images. Law enforcement investigators were asked to identify specific age groups of children depicted in child pornography. This information was used as a measure of the age of children in these images. Investigators knew the age of children depicted in all cases, and therefore there were no missing data for this measure. Offenders who possessed some child pornography with images of children under 13 were coded as 1 and those who did not possess any such images were coded as 0.

Criminality of preparatory acts. A second proof issue related to the criminality of some *preparatory* acts, such as online sexual solicitation. It is argued here that cases in which victims and offenders never met in person and/or no illegal sexual activity occurred can be considered "preparatory acts." Law enforcement investigators were asked whether or not a meeting occurred between the victim and the offender in cases in which the parties met online. In online meeting cases as well as those in which the victim and the offender had a prior relationship, law enforcement investigators were asked whether "there was any illegal sexual activity between the victim and the offender." Illegal activity could have included the following kinds of acts: non-contact, inappropriate touching, fondling, oral sex, intercourse or other penetration, or some other type of illegal sexual activity. Cases in which investigators reported that there was a meeting or an illegal sexual act occurred were coded as 1, and cases in which no meeting or illegal sexual activity occurred, or "preparatory acts only" cases, were coded as 0. Data were missing on less than 5% of these variables.

Limited offender information. There is also variation in the amount of offender information available to law enforcement agents. In order to make comparisons between missing offender information in N-JOV and OBSTACLES cases, a proxy measure of "limited offender information" was constructed. This measure does not attempt to measure whether or not an offender was identified (although this is identified as a dilemma in OBSTACLES cases), but rather compares the amount of basic offender social information available to law enforcement investigators across OBSTACLES and N-JOV cases. Case-level data were examined to identify a subset of cases in which social information available on offenders was limited. If investigators were lacking ANY information about offender age, gender, race, and area in which the offender lives, it was assumed that the gap in social information would complicate arrest. Those cases were coded as (1) "offender information limited" cases, and other cases were coded as (0) "offender information available."

Reluctant or uncooperative victims. The subsequent qualitative analysis also suggests that reluctant or uncooperative victims can pose dilemmas. Three questions in the from the *Victim* section of the telephone instrument address this issue. First, investigators were asked whether the victim was "not at all cooperative, somewhat cooperative, very cooperative, or extremely cooperative" at the beginning of the investigation. Second, investigators were asked whether this cooperation changed, or whether the victim became more or less cooperative as the case progressed. If there had been a change in victim cooperation, investigators were asked about victim cooperation at the end of the investigation using the above categories.

A variable was created that indicated the victim's level of cooperation at the end of the investigation. This variable reflected victim cooperation at the start of the investigation if there had been no change, and victim cooperation at the end of the investigation if there had been some change. Law enforcement investigators' responses to were dichotomized to reflect victims who were either (1) very or extremely cooperative or (0) not at all or somewhat cooperative by the end of the investigation. Less than 5% of data were missing for this measure.

Training/Resources/Collaboration. The original measure asked investigators whether or not they had been able to receive any training in Internet sex crimes against minors. Those investigators who reported attending training were coded as 1 and those without training were coded as 0. Information regarding investigator training was not collected on about 16% of cases, and therefore dummy categorical measures are included in analyses to control for missing data.

Primary Research Questions

Qualitative case summary analysis:

The analysis of OBSTACLES qualitative case summary data involves one primary research question. *What are the primary dilemmas in law enforcement investigations of these crimes?* Dilemmas were primarily captured in the OBSTACLES section of the telephone survey, in which interviewers asked law enforcement investigators about particular problems that arose during the investigation.

Quantitative data analysis:

Black's theories (1976), and more generally the sociology of law suggest that the social structure of a case is determined in part by the relation of victim and offender characteristics. Therefore, only those cases in which a victim was identified and contacted by a law enforcement agency will be used in this study's quantitative analyses. Comparisons of cases in which an arrest was made and those in which no offender was arrested will be conducted using quantitative data from both OBSTACLES and N-JOV cases. This analysis will examine the following questions:

1. *Are cases involving adult offenders more likely to receive legal attention than cases with minor offenders?*
2. *Are cases involving white victims more likely to receive legal attention than other cases?*
3. *Are cases involving female victims more likely to receive legal attention than other cases?*
4. *Are cases involving less socially respectable victims (those with criminal or run away histories) more likely to receive legal attention than other cases?*
5. *Are cases involving strangers more likely to receive legal attention than cases in which victims and offenders are either family members or acquaintances?*
6. *Are cases involving upward vertical direction more likely to receive legal attention than cases involving downward or lateral vertical direction?*
7. *Are legal context variables, including production of graphic images, preparatory acts, limited offender data, victim cooperation, and investigator training statistically related to legal action taken in these cases?*

8. *Do patterns found in these bivariate analyses of sociological variables hold when legal context variables are added as controls in multivariate analyses?*

Data Analysis

Quantitative and qualitative data were compiled in these telephone interviews with law enforcement investigators. The primary focus of this dissertation is to examine the 68 Internet sex crime against minors cases in which no arrest was made, although a secondary analysis will compare OBSTACLES and N-JOV data.

An agency database for the OBSTACLES project was developed using FileMakerPro software, and reflects the structure of the N-JOV agency database. The agency database contains agency level data from the original N-JOV mail survey, and includes only those agencies that reported cases in which no arrest was made. Agency contact information, the number of non-arrest cases, the number of N-JOV cases, investigator names, case numbers and other agency level data were entered into this database. This database was used to produce call records for each case in the OBSTACLES sample and to update respondent contact information. Investigators were asked if they would like a copy of these results once the study is completed, and the FileMakerPro database will be used to create mail labels for the respondents who requested copies of results.

The overall data analysis will include three components. First, Chapter 3, presents a development of case types and a descriptive analysis of the cases in the OBSTACLES sample. Second, the qualitative results section involves a qualitative analysis examining law enforcement perceptions of barriers to arrest, resulting in the development of specific themes related to arrest likelihood in Internet sex crimes against minors.

Interviewers saved case summary information in NVivo qualitative software compatible format. These case summaries were analyzed using NVivo qualitative software in order to identify specific types of dilemmas noted by law enforcement investigators. The 68 case summaries were reviewed and coded for consistent themes. The themes were coded using key words and contextual information derived from the OBSTACLES case summaries. The final qualitative analysis suggested four general categories of dilemmas reported by law enforcement investigators, which do not represent mutually exclusive categories. One of the N-JOV research assistants independently coded a sub-sample of ten randomly selected OBSTACLES cases to evaluate coding reliability. The final qualitative codes were used to develop qualitative narratives, and were also coded as variables in an existing SPSS OBSTACLES database.

Third, *identified* victim cases (those cases in which law enforcement investigators located and contacted an Internet-related victim) in which no arrest was made will be compared to the larger sample of N-JOV identified victim cases in which law enforcement made an arrest.

Prior to entering interview data for this project, SPSS Data Entry Builder 3.0 was used to develop a data entry template for case level data. The OBSTACLES section Data Entry program was designed by one of the N-JOV study principal research investigators so that it would be compatible with the existing Data Entry system used for N-JOV. The SPSS Data Entry Builder 3.0 program facilitated entering data from paper copies of interviews directly into a SPSS data file. To ensure coding reliability, all OBSTACLES project data were double entered into the SPSS Data Entry Builder 3.0 program by one of the N-JOV co-investigators and the OBSTACLES investigator.

OBSTACLES quantitative data for each survey section were analyzed for the study descriptives presented in the next chapter. In addition, data from the 68 OBSTACLES cases were merged with data from the 464 N-JOV cases for each survey section. The individual merged survey sections were combined into one large data set consisting of 532 cases. This merged data set was used for all Chapter 3 and Chapter 4 analyses. Chapter 5 analyses use a sub-sample of cases with identified victims. It should be noted that N-JOV cases were sampled using a specific methodology designed for weighted analyses, and that this exploratory analysis does not use those weights because the OBSTACLES cases were not weighted.

Chi-square was selected as a method of bivariate analysis between variables measuring social characteristics, legal controls, and law enforcement effort, because all study variables are categorical. Bivariate relationships were examined for significant relationships (alpha of .05), taking effect sizes into consideration. Those social and control variables with statistically significant relationships in bivariate analyses were included in multivariate analyses. Logistic regression was conducted as a method of multivariate analysis to identify predictors of legal action (arrest, search, seizure and overall legal involvement). SPSS version 11.5 was used for univariate and bivariate analyses and STATA version 7 was used to conduct logistic regression analyses.

CHAPTER 3

RESULTS: OBSTACLES CASE TYPES & STUDY DESCRIPTIVES

Characteristics of OBSTACLES Cases

The author collected data from a sample of 68 OBSTACLES cases in which law enforcement agents were unable to make an arrest in an Internet sex crime against a minor. Characteristics of the OBSTACLES cases are explored here. In addition, some comparisons between the OBSTACLES and National Juvenile Online Victimization study (N-JOV) cases are presented.

The variation in these OBSTACLES cases is notable, and is contrary to preliminary expectations in at least one way. Describing these crimes as "online *child* sexual abuse crimes" may be misleading. More than two-thirds (68%) of the identified victims in the OBSTACLES cases (N=31) were between the ages of 13 and 17. The OBSTACLES case victims ranged in age from 10 to 17 with an average age of 14 (s.d.=2 years). These results suggest that it may be more appropriate to consider these incidents as crimes against *minors* (or even adolescents), rather than *children.* Drawing from recent research by Finkelhor, Wolak, and Mitchell (2003a) this project will characterize these crimes as Internet sex crimes against minors (ISCAM).

Case Types

This analysis will characterize the OBSTACLES cases into three primary groups based on case types in the N-JOV study (Wolak et al. 2003a). The first group of cases includes all incidents involving an identified minor victim and will be described as "Internet Crimes with Identified Victims" (I-CIV) cases (Table 2).

I-CIV Cases. This is the only category that involves victims who were identified, contacted, and included an offender suspected of committing a criminal offense on the Internet. These cases ranged from sexual assault to online solicitation and reducing minors' inhibitions through Internet grooming. This category includes all investigations in which an identified minor victim was sexually exploited using the Internet, or in which a victim was identified in a case involving the *production* of Internet child pornography.

About three-quarters of the victims in the OBSTACLES I-CIV cases met offenders on the Internet (Internet-initiated) and about 25% had some type of prior relationship (family member or acquaintance) with the offender. In the Internet-initiated cases, victims met offenders in chat rooms, during Instant Message (IM) communications, or in other types of Internet interactions. Offenders in family/acquaintance cases were relatives, teachers, mentors, or other individuals known to the victim prior to any Internet communication.

I-STULE Cases. A second category of cases includes all cases in which adults sexually solicited undercover law enforcement investigators posing as juveniles online. These cases will be labeled "Internet solicitations to undercover law enforcement" (I-STULE). These cases involve adults who thought that they were talking with minors, but in reality they were communicating with undercover police officers, so they can be considered "attempts." This category only includes offenders who were involved in undercover cases initiated by law enforcement. In some other cases, law enforcement investigators took on the persona of a victim who had been contacted by an offender online. Those cases are included in the I-CIV category. Offenders who met the I-STULE criteria but were found to have committed Internet crimes against identified victims in the current investigation were also put in the I-CIV category.

I-CHP Cases. A final category of cases reported by law enforcement includes investigations of Internet child pornography possession or distribution in which no minor victim was identified or contacted. These cases will be categorized as "Internet child pornography" (I-CHP) investigations. Suspects in these cases used the Internet to distribute, collect, or trade child pornography. As noted previously, it is not uncommon for victims to remain unidentified in law enforcement investigations of child pornography possession and distribution. In such cases, it may be that images were taken off of the Internet before the minors could be identified, that the Internet images did not provide enough evidence to identify the victim, or that the agency suspected that the images originated outside of the United States.

Table 2: Types of cases in the OBSTACLES and N-JOV samples

Internet Sex Crime Against a Minor (ISCAM) Case Type*	OBSTACLES (n=68)	N-JOV (n= 464)
Internet crimes with identified victims (I-CIV)	41% (28)	44% (205)
Internet Solicitation to Undercover Law Enforcement (I-STULE)	9% (6)	21% (96)
Internet child pornography (I-CHP)	50% (34)	35% (163)

* p < .05

Process of Categorization with OBSTACLES Cases

Although some of the OBSTACLES cases were straightforward in terms of classification, the complexity of many of these cases deserves note. For example, although any case involving an identified victim is classified as an I-CIV investigation here, some suspects in these cases also possessed or distributed child pornography. Consider this example from the OBSTACLES study that was classified as an I-CIV case and also involved the distribution of child pornography:

The case first came to police attention when a father reported to an Internet crime tip line that his 12-year-old daughter had been pressured to send a nude picture of herself to an online "friend." This juvenile initially thought that she was communicating with another juvenile in Europe. Law enforcement investigators traced the suspect's Internet Service Provider account information, and found that the account actually belonged to an adult in South America. This "friend" was never identified, despite the trace to South America. In addition to the Internet grooming that led up to the production of this image by the victim, the suspect in the case sent the girl close to 50 explicit child pornography images.

Since an Internet victim was identified, this is considered an I-CIV case in this study. However, the suspect also sent the juvenile victim images of child pornography over the Internet and the juvenile send produced child pornography to the offender. In other cases, offenders were suspected of committing crimes both on and offline. Since this study focused on those crimes with an Internet-nexus, data were primarily collected on the Internet component of these allegations. For example, some child pornography possession and distribution cases involved an identified, non-Internet related victim. That was the situation in the following case:

Police received a report that a 46-year-old male sexually exploited a boy who he was mentoring. Police were alerted to the suspect when the allegation of sexual exploitation was made. As a result of the investigation, a search warrant was *procured and executed on the suspect's residence and his computer was seized. Investigators found deleted files, which appeared to be child pornography. However, the images depicted minors in nude or suggestive poses, and did not meet the state's definition of child pornography. The agency was not able to file sexual exploitation charges either, so no arrest was made in the case.*

This case was classified as an I-CHP incident for this study, since the suspect had child pornography images on his computer. Again, although the case involved a sexual exploitation of an identified minor, that component of the alleged crime was not Internet-related, therefore the above is not an I-CIV case.

An examination of the characteristics of these three general case types, the suspected offenders, and the identified victims provides a useful context for studying dilemmas described by law enforcement investigators. Although examining cases in which no arrest was made was a primary focus of this research, comparisons are also made with the larger sample of N-JOV cases. In some instances, the characteristics of OBSTACLES and N-JOV cases are similar, and in others there are differences.

Characteristics of Victims and Offenders in OBSTACLES Cases

Data collected in this study suggest that there are differences in the amount of victim and offender information available in investigations of Internet sex crimes against minors. Specifically, it appears that law enforcement agents were generally more certain about victim characteristics than offender information. This is particularly true in the OBSTACLES cases. In that sample, for instance, police knew victim age and gender in all 28 cases involving identified minors, and were unsure of race for only one victim. However, police did not know suspect age in 28% of cases, race in 31% of incidents, or gender in 15% of these OBSTACLES investigations.

Victim Characteristics

About forty percent of the OBSTACLES and N-JOV cases involved *identified* victims, or victims who law enforcement agents located and contacted. The majority of victims in both OBSTACLES and N-JOV cases were female adolescents. There were statistically significant differences in victim race and income for OBSTACLES and N-JOV cases, in that victims in arrest cases were more likely to be White and high income than victims in the cases in which no arrest was made (Table 3).

Table 3: OBSTACLES and N-JOV Victim Characteristics

Overall (N=233)	**OBSTACLES (12%)**	**N-JOV (88%)**
Victim Age		
Under 13 (n= 61)	7%	93%
13 or over (n= 171)	14%	86%
Don't know victim age (n=1)	0	100%
Victim race		
White (n=206)	10%	90%
African-American (n=12) *	33%	67%
Other race (n=7)	14%	86%
DK Victim race (n=3) *	33%	67%
Victim HH income		
50K and under (n=62)	8%	92%
Over 50K (n=111) **	6%	94%
Don't know Victim income (n=59) ***	27%	73%
Victim Gender		
Male (n=72)	15%	85%
Female (n=161)	11%	89%

* $p \leq .05$, ** $p \leq .01$, *** $p \leq .001$

Offender characteristics

As noted previously, both individuals suspected of committing crimes in OBSTACLES cases and those arrested for Internet sex crimes against minors in N-

JOV cases are categorized as offenders in these analyses. Characteristics of N-JOV and OBSTACLES offenders are presented in Table 4. Investigators were unsure of suspect characteristics in many of the OBSTACLES cases, suggesting that offender data may be somewhat socially invisible (Black 1989) in some of these investigations. In the OBSTACLES cases in which police were able to ascertain characteristics, the majority of the suspects were white, male adults with incomes under $50,000. There were statistically significant differences in OBSTACLES and N-JOV cases for all offender characteristics.

Table 4: OBSTACLES and N-JOV Offender characteristics

Offender characteristics (N= 532)	OBSTACLES (13%)	N-JOV (87%)
Offender age		
Offender under 18 (n=21)	10%	90%
Offender 18 to 39 (n=276) ***	8%	92%
Offender over 40 (n=213)	10%	90%
Don't know O's age (n=18) ***	100%	0
Offender race		
White (n=482) ***	8%	92%
African-American (n=15)	20%	80%
Other (n=11)	46%	56%
Don't know offender race (n=22) ***	88%	13%
Offender income		
50K or under (n=279) ***	5%	95%
Over 50K (n=150)	7%	93%
Don't know offender income (n=103) ***	43%	57%
Offender gender		
Male (n=515) ***	11%	89%
Female (n=7)	43%	57%
DK (n=10) ***	100%	0

* p ≤ .05, ** p ≤ .01, *** p ≤ .001

Demographic and Case Characteristics by Case Type

Internet crimes with identified victims (I-CIV) cases

As was true with the general case types, Internet crimes with identified victims in the OBSTACLES sample were more varied than anticipated. It was expected that cases examined here would consist of an adult contacting a juvenile online, sexually soliciting that minor, and then assaulting that minor at an actual meeting. While law enforcement agents reported those types of incidents, the OBSTACLES cases also include a more diverse array of Internet crimes. Other OBSTACLES cases with identified victims featured: 1) incidents in which minors were asked to send sexually explicit images of themselves to a stranger over the Internet, 2) sexual solicitations by adults the minor never met in person, and 3) distribution of graphic images of Internet child pornography to minors.

Comparisons between the N-JOV and OBSTACLES samples suggest some differences between arrest and non-arrest cases (Table 5). About three-quarters of the OBSTACLES cases involved victims and offenders who met on the Internet (Internet-initiated cases), as compared to about half of the N-JOV victims, a difference that is statistically significant (Pearson $X^2 = 6.539$, $p = .011$, Phi = .168). Although other differences were not statistically significant, they deserve note.

Law enforcement investigators were asked whether or not "any illegal sexual activity," which could include anything from non-contact to intercourse or other penetration, took place between the victim and the offender. Some type of illegal sexual activity took place in 46% of Internet-Initiated OBSTACLES I-CIV cases and

66% of N-JOV I-CIV cases. Such illegal sexual activity was reported in about 10% of both Internet-initiated and family/acquaintance OBSTACLES cases and about 90% of N-JOV cases. I-CIV cases that did not include illegal sexual activity involved a range of incidents such as online grooming (decreasing children's inhibitions), unsubstantiated allegations of child pornography production, and other incidents which could be considered preparatory or attempted sexual exploitations. Offenders in these cases produced pornographic images of an *identified* victim in about 20% of OBSTACLES and forty percent of N-JOV I-CIV cases.

Table 5: Comparisons of I-CIV cases for OBSTACLES and N-JOV

Overall I-CIV Case characteristics (N = 233)	OBSTACLES (12%)	N-JOV (88%)
Victim/Offender Relationship*		
Internet-initiated (n = 122)	17% (21)	83% (101)
Family/acquaintance (n= 111)	6% (7)	94% (104)
Illegal sexual activity between victim & Offender (N=144)	8% (12)	92% (132)
Internet-initiated (n= 81)	9% (7)	91% (74)
Family/acquaintance (n =63)	8% (5)	92% (58)
Offender produced child pornography (n= 83)	7% (6)	93% (77)

* p < .05

Internet Solicitations to Undercover Law Enforcement (I-STULE)

A second category of cases includes all those cases in which an offender solicited an undercover law enforcement agent posing as a minor on the Internet. For both N-JOV and OBSTACLES cases, the majority of contacts were made in chat rooms. Also included in this category are three cases in which adult civilians initiated some type of undercover "investigation" or otherwise engaged with an offender suspected of committing an Internet sex crime against a minor victim. Significantly, no OBSTACLES I-STULE case featured an actual meeting between law enforcement agents and a suspected offender (Pearson $X^2 = 17.264$, p. = .000, Cramer's V = .328).

In addition, there were statistically significant differences between OBSTACLES and N-JOV cases in which a meeting was planned but did not occur (Pearson $X^2 = 3.87$, p. = .049, Phi = -.199). More than a fifth of both OBSTACLES and N-JOV cases included some attempted meeting between an offender and law enforcement (Table 6).

Table 6: Comparisons of I-STULE cases for OBSTACLES and N-JOV

I-STULE Case characteristics (N=102)	OBSTACLES (6%)	N-JOV (94%)
Where law enforcement agent met offender		
Chat room (n=90)	6% (4)	94% (60)
Instant Messages (n=30)	0	100% (24)
E-Mail (n=31)	0	100% (7)
Met some other way (n=8)	0	100% (4)
No law enforcement agent (n=2)	67% (2)	33% (1)
There was a face-to-face meeting between offender and law enforcement agents (n= 73)***	0	100% (73)
Such a meeting was planned/did not occur (n= 30) *	10% (3)	90% (27)

* $p < .05$, ** $p < .01$, *** $p < .001$

Internet Child Pornography (I-CHP) Investigations

Those cases in which law enforcement investigators reported the possession or distribution of child pornography images, with no evidence that an offender produced images of an identified victim, were classified as Internet Child Pornography (I-CHP) investigations. This category includes a range of cases, although there was somewhat less variation within the OBSTACLES incidents than in Internet crimes with identified victims (I-CIV). The OBSTACLES I-CHP cases include unsubstantiated allegations of child pornography possession, anonymous online posting of child pornography, borderline cases in which children depicted in images may or may not be minors, and proactive undercover investigations of suspected child pornography offenders. The cases discussed here all contain an allegation or discovery of child pornography collected or distributed via the Internet.

It is important to note that the cases classified here as Internet child pornography did not involve any online correspondence, exchange of images, or other Internet connection between an adult offender and an identified juvenile victim. None of the victims depicted in the child pornography images were identified or contacted by law enforcement. However, as noted previously, some of the cases included in this category may involve an alleged sexual offense between an adult and a minor victim, but with no Internet connection between the victim and the offender. For example, a suspect in one case sexually assaulted a child living in his neighborhood (no Internet connection here).

Internet child pornography cases made up half of the OBSTACLES sample (N=34), as compared to 35% (N=163) of the N-JOV sample (Table 7). The nature and content of the child pornography images found in the OBSTACLES and N-JOV cases varied significantly, in that offenders arrested in Internet child pornography cases were more likely to possess collections including graphic sexual images, or images that focused on genitals or showed explicit sexual activity (Pearson X^2 = 30.87, p = .000, Phi. = .332). There were also statistically significant differences between these two samples in terms of whether or not images showed penetration of a child (Pearson X^2 = 18.95, p = .001, Phi. = .310). In addition, the N-JOV offenders were significantly more likely to possess images of nudity or semi-nudity than suspects in OBSTACLES cases (Pearson X^2 = 31.28, p = .000, Phi. = .398).

Table 7: OBSTACLES and N-JOV Internet Child Pornography cases

Characteristics of Internet Child Pornography Collections (N= 197)	OBSTACLES (17%)	N-JOV (83%)
Included graphic sexual images (n = 182) ***	13% (24)	87% (158)
Pictures showed penetration (n= 159)***	11% (18)	89% (141)
Images featured nudity or semi-nudity (n = 170)***	14% (24)	86% (146)

* p < .05, ** p < .01, *** p ≤ .001

In conclusion, the OBSTACLES cases feature a range of suspected criminal offenses. The characteristics of these incidents suggest some distinctions between the OBSTACLES cases and the N-JOV cases in which an arrest was made by a law enforcement agency. Case characteristics suggest practical differences in whether or not illegal sexual acts occurred and the relationship between victims and offenders. In addition, law enforcement agents were less likely to have complete offender information in the OBSTACLES incidents than in the N-JOV cases.

This analysis of OBSTACLES and N-JOV case characteristics introduces some potential dilemmas in investigations of Internet sex crimes against minors, such as missing offender information. The following chapter examines OBSTACLES case summaries for additional insight into these dilemmas.

CHAPTER 4

RESULTS: QUALITATIVE ANALYSIS OF LAW ENFORCEMENT DILEMMAS IN INTERNET SEX CRIMES AGAINST MINORS

Despite the variation in case types and incident characteristics noted previously, all of these investigations share a primary similarity. Law enforcement agencies were not able to make an arrest in any of these alleged crimes. Why was no arrest made in these Internet sex crimes against minors?

There is no single explanation for why arrests did not occur in these cases, and the dilemmas reported by law enforcement involve complex social and legal dynamics. Proving that a crime occurred, victim cooperation, collaborations with other jurisdictions, and offender identification all complicate these investigations. Some of the dilemmas presented may be directly related to the nature of computer crime, and others could be problematic with or without an Internet-nexus.

The dilemmas identified here can be classified into four general categories. First, law enforcement agents were not always able to prove that a criminal act had taken place. Second, investigators reported that it was not always possible to identify specific offenders in these incidents. Third, victims who were reluctant to testify or to cooperate with law enforcement posed challenges. Finally, some agencies lacked training and resources required in these investigations, or reported challenges in jurisdictional collaboration. These categories are not mutually exclusive, since investigators may have noted multiple dilemmas related to one case. Overall, these dilemmas seem to present problematic, although not insurmountable barriers for the criminal justice system. For many of the dilemmas considered here, remedies either exist or could be implemented to minimize the impact of these challenges on law enforcement investigations of Internet sex crimes against minors (Table 8).

Table 8: Dilemmas in Internet sex crimes against minors

Issues in Internet Sex Crimes Against Minors (ISCAM) cases	Number of dilemmas (N=101)	% of total dilemmas (N=101)
1. **Proof that a crime occurred**	**26**	**26%**
a. Defining child pornography (graphic images and child age)	9	9%
b. Criminality of preparatory acts (illegal sexual acts and actual meetings)	21	21%
c. Victim "age of consent" issues	4	4%
d. Other proof issues	9	9%
2. **Inability to identify offender**	**34**	**34%**
a. Not enough information to identify offender	21	21%
b. Multiple computer users	5	5%
c. Too much time passed to identify offender	8	8%
3. **Reluctant or uncooperative victims**	**11**	**11%**
4. **Training/Resource/collaboration dilemmas**	**13**	**13%**
a. Gaps in resources/training	4	4%
b. Multi-jurisdictional cooperation	9	9%
c. Other agency took over	17	17%

Proof that a Crime Occurred

Obviously, law enforcement investigators need to prove that a crime occurs prior to making an arrest in Internet sex crimes against minors. These investigators are familiar with state statutes, and can identify and act on behavior considered criminal under those legal realities. So what complicates this issue?

Law enforcement investigators reported that at least four specific types of dilemmas made it difficult to prove that an Internet sex crime against a minor had occurred. Investigators reported challenges related to the following: 1) defining child pornography, 2) criminality of preparatory acts, 3) victim age of consent, and 4) other proof issues. These proof dilemmas suggest compelling questions about statutory issues and practical complications in these investigations.

Dilemmas related to definitions of child pornography

What types of images can be defined as child pornography? If an image depicts nude minors in suggestive poses, can it be considered child pornography? How can investigators prove that children in an image can legally be considered minors?

These questions are key issues in a heated debate regarding child pornography and can be problematic in I-CIV cases involving the production of child pornography as well as I-CHP cases. The controversy reflects ambiguity in how child pornography should be constructed, both socially and legally. There is likely consensus, for example, that an image of a 4-year-old boy being raped by an adult male could be considered child pornography. However, the cases identified in this study illuminate that there are divergent views regarding what constitutes child pornography. First, there may not be consensus regarding what types of images are graphic or explicit enough to fit existing definitions of child pornography. Second, it appears that images that depict prepubescent children are more likely to be considered child pornography than are those portraying older juveniles. Consider the following case:

A *Rent-A-Center contacted law enforcement when it repossessed a 40-year-old suspect's computer from his suburban home. The suspect lived alone, and when the Rent-A-Center staff took the computer, he told them "Don't look on my hard drive." They did, and found images of naked children. The law enforcement investigators found about 100 images of naked children, either at a nude beach or in a birch forest. The investigator believed that the images were a part of a series of images produced in Russia known to law enforcement. The investigator in this case described the images possessed by the suspect "Lolita art." However, investigators were not able to prove that the suspect possessed any images that could be considered child pornography in his collection. Since images of naked children without graphic sexual activity or that do not focus on the genitals do not meet that state's definition of child pornography, the agency was unable to arrest the suspect.*

Determining whether or not images are explicit or graphic enough to meet the definition of child pornography is a primary dilemma for investigators (Lanning 1992). That is because some images would consistently meet legal definitions of child pornography, and others may not. An image that shows sexually explicit conduct between an adult and a child can clearly be considered child pornography, while images of nude children may be seen by some as artistic or erotic, but not child pornography (Lanning 1992).

Most jurisdictions have some minimum level of explicitness that must be met in order for images to meet statutory requirements for child pornography. While child pornography statutes generally address similar issues, there is variation among state definitions of what constitutes child pornography. For instance, Colorado's statute includes "any sexually exploitative material" (National Center for Prosecution of Child Abuse 1999:10). Alaska's child pornography statute specifically defines what types of activities must appear in child pornography, including "sexual penetration; the lewd touching of another person's genitals, anus, or breast; the lewd touching by another person of the child's genitals, anus, or breast; masturbation; bestiality; the lewd exhibition of the child's genitals; or sexual masochism or sadism" (National Center for Prosecution of Child Abuse 1999:4-5).

Alaska and other states have crafted statutes that may reflect social and legal reluctance to draw overly broad definitions of child pornography. Challenges related to defining online child pornography appear to be part of two larger social and legal discussions: 1) An effort to promote advocacy for juvenile victims of sexual exploitation: and 2) A debate regarding governmental control of the Internet (Mitchell, Finkelhor, and Wolak 2003; Peron 2003).

Advocates for children see child pornography as a form of child sexual abuse or exploitation (Edwards 2000; Hames 1993; Itzin 1994; Lemmey and Tice 2000). This view contends that by definition, the production of child pornography required that a child be sexually victimized. Others claim that the concern over child pornography has led to such liberal definitions that "a huge amount of material that most reasonable people wouldn't classify as child pornography" is now criminalized (Peron 2003:2). From this perspective, governmental controls have created a climate in which parents need to be warned "Don't allow your children to bathe naked" (Peron 2003:2).

Law enforcement agents stress that the intent of these statutes is to criminalize the production or possession of graphic sexual images of children, not to penalize "normal parents who simply have photographs of their nude, young children" (Lanning 1992:33). Generally, images of nude children would only be considered child pornography if they focus on the genital area or are otherwise considered to be lascivious exhibitions (Lanning 1992). However, law enforcement agents are encouraged to consider borderline or questionable material in the context of an offender's entire collection or other incident dynamics (Lanning 1992).

Given this charged debate, it is likely that law enforcement investigators proceed with caution in cases involving borderline images of juveniles, such as child erotica or less than graphic images of child pornography. In one case from this study the images that were produced appeared to be questionable, or even inappropriate, but did not meet required levels of explicitness:

The investigation came to police attention when police pulled over a car and found a 13-year-old girl driving. Soon thereafter, they became suspicious of this girl's relationship with a 47-year-old male in her neighborhood. The victim lived with her mother and had a number of problems in her life. The suspect in the case was a divorced, unemployed male. This adult had no children of his own, but had contact *with several children in the neighborhood. This minor was spending time at the adult's home, and investigator reported that the victim was "letting him take pictures of her and post them on the Internet." Investigators found that the adult was distributing at least 200 digital images and 20 digital videos of the victim on the Internet. In most of the images, the victim posed in her bathing suit and in erotic poses. Interested "consumers" could email the suspect and make request for what the girl should be doing in future pictures. However, none of the images found were considered graphic or explicit enough to be considered child pornography under this state's statutes. In addition, the investigator reported that if the images depict children over 13, the case is considered borderline and a lower priority than cases involving younger victims.*

In the case above, the nature of the image was a major dilemma for investigators. None of the images found on the suspect's computer or posted on the Internet met state definitions of child pornography. Despite what have been criticized as "very broad definitions" (Peron 2003:2), legal statutes and law enforcement investigators did take explicitness into consideration. While recent media reports feature controversies regarding teen modeling agencies and other outlets for suggestive images of juveniles, these images are not currently considered to be criminal activity in most jurisdictions.

In addition, the investigator in the previous example stated that the age of the juvenile depicted in the images contributed to the case outcome. Lanning and Burgess (1989) note that adolescent victims of sex crimes generally elicit less sympathy than younger children. That seems to be the case here, as the investigator's statement suggests that had the victim been younger, the investigation may have ended in an arrest.

Consideration of child's age can be particularly problematic in child pornography possession cases, in which offenders collect images produced by others. Lanning and Burgess stated in 1989 that pedophiles collect, save, and cherish child pornography. If these collectors of child pornography do not produce images themselves, it is unlikely that investigators will be able to identify or contact victims depicted in the images. This reality makes identifying child victims "one of the most difficult and frustrating aspects of law enforcement's job" (Allinich and Kreston 2001:2). This was one of several dilemmas in a case involving a digital video:

A suspect's ex-wife reported that her ex-husband had child pornography on a computer. Law enforcement agents searched the 46-year-old suspect's ISP account and were only able to find one video clip. The victims in the clip looked like minors to the law enforcement investigators, but the prosecutor declined to prosecute as the children "looked to be 14, 15, or 16." During this investigation, police discovered that the suspect was communicating online with a 13-year-old female in another country. The suspect had made this juvenile the beneficiary of his life insurance policy, and wrote "I am absolutely in love with ____" in his Internet service provider profile. However, the victim in this case was never contacted by law enforcement, as there was no evidence that the two had ever met in person.

In this case, the respondent noted that although he was confident that children were minors, ("they don't have any pubic hair") the prosecutor refused to move ahead with the case. From a practical standpoint, and as is suggested in the example above, law enforcement and/or prosecutors may not always be able to determine whether or not children in images fit statutory definitions. Some prosecutors may be hesitant to move ahead with cases in which the only images available depict older children, while others may give priority to these cases.

Prosecutors have legitimate legal concerns about age of children depicted in images. Generally, "children" in child pornography must fit within state's definitions of "child," and those ages and definitions vary. In Michigan, for example, "a child means a person who is less than 18 years of age and is not emancipated by operation of law" (National Center for Prosecution of Child Abuse 1999:24). New Jersey's child pornography statute defines a child as "any person under 16 years of age" and (National Center for Prosecution of Child Abuse 1999:28).

Some jurisdictions use medical experts to testify that children depicted in images are minors (Rosenbloom and Tanner 1998). Expert witnesses can play a valuable role in legal proceedings, by providing testimony to educate and inform jury members, judges, and other legal participants about specific subjects (Holmgren 2002).

The use of medical experts in child sexual exploitation cases is not a new phenomenon. Doctors, nurses, and other medical professionals can be called to testify regarding sexual abuse examinations and other medical procedures in child sex crimes (Holmgren 2002). The use of medical experts in these child pornography cases is a more recent and somewhat controversial development. Medical expert witnesses in child pornography cases generally have not examined the child in a specific image, but rather attempt to determine the chronological age of the child depicted

(Rosenbloom and Tanner 1998). In order to ascertain the age of children depicted, some experts have relied on the Tanner scale, a measurement designed to identify developmental maturity (Rosenbloom and Tanner 1998). However, Tanner and Rosenbloom claim that this use of the Tanner scale is illegitimate and inappropriate (1998). A key feature of expert witness testimony is that it has a scientific basis, and therefore, the use of the Tanner scale may fall under increasing scrutiny.

If as some suggest, the number of pornographic images of children online is increasing (Jenkins 2001), these two definitional dilemmas will likely continue to present challenges for law enforcement. Verifying whether or not images are graphic, explicit, or lascivious enough to fit within state statutes will be a primary difficulty. In addition, investigators and prosecutors will have to be able to ascertain that images depict minors.

Remedies for child pornography dilemmas

It is possible that several existing or potential efforts could remedy some of these definitional dilemmas. Both statutory changes and practical approaches could ameliorate the dilemmas associated with defining child pornography.

- Propose or model uniform child pornography definitions. These revisions could be designed to address issues of explicitness required in images, and could be based on federal statutes or some other criteria.
- Increase consideration of what images fall within statutes. There is room for increased debate regarding what images clearly fall within statutes and what images may be more questionable.

- Evaluate questionable images within a more general context. In evaluating borderline images, investigators could rely on Lanning's (1992) suggestions for evaluating questionable images. These include consideration of the circumstances in which images were produced, an examination of how the images were saved (organized or cataloged), and how they were used by the suspect (were they used to seduce or lower children's inhibitions?) (Lanning 1992).
- Develop a secure, comprehensive law enforcement database of identified child pornography images. Law enforcement agencies in European countries have cataloged known images of child pornography (Persson 2001) and the United States has just begun to compile such a database (Caruso 2003). Since it is generally believed that many of the images in these investigations are passed among child pornography consumers or are "known" to law enforcement agents, such databases could minimize wasted resources if several agencies identify the same image.
- Use expert witnesses to certify that images are child pornography, and when feasible, submit those certified images to the developing federal database of images. Pediatricians and other medical professionals are generally called to testify that a child in a child pornography image is under the statutory age (Rosenbloom and Tanner 1998). While some larger agencies may have resources for obtaining expert witness testimony, smaller agencies may not have the resources to locate or finance expert witnesses.

- Refine or develop existing measures used by expert witnesses. Given the present controversy regarding the Tanner scale, consider developing new measures or refining existing measures of child maturation and development.
- Consider the long and short-term consequences of producing, trading, and posting erotic images of minors that may not fall within definitions of child pornography on the Internet. While child "erotica" is currently not considered illegal, the production of such images and their mass distribution over the Internet deserves additional consideration.

Criminality of preparatory acts

Cases in which law enforcement investigators identified and contacted a minor victim (I-CIV cases) suggest that the criminality of some preparatory acts is uncertain. For example, if an adult sets up a meeting for sex with a minor, but the two never meet, has any crime been committed? Is it a crime for an adult to send adult pornographic images or sexual photographs to minors over the Internet? Is it illegal for an adult to have sexual discussions with juveniles online or for that adult to request that the minor engage in sexual acts? Can "fantasy" discussions of child sexual exploitation be addressed by the legal system? About twenty percent of the dilemmas noted by law enforcement investigators related to the criminality of preparatory acts. This issue is particularly problematic in I-CIV cases in which a suspect had some type of online communication with a minor victim and was not noted as a problem in Internet production of child pornography cases.

If an adult were to introduce himself to a minor in an amusement park and ask for sexual favors, it would likely be considered a criminal act. Would the same be true if the adult met the minor in a teen oriented chat room and asked for sex? The answer to that question varies both according to statutory realities and practical considerations. Consider the following case:

A divorced 47-year-old male contacted a 14-year-old male online in a gay chat room. The victim was a lonely student who had some problems getting along with his parents. The two communicated online for over six months and had over a hundred online interactions. In addition to their online communication, the adult and the minor talked by phone and sent letters to each other. The suspect sent the juvenile nude pictures of himself and adult pornography by email. The juvenile's parents contacted police after they caught their son trying to leave the house to meet this adult and found a letter from the adult to the juvenile. Law enforcement was able to identify the suspect, but since there was no meeting between him and the juvenile, no arrest was made. Police tried to get additional evidence by initiating an undercover reactive investigation in which they posed as the juvenile online for about four months, but the suspect never brought up sexual topics with the undercover investigator. This victim was not at all cooperative with the law enforcement investigation, and police suspected that the juvenile warned the suspect about the undercover investigation.

It may be that most of the Internet-initiated sexual exploitation of a minor cases that come to public attention involved some meeting that actually took place between an adult offender and a juvenile victim. However, it is probable that many more of those meetings are suggested, discussed, and even planned, but never actually occur.

Law enforcement reached an impasse in these cases if they realized that the Internet had been used primarily as a means of preparation to commit a sex crime against a minor. In these cases, it appeared that the Internet was used as a means of decreasing children's inhibitions (grooming) or to sexually solicit minors, but there was no evidence that the incidents fit within existing criminal statutes. It is probable that some of those grooming incidents could have developed into actual exploitations, but were interrupted by the police investigations.

While grooming itself is not generally considered criminal behavior, there is general agreement that it often precedes actual sexual offenses (Brown 2001a). It is unlikely that a law enforcement agency could arrest a suspect based on grooming alone. At the same time, investigators see these adults as likely suspects, and in some instances believe that they actually are "child molesters." This case is illustrative:

An investigator reported an online enticement of a minor female by a 19-year-old male in another state. The victim and the suspect had Internet contact "for a while" and then made plans for the suspect to come to the victim's house for sex. The girl's mother found copies of the communications with the suspect and contacted police. The suspect had asked the victim to go on birth control and had offered to help her with her pap smear. He sent her a picture of himself with a rose in his mouth and two bottles of alcohol. This suspect was also communicating with two or three of the victim's classmates. The victim's mother wrote an email to the suspect to tell him that her daughter was a minor and that the police were involved. The *investigators were able to identify the suspect, but did not proceed with the case, as the victim and suspect did not meet.*

Computer technology allows for creative attempts for law enforcement agents to engage offenders, including investigations in which police take on the persona of a minor victim. In an effort to appear to "be" the juvenile online, investigators go "undercover" as the identified victim, learn the suspect and juvenile's nicknames for each other, visit typical chat rooms, and even have the juvenile victim share ideas about what to say to a suspect online. In other undercover investigations, police "initiate" proactive cases by posing as juveniles online. However, in most of these undercover investigations, if the suspect does not respond, there may not be enough evidence to move forward with the case, as the following case demonstrates:

A law enforcement investigator posed as a 14-year-old female online. An individual claiming to be a bi-sexual female contacted this "victim" in a sexually oriented chat room and brought up sex related topics in the first online interaction. The investigator was able to trace the offender through an Internet Service Provider, and believes that the suspect was actually a 44-year-old man. A meeting was set up between the "victim" and the adult, but the adult failed to show up at the meeting place.

In cases such as the one above, police may not be able to charge offenders with criminal behaviors, if the charge requires an actual meeting. Online solicitations are clearly of concern to both parents and law enforcement officials, and some states have enacted laws to protect children from online solicitations. These statutes may criminalize indecent communication with minors or the use of a computer to commit a criminal act (such as criminal threatening).

In several of the investigations noted here, it appears that incidents that could be considered criminal offline are not currently considered crimes. For example, if an adult sexually solicits a child in an amusement park, the child may be physically threatened and vulnerable. If an adult sexually solicits the same child online, not all jurisdictions would consider it a criminal act. It may seem that in Internet sexual solicitations, the child is most likely not at risk of immediate physical harm. The child could end the communication, change ISP addresses, and report the incident to authorities.

Nevertheless, it is likely that many of the sexual preparatory acts reported here would be crimes if they occurred face to face. For example, if an adult shows a child his penis on a playground, he could be arrested. It is unclear in some jurisdictions whether the same adult would be arrested if he sent a digital photo of his penis to a minor online.

A final question is whether or not "fantasy" conversations between adults can be considered criminal. In some cases it appeared that a suspect was "preparing" to commit a sex crime with a juvenile victim, but there was no evidence that any such act occurred. In fact, in one case there was such discrepancy between online communication and evidence collected during investigations that police wondered if any of the allegations were based in reality. In this case, law enforcement agents suspected that some or all aspects of the case could have been based on some fantasy communication rather than an actual sexual exploitation of a child:

An adult contacted law enforcement when a single 54-year-old male offered his 15-year-old son for sex. In that case, the two adult males communicated online about homosexual activity. One of the adult males called himself "bucking bronco," and shared that he had sexually abused a child in the past. The second adult not only contacted police, but also agreed to continue chatting online with "bucking bronco" and to give information from the online communication to law enforcement agents. Using information collected from the suspect's Internet service provider (ISP) account, the law enforcement agency was able to identify "bucking bronco" and made contact with the suspect. When the law enforcement agency went to talk to the suspect, they discovered that "bucking bronco" did not actually have any children. The police could not prove any criminal act, as "bucking bronco" claimed that his comment was "just a turn on."

Investigators were able to resolve that case and identify the suspected offender. By collecting information from the suspect's ISP account, law enforcement was able to ascertain that no actual sexual exploitation of a minor had taken place. Fantasy is not illegal, and this case appeared to really be a fantasy. This may have been a stronger case if there had been some concrete evidence, such as if there had been any indication that a real child was at risk or if the suspect had a previous sex offense against a minor. It is unclear when or if these fantasy cases could be considered criminal threatening. Such cases raise questions, for example, about whether a person with a previous sex offense would be charged with a criminal act if he/she solicited a child for sex via the Internet while serving a life sentence in prison.

Remedies related to preparatory acts

There may be uniform remedies for some dilemmas associated with preparatory acts, and others may need to be addressed on a jurisdictional level.

- Continue debates about what preparatory Internet sex acts can or should be criminalized. For example, why isn't solicitation always a crime? Could it be considered a form of criminal threatening within this context? It may be difficult, if not impossible to legislate all types of online sexual solicitations to minors, especially those between similar-age peers.

- Consider model legislation/statutes constructed as "indecent communication with a minor" laws, crafted to address adult/child communication online. This type of legislation may circumvent complications related to enforcing a statute that targets sexual solicitation in general.

- Provide clear messages to parents about what should be reported, and make every effort to assist parents in minimizing minor's exposure to these preparatory acts. Many law enforcement agencies provide preventative training and education for youth and parents. Parents and youth should be encouraged to report preparatory acts, and when possible law enforcement should continue to respond to these reports. However, this could potentially lead to some backlash, if parents infer that police departments are unable to do anything to protect children from solicitations online.

- Assess whether there are characteristics that make these solicitations appear more aggressive. For example, did the suspect visit the victim's town, buy a plane ticket, threaten or harass the victim?

- If online sexual solicitations appear to be potentially dangerous, such as if the offender travels to the victim's home town, law enforcement agents could consider taking on the persona of the minor victim. In that way, investigators may be able to set up a meeting with the offender or to collect enough evidence of criminal threatening to arrest the suspect.

- Continue to use grooming evidence to support a victim's testimony or provide more information about offending behavior. Although these actions are not considered criminal in and of themselves in the United States, British lawmakers have recently endorsed legislation directed at grooming behaviors on the Internet (Kelland 2003).

- Careful consideration needs to be undertaken as to whether fantasy claims can be criminalized without infringing on First Amendment rights. For example, consideration could be given to the specificity of the fantasy and any actual steps taken by an offender (i.e., did the offender send the victim a plane ticket, did the offender make any specific plans to visit the victim's home?).

Dilemmas related to victim "age of consent"

Is it a crime for a 21-year-old female to travel to the United States from a neighboring country to have sex with a 16-year-old male? Under what conditions can a juvenile "consent" to having sex with an adult?

In about four percent of I-CIV cases, investigators are unable to prove that a crime occurred because of a victim's age. If police learned that a victim in a case was old enough to give consent to sexual activity and gave that consent, there may be no crime. Victim age was a dilemma in a case involving a 33-year-old male and a 17-year-old female:

The juvenile posted a personal ad online, in which she claimed to be 22-years-old. The adult responded to the ad, and the juvenile told him that she was 18. They met once in a movie theater, and again at the victim's house. The case came to police attention when the juvenile's parents came home late one night and found the adult and the juvenile putting their clothes on in her room. The parents found a metal ring, a rope, and a camera on the couch. The victim said that the sex was consensual and was not interested in pressing charges.

In this instance, the victim was 17, which was old enough to consent to sexual acts with an adult in that state. Had the victim been 13, or had the state statute defined a minor as under age 18, the outcome may have been different. However, the based on the facts of the case, no crime occurred.

There is no societal or legal consensus regarding the age at which teens can consent to sex (Elstein and Davis 1997). There is some consensus that children under the age of 15 are "neither legally nor developmentally capable of consenting to sexual relationships with adults" (Elstein and Davis 1997:1). All states specify an age at which a juvenile is considered too young to consent to sexual acts under law, but that age varies widely (Elstein and Davis 1997). Statutory limits for age of consent range from 14 (Hawaii) to 18 (Arizona, Utah, and others), and the majority of states protect children until 15, 16, or 17 years of age (Elstein and Davis 1997). If a juvenile is older than the age of consent and agrees to have sex with an adult, it may be difficult for law enforcement investigators to move ahead with a case. Internet sex crimes in which victims and offenders meet online may illustrate specific dilemmas about marginal cases in which victims are at or near the age of consent. For example, no arrest was made in a case in which a 16-year-old female victim traveled to another state and had sex with a 51-year-old, married, adult, male offender:

The suspect responded to an ad the victim put out on a BDSM (Bondage, Discipline, Sadism, and Masochism) website, advertising herself. The suspect talked to the victim's foster mother and convinced her that his home was a "safe place to come." The victim flew to the suspect's state and lived as his "sex slave" for a period of time. Investigators found one image of the victim naked on the offender's computer. The victim turned 16 during the investigation, which was the state's age of consent, and so no arrest was made in the case. The investigator stated that the victim's age was the primary problem for the investigating agency and that the victim "knew what she was getting into, so her credibility was not good." This 16-year-old had been the victim in two or three other crimes investigated by this agency. They were not able to charge the suspect in this case with any crime, due to the victim's *age, as well as weaknesses in her testimony. The respondent noted that the victim returned home, and has continued to communicate with the suspect online.*

This case raises several questions regarding law enforcement decisions in cases involving identified minor victims. For example, how vigorously should age of consent laws be applied? The suspect in this case was not charged with a sex crime, since the victim turned 16 during the investigation and appears to have acted consensually. However, it would seem that investigators may have been able to charge the adult with sex crimes that occurred before the juvenile turned 16 or even after she turned 16 since the crime occurred when she was underage.

It is conceivable that under different circumstances, police would have pursued this case. There may have been an arrest if the offender had used force or coercion to lure the victim away, or if there had been some significant power or authority differential between the victim and offender. The investigator stated that the victim "advertised" herself, which may have impacted the case outcome.

If victims are at or close to the age of consent, their age may influence the likelihood of arrest in these online meeting cases. At the same time, other victim issues may also impact these investigations.

Remedies related to age of consent

While others have debated age of consent issues (Elstein and Davis 1997), the impact of the Internet on these crimes has not been addressed. The remedies suggested here are intended to address dilemmas in cases with an Internet nexus, but may apply to other cases as well.

- Consideration of whether uniformity in age of consent statutes is advisable or feasible. A revision in the minimum age requirements was suggested by Elstein & Davis (1997). They suggest that such revisions focus on girls, and state that there should be statutory protections for girls ages 10-15 (in particular those having sex with men over the age of 20). Statutory uniformity could clarify at what age a minor can legally consent to sexual activity, regardless of the jurisdiction in which the crime occurs. Alternatively, such uniformity may lead to laws that do not adequately address or reflect community standards or existing state statutes.

<u>Other proof issues</u>

Other proof issues can also create challenges for law enforcement investigators (9% of the dilemmas reported here). As one example, digital evidence can often provide proof of a criminal act in computer crimes. An offender may take digital photographs during a sexual abuse of a juvenile victim and save them on a computer, allowing law enforcement to retrieve those images and use them as evidence. However, in order to collect this evidence, law enforcement agents must be able to access the files on a suspect's computer. Evidence collection was a significant problem in a case (1213) involving an allegation that a 56-year-old male gave his foster daughter and two of her friends (all 11 years old) a digital camera to use at a slumber party at his house:

One of the girls told her mother that her friend's foster father asked the girls to take pictures of each other and then put the images of her on his computer. The victims reported that they took about 30 photos over 45 minutes. Law enforcement *believed that the images were sexual in nature and went to talk with the suspected offender. However, they were not able to collect any evidence in this case, because when they arrived at the suspect's house, his wife told them that her husband "took his computer fishing and came home without it." Nor were they able to interview the suspect. The investigator reported that while law enforcement agents were talking to the suspect's wife at the front door, the suspect committed suicide in the back of the house. Investigators wanted to interview the suspect's foster daughter, but the suspect's wife would not allow the girl to talk to law enforcement. The investigators were not able to build a case without the computer evidence, an interview with the suspect, or the victim's testimony.*

If the only evidence of a crime is assumed to be on a computer, law enforcement agents must be able to view the evidence in order to proceed with a case. This example, while extreme in its outcome, is likely also indicative of a number of challenges related to these cases. If police are not able to find any evidence of a crime and cannot interview a suspected offender, the case relies on the testimony of child victims. Without the computer, an interview with the suspect, or testimony from the children involved, it was difficult to move ahead.

Inability to Identify Offenders

Identifying offenders in I-CIV, I-STULE and I-CHP cases can pose significant challenges for law enforcement. A third of the dilemmas reported in these OBSTACLES cases related to challenges in identifying offenders. Law enforcement investigators reported that at lest three specific types of dilemmas make it difficult to identify offenders. These challenges included the following: 1) not having enough information to identify an offender, 2) multiple users for a computer, and 3) passage of too much time to identify an offender.

Not enough information to identify offender

About twenty percent of the dilemmas reported here related to whether or not police could to determine either: 1) who contacted juvenile victims online or 2) who posted or sent images of child pornography over the Internet. As the following case illustrates, police are not always able to narrow down a suspect's ISP account information. Some suspects used "rotating ISP" accounts that change address information, or WebTV connections, which made it difficult for some agencies to track individual offenders:

An 11-year-old female was spending time at home with an illness. Her teacher used a computer program called "CUSeeMe" to connect this girl with her classmates. Using this program, the girl could watch what was happening in her class and could communicate with her teacher and classmates. However, due to a mistake the teacher made in setting up the program, it was not "closed" to others on the Internet. As a result, the girl received several sexually suggestive messages and a picture of an adult penis while communicating with her class. The victim deleted the images from her computer, and the investigator reported that the ISP provider did not have any information about the suspect. The investigator believes that the suspect in this case may have been able to see the girl as a function of CUSeeMe.

In this I-CIV case, there was not enough information available to identify the offender. The respondent stated that it might have been easier to identify the suspect if he had sent a picture of his entire body, rather than just an image of a penis. The

ISP provider was unable to identify the offender here, but in other cases offenders maintain anonymity by using false names, changing ISP account information, or making other efforts to conceal identities.

Obviously, I-CHP investigations cannot end in arrest if no offender can be identified. In some child pornography cases, offenders cannot be traced online due to technological challenges, changing identities, or other computer issues. In addition, some offenders left town or fled the country and were never contacted by law enforcement. Cases involving possession of child pornography may be problematic if investigators cannot prove that the suspect was the person sitting in front of the computer (Allinich and Kreston 2001). In one such undercover investigation:

An investigator was posing as a 14-year-old girl in a chat room. A 23-year-old male began communicating with the "victim" using Inter-Relay Chat. This suspect sent the undercover agent 55 images of child pornography in a period of 45 minutes. The investigator tried to identify the suspect using various techniques, but was unable to learn more than that the suspect lived in Europe. The investigator did forward the case on to Customs in hopes that they could identify the suspect.

In addition, it is possible that some suspects can "hide" on the Internet by changing their ISP addresses, using anonymous posting, or some other form of identity deception. In other instances, law enforcement may find images of child pornography online, but have no idea of who posted them on the Internet. In other cases, investigators reached a dead end when they learned that there was no way to determine who posted images. This occurred in a case in which an agency received report from the National Center for Missing and Exploited Children:

The report identified three Internet pages with an ISP address near their jurisdiction. The websites contained between 50 and 100 child pornography images in "thumbnails" and "collages." The investigator traced the route of the images using specialized software and identified the original ISP. The investigator met with the service provider and asked the ISP to search their security network. During that search, the ISP found that they had sublet the address in question to a domain that allows people to post things anonymously. As a result, the investigation could not go any further.

In the previous I-CHP case, law enforcement agents discovered images or receive reports of child pornography online, and attempted to trace ownership back to one offender. There may be a multitude of reasons why investigators are unable to locate offenders. For example, one state requires law enforcement agents to prove that a suspect is physically in their state in order to pursue a case.

Multiple Computer Users

Law enforcement investigators also reported that multiple computer users can present offender identification challenges in cases in which there are allegations of child pornography possession. A primary issue in these I-CHP cases involves identifying who downloaded and/or saved child pornography images found on a computer. Five percent of the dilemmas reported by law enforcement investigators related to narrowing down one specific offender. In one case:

A computer shop called a law enforcement agency to report that child pornography had been found on a computer. By the time the police arrived, the owner of the computer was outside of the store. The 52-year-old married suspect was *detained, and consented to a search of his home, car, and office. The suspect was an accountant, and other partners in the firm had access to the computer in question. Numerous images were found in unallocated space on the suspect's computer, but law enforcement investigators could not prove who download them.*

Cases in which a third party, such as a computer repair shop, find images on a computer may be more vulnerable to this multiple user dilemma than other investigations. In cases where third party reports are made to law enforcement, no one has actually seen an offender downloading images, and therefore, forensic examinations have to be able to prove who was actually responsible for the crime.

Too Much Time Passes to Identify Offenders

An additional dilemma in identifying offenders in these Internet crimes is related to "staleness." When police refer to "staleness" in Internet crimes, they generally mean that too much time has passed for investigators to determine who committed a crime. Due to the nature of the Internet, evidence of child pornography crimes can be difficult to retrieve after prolonged periods of time. As one investigator reported, "things happen so fast" in these crimes, and the bureaucratic nature of law enforcement agencies may slow investigations. Computer evidence may be deleted or ISP addresses cancelled by the time that agencies receive reports of alleged child pornography crimes, and therefore too much time may have passed to arrest an offender. Staleness was a dilemma for investigators in a case involving a report of child pornography possession:

During a "custody battle," a child reported seeing a parent access a pornography site on the computer. The child reported seeing the images six years *prior to the report, there were no computer print outs of the images, no discs to consider as evidence, and no concrete evidence that the child had seen the pornography. The investigator in the case felt that the information was so old that they could not pursue it.*

As that case suggests, staleness can be problematic if citizens wait too long to report Internet child pornography cases to law enforcement. Staleness issues can also plague cases initiated by other agencies. For instance, federal agencies and Internet Crimes Against Children Task Forces may investigate specific child pornography websites. Once investigators find that a suspect is downloading child pornography, they will collect information about that suspect's identity, online communications and other evidence. In some cases in this study, federal agencies or ICAC Task Forces contacted investigators to let them know that a suspect lived in their jurisdiction. Generally, investigators at the initiating agency are encouraged to immediately provide the investigators in the suspect's jurisdiction with materials and evidence collected in the online investigation (Astrowsky and Kreston 2001). However, there can be significant delays between initial online acts and the arrival of supporting documents. In one case, a federal agency was investigating everyone who had downloaded child pornography from a specific website:

Federal investigators had a server log listing all of the individuals known to have downloaded child pornography from the site. A law enforcement agency was contacted as a suspect lived in their jurisdiction. By the time the agency did receive information for the federal agency, the case was a year old. When the local agency *attempted to contact the suspect, he had moved. They tried to track him using his Internet Service Provider account, but it was no longer active.*

Basically, any alleged criminal incident will reach a dead end if no offender is identified. Whether a law enforcement agency is investigating a burglary, physical assault, or most other crimes, no arrest can be made without an identified offender. This raises a key question. Are Internet crimes different? Perhaps they are different, in at least one way. The Internet leaves a trail, and with advances in law enforcement investigative techniques and training, it may be increasingly possible for police to follow that trail. It is possible, for example, that offenders in some of these cases could have been identified using additional resources, forensic investigations, or collaborations with other agencies. Alternatively, offenders may be increasingly able to "hide, or conceal digital evidence, and manipulate online identities.

<u>Remedies related to offender identification</u>

In some instances, the characteristics of a case may make it impossible for investigators to identify offenders. However, there may be some remedial steps that could facilitate identifying suspects in Internet sex crimes against minors.

- Advocate for increased Internet service provider compliance with law enforcement agencies.
- Provide specific law enforcement training in identifying Internet offenders.
- Encourage small or rural law enforcement agencies to collaboration with ICAC Task Forces and Federal agencies in an effort to improve suspect identification rates.

- In an effort to remedy staleness issues, develop strategies for quick processing of cases.

Reluctant or Uncooperative Victims

What if juveniles are victims according to legal statutes, but are unwilling to cooperate with a police investigation? Are there specific factors that weaken victim testimony in statutory rape cases?

Even if investigators determine that a juvenile can be classified as a "minor victim" under state statutes, I-CIV cases involving sexual activity between juveniles and adults may pose dilemmas. Eleven percent of the dilemmas noted by law enforcement investigators related to juvenile victims' unwillingness to cooperate with police or concerns that victim testimonies were too weak to proceed with a case.

Victims were seen as uncooperative if they were hesitant to provide evidence of email chat and other online communication, warned the suspect that police were involved, were unwilling to give an account of what had happened, or would only talk to police after significant parental pressure. Arrests were unlikely if victims were unwilling to cooperate with investigators in Internet-initiated child sexual exploitation crimes. One case with a victim the investigator described as not at all cooperative came to police attention during the investigation of a homicide:

A 15-year-old male was identified as a possible victim of an adult male sex ring. This victim lived in a suburban neighborhood with both parents, and had reportedly met one of the offenders in a "Guys for Guys" chat room. Investigators suspected that this 56-year-old adult had sexually abused the minor. The victim did *not want to cooperate with the investigation, in part because he had already testified against 3 or 4 other defendants involved in the sex ring. The victim finally agreed to cooperate after much parental encouragement. Despite the victim's final willingness to work with police, it was decided that the victim's statement was "weak" and the case did not move forward.*

In that case, the male victim's initial unwillingness to cooperate may have influenced the case outcome. It is worth noting that even after the victim gave in to parental pressure and agreed to talk to law enforcement, police determined the victim's testimony was too weak to support arresting the suspect. It appears that both the victim's lack of cooperation and some features of the crime itself impacted the case outcome.

Sexual acts between minors under the age of consent and adults are commonly referred to as "statutory rape" crimes (Davis and Twombly 2000). Although statutory rape is a common term, most state statutes refer to these crimes as "rape, sexual assault, and unlawful sexual intercourse" (Davis and Twombly 2000:1).

Elstein and Smith claim that in general, the legal system provides a "lukewarm response to allegations of sexual misconduct between adults and teenagers" (Elstein and Smith 2000:2). This hesitation to proceed with cases may be related to the strength of the victim's testimony. For example, adolescents may believe that they consented to sexual activity, even if they are not legally able to do so. This was an issue in the following case:

A 16-year-old male told his mother that an adult male he met on the Internet sexually assaulted him. The victim had contracted crabs from this adult offender, *and reported to his mother that this abuse had been going on for over a year (since the victim was 15). After an initial meeting at a train station, the victim and offender met multiple times at the offender's home, which was in another state. The respondent in this case stated that the state taskforce was not interested in the case, and that no law enforcement agency in the offender's state was ever contacted. The law enforcement investigator stated that the victim was initially "not cooperative," but that he later agreed to give police some email messages from this primary offender. The respondent classified this investigation as a "dead case".*

In this case, it is likely that lack of cooperation by the victim and the fact that he met with the offender on multiple occasions contributed to the investigator viewing this as a "dead case." The investigator may have viewed the victim as consenting to sex, although legal statutes do not allow minors to give such consent. It appears that despite statutory requirements, investigators and prosecutors are hesitant to proceed with some of these cases.

Some Internet-initiated sex crimes may be discounted because the adolescents are not particularly compelling victims, particularly if they appear to have "advertised" online or otherwise initiated online sexual communication with an adult. The nature of these specific cases should be considered within the general legal view of statutory rape crimes.

Elstein and colleagues suggest that the legal system does not prioritize statutory rape cases, and that these juvenile victims are basically ignored (Elstein and Davis 1997; Elstein and Smith 2000). According to this perspective, statutory rape victims are not given the legal support and protection they deserve. If these cases go to trial for example, jurors may not take older adolescent victims seriously (Elstein and Davis 1997).

Remedies related to uncooperative or reluctant victims

The dilemmas noted here could be problematic in statutory crimes with or without an Internet nexus. In general, legal action may be less likely in cases involving victims who are seen as uncooperative or "compliant" (Berliner 2002:3). However, it may be possible to minimize these complications and pursue criminal charges in some of these cases.

- Explore options for working with victims who experienced long-term grooming by offenders, or those who have developed intimate online relationships with adults. In some statutory rape crimes, victims may be reluctant to proceed with a prosecution, or may not be seen by a jury as "sympathetic victims" (Elstein and Davis 1997:1). In order to address these and other issues, specialized law enforcement and prosecution units, victim witness advocates, and the use of multidisciplinary teams, are already utilized in many jurisdictions. Additional remedies could include joint law enforcement/prosecutor training on working with reluctant victims, vertical prosecutions (in which one prosecutor handles a case from beginning to end), and the development of support groups for these victims.
- Examine the feasibility and desirability of mandatory reporting of these crimes. It is likely that mandating the reporting of statutory rape would direct legal attention at these victims of Internet sexual exploitation and could result in additional arrests and prosecutions in cases such as the ones described here.

However, such policies may also mandate action in statutory cases that will receive a more tepid community response. Elstein & Davis note that the general public may not see statutory rape crimes as particularly serious incidents. For example, victims and offenders are basically peers in some statutory crimes, and in others, the "offender" may be the father of the victim's child or a long-term partner of the "victim" (Elstein and Davis 1997).

- Support efforts to educate youth, parents, and the general public on the legal realities in these cases. In most jurisdictions, sex between adults and adolescents is illegal, and although some adolescents may feel that they consented to sexual activity, minors cannot provide such consent.

Training, Resource, and Collaboration Dilemmas

Can investigator training impact the outcome of Internet sex crimes against minors? What resource gaps currently exist for law enforcement agencies investigating Internet sex crimes against minors? What makes it difficult for law enforcement agencies to collaborate in these investigations?

Gaps in training, resources, and collaboration were problematic for the investigators interviewed in this study. About 13% of the dilemmas noted here related to training, resource, or collaboration issues. These dilemmas could be problematic in I-CIV, I-STULE or I-CHP cases.

Gaps in resources and training

Thirteen percent of the dilemmas reported here related to gaps in needed resources or training in Internet sex crimes against minors. In terms of training, it may be that inexperienced investigators underestimate the complexities of crimes with a computer-nexus. Consider the following case:

A *45-year-old male and his adult son were involved in a domestic dispute in which the father kicked the son out of the house. When the son was leaving, he knocked over a box of computer disks and took a few with him. The son took a look at the contents of the disks, and found that they were labeled with titles like, "Young blondes" and contained images the son described as "young naked girls in sexual positions." The son returned the disks to his father, and the two got into another dispute. A local law enforcement agency responded to the dispute, and the son told the officer about the disks. The responding officer asked the father if he had child pornography, and the father answered that he did not. When the agency tried to get a search warrant the next day, the prosecutor would not give them one, believing that too much time had passed and that the suspect had most likely erased the disks. The investigator stated that the responding officer was "young and inexperienced" and should have talked to a supervisor before talking to the suspect.*

Even if investigators have been trained in computer crime investigation, specific cases may exceed the resources of a law enforcement agency. Investigating online crimes can be complex and expensive for agencies, since many of these cases require forensic examinations of computers. Access to computer technology is far from universal within law enforcement, and about 41% of the law enforcement agencies reporting on these OBSTACLES cases reported having no such capabilities. This may be due to the specialized equipment and staff required for forensic laboratories. However, many smaller agencies reported routine collaborations with statewide task forces or larger departments for forensic assistance.

Multi-jurisdictional Cooperation

Multi-jurisdictional collaboration can provide benefits, and can be the key to success in these investigations (Astrowsky and Kreston 2001). For example, agencies can share resources, personnel, expertise, and computer forensic capabilities (Whitcomb and Eastin 1998). At the same time, the multi-jurisdictional nature of these cases can create an entirely new set of dilemmas, as in the following case:

An investigator (Det. A) was contacted by an investigator in another jurisdiction (Det. B). Det. B was involved in a reactive undercover investigation in which a 12-year-old girl was communicating with a male suspect in Det. A's small town. Det. B knew the suspect's name, but that was not enough to move ahead, because Det. A knew two family members with the same name. Det. A had strong suspicions that it was the older of the two family members, a 50-year-old male who police suspected sexually abused his own children in the past. Det. A encouraged Det. B to turn the case over to a federal agency that would be better able to "run with it," but Det. B's agency "would not let us because it was in their jurisdiction." The suspect stopped sending email to Det. B, no arrest was made, and Det. A never heard from that law enforcement agency again.

No arrest was made in the case above, in part due to complications in jurisdictional collaboration. Although there has been little research regarding collaboration between agencies, it is clear that it can present some complications. Multi-jurisdictional collaboration can lead to role ambiguities as agencies attempt to determine which agency will do what aspect of an investigation. There may be venue issues in cases involving law enforcement agencies from multiple states, as investigators evaluate where the crime actually occurred and which state's statutes apply. Finally, there may be disparities in human and forensic resources across agencies. Multi-jurisdictional cases can bring those features quickly to the surface, and may create friction between departments. Perhaps as a result of these complications, some agencies were hesitant to contact other agencies in cases that crossed jurisdictions. This was an issue in a case in which child pornography was found on a 45-year old man's laptop:

The suspect was a wealthy businessman who regularly went from job to job. He had recently been fired from his job and moved to Europe. Soon after, a co-worker found child pornography on the suspect's old computer. The law enforcement investigator and prosecutor decided not to contact a law enforcement agency in Europe. However, before this decision had been finalized, the investigating agency did contact the suspect's new employer in Europe. During that conversation, law enforcement agents indicated the reason for calling.

It is interesting to note that while no other law enforcement agency was contacted in this case, the investigator saw this crime as worth noting to the suspect's new employer. This investigator stated that jurisdictional problems, specifically that there was no contact with a European law enforcement agency, made it impossible to make an arrest in this case.

Multi-jurisdictional investigations can clearly impact the outcome of Internet sex crimes against minors against minors. Not only is it often difficult to establish jurisdiction in Internet sex crimes against minors against minors (Brown 2001b), but there are also challenges related to collaboration among agencies. There may be uncertainty regarding what state has jurisdiction if victims and offenders live in different states, or if a suspect sends child pornography to someone in a neighboring jurisdiction.

These investigations increasingly rely upon a "Task Force Model" of multi-agency teams (Whitcomb and Eastin 1998) and there is general agreement that law enforcement agency task forces facilitate investigations of Internet crimes with child victims (United States Department of Justice 2000). These task forces provide advantages to law enforcement in that they provide "explicit dedication of manpower and resources," as well as a sense of interpersonal support for investigators (Whitcomb and Eastin 22). They typically involve state, local, and federal network of law enforcement professionals, often from multiple jurisdictions (Klain et al. 2001).

Once it is clear which jurisdictions could have an interest in the case, there may be benefits and/or complications related to collaboration. With the assistance of a task force or another agency, investigators may be able to pursue cases that would otherwise fall beyond the agency's reach or charge an offender with stiffer penalties. Alternatively, when agencies are required to work together on a case, it may exacerbate other problems, such as turf issues, training needs, and resource availability.

Other Agency Took Over

In other cases included in this study, investigators reported that they passed a case on to another agency that could be better able to follow up with an investigation.

If a case was passed on, the initiating law enforcement agency was often unable to make an arrest. About a quarter of the investigators (17 cases) interviewed for this study noted that some other agency took over a case before the initial agency could make an arrest. Some perceived this passing on of cases as a jurisdictional problem, particularly if they were never notified about the case outcome. Some suggest that passing cases on to other agencies can be an appropriate response in these cases, as cooperation between agencies may facilitate arrest and protect child victims (Astrowsky and Kreston 2001), such as in this case:

A law enforcement agency received a report that a 14-year-old female had been communicating online with a 46-year-old adult. This adult had initially told the victim that he was 18, and she had given him her phone number and her address. Once she learned that he was 46, the victim was upset and told her mother, who then contacted police. The initial investigator was able to track down the offender's identity by obtaining a subpoena for the suspect's WebTV account. This investigator identified the suspect, who lived in another state and operated an online escort service. Once the investigator learned that the suspect lived on the other side of the country, he turned the case over to the FBI. Although the initial agency was unable to make an arrest in the case, the investigator felt that the FBI would be better able to keep an eye on the offender and to deal with the distance involved in the investigation.

Again, it may be that passing on a case such as the one above is completely appropriate and does not actually involve any "dilemma". Law enforcement investigators, however, may view these outcomes as problematic, in that they are unable to arrest a suspect.

Remedies to training, resource and collaboration dilemmas

The suggestions here are proposed for Internet-related sex crimes against minors, but could also be beneficial in other types of investigations involving multiple law enforcement jurisdictions.

- Increase opportunities, training, and funding for linking organizations and collaborating with existing Internet Crimes Against Children Task Force agencies.
- Encourage smaller law enforcement agencies and those in rural areas to reach out to state, federal or ICAC resources when presented with Internet crimes involving minors.
- Support additional research into multi-jurisdictional collaboration, such as what works and what needs work? What facilitates formal and informal collaboration?
- Investigate alternative models for sharing information between agencies. Models could be developed so that when agencies pass cases on to other jurisdictions, they can expect to hear back about the case outcome as in medical models of collaboration. These efforts would allow agencies to share information, and also to share in the "glory" or the recognition for the case.

Comparison of Dilemmas in OBSTACLES & N-JOV Cases

There is little empirical evidence regarding the dilemmas involved in investigating Internet sex crimes against minors, and therefore a primary focus of this study is to identify specific challenges related to investigations of these crimes. As noted, investigators reported 101 dilemmas in these 68 Internet sex crimes against minors. The challenges reported by law enforcement agents appear to vary according to the type of case, the characteristics of the individuals involved, and the legal context within which the incidents occur.

The dilemmas noted here were derived from a qualitative analysis of interview summaries. Case summaries were analyzed for all cases in which police were unable to arrest a suspect in an Internet Sex Crime Against a Minor. A key question is whether or not these dilemmas are empirically related to case outcome (such as arrest versus non-arrest) in this sample of law enforcement investigations.

In an effort to answer that question, measures of each of these dilemmas were examined for both OBSTACLES and N-JOV cases. These bivariate analyses explore whether the dilemmas noted by law enforcement were related to arrest in this sample of Internet sex crimes against minor cases. For this analysis the 68 non-arrest OBSTACLES cases were compared to 464 N-JOV arrest cases.

Since the dilemmas noted previously (proof issues, criminality of preparatory acts, ability to identify offenders, uncooperative victims, and collaboration/training gaps) were derived from a qualitative analysis, the original instrument does not include questions specifically designed to measure all of these issues. As a result, some proxy items from the original instrument were selected here. These measures, which generally reflect the legal context of these crimes, were described in Chapter 2: Methodology. These items may be imperfect measures, but do address some of the issues presented in the proceeding section (Table 9).

Proof issues

Two of the proof dilemmas identified by law enforcement agents will be examined here. The first proof dilemma, defining child pornography, can be problematic in I-CHP cases and I-CIV investigations of child pornography production. To examine whether differences in child pornography definitions related to case outcome, OBSTACLES and N-JOV cases will be compared in terms of child pornography definitions. The second proof dilemma, whether cases were limited to preparatory acts or involved additional actions is a consideration in I-CIV cases.

Definitions of Child Pornography. Law enforcement investigators reported two key dilemmas in I-CHP cases. Investigators shared that cases without graphic images and those involving images of older children presented challenges. To examine whether or not those challenges were related to arrest outcomes, two measures were extracted from the original instrument. These original measures do appear to have face validity in terms of defining child pornography.

Graphic nature of images. As noted in Chapter 2: Methodology, investigators were asked whether child pornography in both the production and possession cases included graphic sexual images, "images that focused on genitals or showed explicit sexual activity." The relationship between possession of graphic images and arrest was consistent with law enforcement investigators' accounts of these investigations.

Cases in which offenders possessed or produced any graphic images were more likely to end in arrest than cases in which an offender did not produce or possess graphic sexual images (Pearson X^2=27.634, p= .000, Phi = .270).

Age of children in child pornography images. Law enforcement investigators were asked to identify specific age groups of children depicted in child pornography. Cases were dichotomized into those involving child pornography with images of children under 13 and those with no such images. There were no statistically significant relations between the age of children depicted in images and arrest outcome.

Criminality of Preparatory Acts. A second proof issue is the criminality of preparatory acts. Again, this dilemma was problematic in I-CIV cases involving some communication between a minor and a suspected offender. Based on the qualitative summaries presented previously, two key features of these crimes could be construed as markers of preparatory acts: 1) Whether or not these cases involve actual meetings between victims and offenders: and 2) Whether or not the case involved illegal sexual activity. As noted previously, law enforcement investigators were asked whether or not a meeting occurred between the victim and the offender in cases in which the parties met online. In online meeting cases as well as those in which the victim and the offender had a prior relationship, law enforcement investigators were asked whether "there was any illegal sexual activity between the victim and the offender." Illegal activity could have included the following kinds of acts: non-contact, inappropriate touching, fondling, oral sex, intercourse or other penetration, or some other type of illegal sexual activity.

Adult offenders met with minor victims and/or engaged in illegal sexual activity in about eighty percent (N=190) of the OBSTACLES and N-JOV cases examined here. The remaining 20% of these cases were limited to preparatory acts. Consistent with law enforcement investigator reports, arrest was less likely in cases involving preparatory acts (Pearson X^2=21.043, p= .000, Phi = .301).

Limited offender information

There is also variation in the amount of offender information available to law enforcement agents. Offender information was collected for both OBSTACLES and N-JOV studies. In about 30% of OBSTACLES cases, investigators were never able to identify a suspect. Basic offender data were collected for each OBSTACLES case, even if there was limited social information available to police. On the other hand, offenders were identified and arrested in all N-JOV cases. Again, in order to make comparisons between missing offender information in N-JOV and OBSTACLES cases, a proxy measure of "limited offender information" was constructed. This measure does not attempt to measure whether or not an offender was identified (only a dilemma in OBSTACLES cases), but rather compares the amount of basic offender social information available to law enforcement investigators across OBSTACLES and N-JOV cases.

If investigators were lacking ANY information about offender age, gender, race, and area in which the offender lives, it was assumed that the gap in social information would complicate arrest. As expected, the cases in which investigators lacked information on offender's age, gender, race, or living area were less likely to end in arrest. Only 35% of the cases in which some of this basic information was available ended in arrest (Pearson X^2=48.149, p= .000, Phi = -.455).

Reluctant or uncooperative victims

In the subset of cases involving identified victims (n=233), investigators were asked two or three questions about victim cooperation. As noted previously, victim cooperation was dichotomized to reflect victims who were either (1) very or extremely cooperative or (0) not at all or somewhat cooperative by the end of the investigation. There were statistically significant differences between victims' levels of cooperation, with over 90% of cases with cooperative victims ending in arrest (Pearson X^2=5.097, p= .024, Phi = .149).

Training/Resources/Collaboration

The original measure asked investigators whether or not they had been able to receive any training in Internet sex crimes against minors. This analysis examines differences between those investigators who reported attending Internet sex crime against minor training and those who were unable to attend training. Investigators were also asked if other agencies were involved in the investigation.

There were no statistically significant differences in training or collaboration and arrest. In terms of collaboration, this may be a result of the complicated nature of collaboration. As noted previously, having additional agencies involved may be an asset or a dilemma for law enforcement agents. This ambiguity may explain why there are no findings here (Table 9). More than 5% of data on investigator training were missing, and examination of a missing data comparison dummy variable was found to be non-significant.

Table 9: Comparison of Dilemmas in OBSTACLES and N-JOV cases

Characteristic (N= 532)	OBSTACLES Cases (13%)	N-JOV Cases (87%)
Proof that a crime occurred		
[a] Defining Child Pornography		
Any graphic images (n=324)***	8% (27)	92% (297)
Image of children under 13 (n=295)	10% (26)	91% (269)
Criminality of Preparatory Acts (N=228)		
Case involved meeting/illegal sex act (n=186)***	7% (13)	93% (173)
Challenges related to identifying offender (N=532)		
Limited offender data (n=39)***	74% (29)	26% (10)
Reluctant or uncooperative victims (N= 200)		
Victim cooperative (n=151)	9% (13)	91% (138)
Training/Collaboration[b]		
Training in Internet sex crimes against minors (n=273)	14% (38)	86% (235)
Multi-jurisdictional cooperation (n=318)	13% (40)	87% (278)

[a] Defining child pornography analyses are limited to cases involving possession or production of child pornography (N= 337 and 328 respectively).

[b] Training and collaboration were measured for all case types (N= 387 and 532 respectively).

* p < .05, ** p < .01, *** p < .001

In conclusion, law enforcement agents described a range of dilemmas that may complicate investigations of Internet Sex Crimes Against Minors. These issues include definitional child pornography concerns, whether preparatory acts can be considered criminal, challenges in identifying offenders, working with uncooperative victims, and training/collaboration dilemmas. Some, but not all of these dilemmas appear to be empirically related to arrest in these cases. Whether or not images are graphic, commission of an illegal sex act or actual meeting with a victim, and gaps in offender information are all significantly related to arrest. A sociological analysis based on Black's propositions may provide a more comprehensive understanding of legal response to Internet Sex Crimes Against Minors.

CHAPTER 5

RESULTS: QUANTITATIVE ANALYSIS OF LAW ENFORCEMENT INVOLVEMENT

A secondary goal of this study is to provide a sociological analysis of arrest and other law enforcement action in Internet sex crimes against minors. Donald Black, M. P. Baumgartner and other sociologists of law have found that social characteristics of victims and offenders often influence legal responses, including arrest (Baumgartner 2001; Black 1980; Cooney 1999; O'Barr 1999; Stanko 1999). The sociology of law predicts that if two crimes occur in the same town, under the same statutes, and have similar amounts of evidence, the social structure of the cases will predict legal outcomes. In terms of Internet sex crimes, this would suggest that if cases occur in a similar legal context, the social characteristics of victims and offenders predict whether or not law enforcement agents make an arrest or take other legal action. Obviously, this view assumes that the social characteristics are known to law enforcement. It is possible that such characteristics are often invisible to law enforcement in Internet sex crimes against minors. Thus, if there were no social information available to law enforcement, the social structure of the case would not influence legal outcomes.

The following analyses explore whether Black's (1976) predictions that the relation between *victim and offender* characteristics, controlling for contextual legal factors, predict arrest and other law enforcement action in Internet sex crimes against minors. In order to limit these analyses to cases in which relationships between victims and offenders could be measured, a reduced data set was produced. This subset included only Internet crimes against identified victims (I-CIV cases). This reduced data set included 28 OBSTACLES cases and 205 N-JOV cases (N=233). In effect, this means that each of these 233 cases involved a victim who was identified and contacted, and an offender who police may or may not have ever contacted. Data were collected on all offenders in both N-JOV and OBSTACLES studies, as law enforcement agents generally know something about offenders, even if they were never located or contacted.

This *identified victim* file was used in all subsequent sociological analyses. These analyses examined relationships between the study's independent variables, selected legal context variables, and five dependent variables. The dependent variables in this analysis include arrest, search, seizure, multiple agency involvement, and overall law enforcement involvement. As noted previously, arrest, search and seizure are all weakly correlated with the involvement of multiple jurisdictions, but this variable does not appear to contribute to an explanation of overall *police involvement.* It may be that other factors, such as where the victim and offender live in relation to each other, predict how many agencies are involved in these cases. There were no significant relationships between any of the independent variables and whether or not multiple law enforcement jurisdictions were involved. As a result, bivariate results are not displayed here, and no multivariate analyses will be conducted with multiple jurisdictions as a dependent variable.

Offender age, victim race, victim gender, victim respectability, relational distance, and vertical distance were selected as independent variables fitting within

Black's theoretical frame. In order to control for the legal context of these cases, the variables derived from the qualitative analysis of law enforcement dilemmas were also included. Many of the dilemmas reported by law enforcement agencies could be considered part of the legal context of these crimes. As argued by Cooney (1999), the social structure of a crime may influence the legal context. However, for the purposes of analyzing this subset of I-CIV cases, all six variables derived from the previous qualitative analysis will be used as controls, or measures of legal context. These control variables include: 1) graphic nature of produced child pornography, 2) whether offenders produced images of minors under age 13, 3) criminality of preparatory acts, 4) missing offender identification, 5) victim cooperation, and 6) investigator training.

Bivariate Analyses

Bivariate cross-tabulation and chi-square results of relationships between all study sociological independent variables, legal context variables, and the primary dependent variables appear in Table 10. The analyses in the previous chapter used the intact merged N-JOV and OBSTACLES file, which includes cases with and without identified victims. The sociology of law examines the relationship between victim and offender characteristics, and therefore, analyses were re-run using the reduced *identified victim* file of I-CIV cases for all subsequent analyses. As noted previously, dummy variables are included if missing values for specific variables totaled more than five percent (offender age, victim respectability, vertical direction, and investigator training).

Sociological variables

Bivariate analyses examined all relationships between sociological variables and type of legal action taken in a case. See Table 10 for a summary of these relationships.

Age of offender. The age of the offender was significantly related to arrest, search, computer seizure, and high legal involvement in these bivariate analyses. About ninety percent of adult offenders were arrested, a difference that was statistically significant (Pearson X^2= 18.205, p =. 000, Phi = .280). Cases in which the offender was an adult were significantly more likely (89%) to result in a search than cases involving minor offenders (Pearson X^2= 8.752, p =. 003, Phi = -.194). A computer was seized in close to 90% of the cases involving a minor offender (Pearson X^2 = 20.91, p = .000, Phi = -.30). In addition, high legal involvement was significantly more likely in cases involving adult offenders (Pearson X^2=39.35, p=.000, Phi = .411).

Race. These results indicate bivariate relationships between victim race and arrest. About ninety percent of cases with White victims ended in arrest, as compared to 74% of cases involving a victim of another race (Pearson X^2= 4.86, p=.028, Phi = .147). As predicted by Black (1976), arrest was most likely in cases in which the victim was White. This generally supports Black's proposition that the social status of victims and offenders predicts the amount of legal involvement (1976).

Victim-Offender relationship/Relational distance. Bivariate analysis suggests that all four dependent variables are significantly related to relational distance. Law enforcement action, in the form of arrest, search, seizure, and overall legal involvement, was more likely if victims and offenders had some prior relationship. Ninety-four percent of the cases in which victims and offenders had a prior relationship ended in arrest, as compared to 83% of cases involving strangers (X^2= 6.54, p =. 011, Phi .168). Cases involving "strangers" met online (79%) were less likely to involve a search by a law enforcement agency than cases in which the parties had a prior face-to-face relationship (94%) (X^2=10.76, p = .001, Phi =.215).

Whether or not a computer was seized was also related to the relational distance between victim and offender in this bivariate analysis. As with arrest and search, computers were seized in fewer cases involving strangers (75%) than those in which the victim and offender knew each other face-to-face (93%) (X^2=12.86, p= .000, Phi = .235). It follows that high law enforcement involvement was more likely in cases in which the victim and offender had a prior face-to-face relationship. Eighty-eight percent of the cases involving family members or acquaintances had high legal involvement as compared to 69% of those in which the victims and offenders were strangers (Pearson X^2=12.84, p=.000, Phi = .235).

These bivariate findings run counter to Black's prediction and other sociological research findings that cases in which parties are strangers are more likely to be subject to legal attention (Black 1989).

Victim-offender income/Vertical direction. Statistically significant relations were found between victim-offender income and arrest, search, and legal involvement. However, dummy variables reflecting missing data in these measures were also statistically significant, suggesting that significant relations may be a function of missing data. For instance, 72% of cases in which data were missing on offender or victim income ended in arrest as compared to 96% of cases in which such information was known to law enforcement (Pearson X^2=29.06, p=.000, Phi = -.353).

Non-significant sociological relations. No statistically significant relations were found between victim gender or victim respectability and type of action taken. It appears that there is little variation in those variables, regardless of the law enforcement action taken.

Legal context variables

Five of the legal context variables identified in the previous qualitative analysis were included as controls in these bivariate analyses. The variable measuring *possession* of images of children under 13 years of age does not apply to this analysis of I-CIV cases, since I-CIV cases include only those child pornography cases in which an offender produced images of an identified victim. This analysis only includes I-CIV incidents, and therefore does not address possession of child pornography. Summaries of relations between these legal context variables and action taken are presented in Table 10.

Production of graphic images. Arrest was more likely in cases in which offenders produced graphic sexual images of children (97%) than in cases involving no graphic images (82%) (X^2= 5.233, p =. 022, Phi = .253). There were no statistically significant relationships between the graphic nature of images produced and search, seizure or overall legal involvement.

Preparatory acts. All four dependent variables examined here have a statistically significant relationship with the nature of these Internet sex crimes against minors. All four outcomes were less likely if cases were limited to preparatory acts. Specifically, these bivariate results suggest that arrest was more likely if there was an actual meeting or illegal sexual activity (93%) than if the incident was limited to a preparatory act (73%)(X^2= 14.59, p =. 000, Phi = .254).

As with arrest, searches were also more likely in cases in which victims and offenders met or had sexual activity (91%) than in those limited to preparatory acts (68%) (X^2=15.60, p = .000, Phi = .263). Investigators were more likely to seize a computer in cases in which victims and offenders met or had sexual activity (88%) than in preparatory act only cases (73%) (X^2=5.90, p= .015, Phi = .162). High legal involvement was also more likely in cases in which the victim and offender met or had sexual activity (83%) than in cases limited to preparatory acts (60%) (X^2=10.88, p=.001, Phi = .219).

Limited offender information. These bivariate analyses suggest a strong statistical relationship between legal outcomes and the amount of offender information available in a case. It is not surprising that law enforcement investigators knew basic offender information in 92% of N-JOV arrest cases as compared to 35% of the OBSTACLES cases (X^2= 48.149, p =. 000, Phi = -.455). While police could make an arrest and not know the type of area in which the offender lives, for instance, it is unlikely that the offender's gender, race or other social information would be unknown. In addition, about half of the cases with limited offender data resulted in a search, as compared to 88% of those cases with more comprehensive offender information (X^2=16.32, p = .000, Phi = -.265).

Cases with limited offender information (59%) were less likely to lead to a computer seizure than those cases in which offender social information was known to law enforcement (86%) (X^2=10.20, p= .001, Phi = .209). Finally, high legal involvement was more likely in cases in which there was offender information available (82%) than in those cases limited offender information (35%) (X^2=19.66, p=.000, Phi = -.291).

Investigator training. Investigator training was significantly related to search, computer seizure, and overall law enforcement involvement in these cases. Law enforcement investigators who had completed some training in Internet sex crimes against minors were more likely to report that a search had been completed in a case (90%) than those investigators with no training (83%) (Pearson X^2=4.10, p= .043, Phi = .146). Cases in which investigators have had some training in Internet Sex Crimes Against Minors (89%) were more likely to result in a computer seizure than those cases in which investigators had no training (74%) (X^2=4.41, p= .036, Phi = .168). In addition, overall legal involvement was reported in a higher percentage of cases (83%) in which the investigator had completed training (Pearson X^2=4.49, p= .034, Phi = .153). Dummy variables accounting for missing training data were included in these analyses and were not found to be significantly related to any measure of action taken. Given the challenges associated with maintaining a chain of computer evidence and conducting computer forensic exams, it is logical that investigators with training would be more likely to conduct a search and seize a computer.

Non-significant legal context relations. These bivariate results find no statistically significant relations between victim cooperation and any of the law enforcement actions examined here.

Table 10: Social and Legal Aspects of Case by Action Taken

	Arrest (88%)	**Search (86%)**	**Seizure (84%)**	**High Legal Involvement (78%)**
SOCIOLOGICAL VARIABLES				
Offender age (N=233)				
Minor Offender (n=15)	100%	50%	25%	25%
Adult Offender (n=218)	90% ***	89% ***	88% ***	83% ***
Don't Know Offender Age (n=7)	0% ***	14% ***	14% ***	0% ***
Victim race (N= 225)				
White Victim (N = 206)	90% *	88%	85%	80%
Other race Victim (N=19)	74%	74%	74%	68%
Victim gender (N=233)				
Female Victim (n = 161)	89%	88%	84%	78%
Male Victim (n = 72)	85%	82%	83%	79%
Victim Respectability (N=233)				
Victim not respectable (n=38)	87%	90%	84%	74%
Victim respectable (n=153)	90%	87%	87%	81%
Don't know (n=42)	81%	76% *	76%	71%
Relational distance (N=233)				
Prior relationship (n=111)	94% *	94% ***	93% ***	88% ***
Strangers (n= 122)	83%	79%	75%	69%
Vertical direction (N=233)				
Victim higher income (n =45)	98%	89%	89%	82%
Victim equal/lower income (n=110)	97%**	92% *	88%	86% **
Don't know (n = 78)	72%***	76%**	74%**	65% ***
LEGAL CONTEXT VARIABLES				
Produced graphic images (N=82)				
Any graphic images (n=60)	97% *	96%	97%	94%
No graphic images (n=22)	82%	96%	96%	82%
Preparatory acts (N=226)				
Preparatory act only (n=40)	73% ***	68% ***	73% *	60% ***
Meeting or illegal sex act (n=186)	93%	91%	88%	83%
Limited offender data (N=233)				
Offender data limited (n=17)	35% ***	53% ***	59% **	35% ***
Offender data available (n=216)	92%	88%	86%	82%
Victim cooperation (N=220)				
Victim not cooperative (n=69)	84%	87%	87%	73%
Victim cooperative (n=151)	91%	87%	83%	82%
Investigator training (N=191)				
No training (n=35)	89%	83%	74%	69%
Yes training (n=122)	89%	90%*	89% *	83%*
Don't know (n=34)	79%	77%	79%	71%

* p≤ .05, ** p ≤ .01, *** p ≤ .001

Multivariate Analysis

All variables in this analysis are categorical, and therefore a series of logistic regression analyses were conducted to examine arrest, search, seizure, and overall legal involvement outcomes. All independent and control variables were included in initial logistic regression models, but appear to contribute to model instability. Therefore, only those independent and control variables identified as significant predictors in bivariate analyses were included in multivariate models.

The multivariate analyses presented here used search strategies for selecting variables that may impact protection against a Type I (overinterpreting results) error. Since these analyses use only those relationships that were significant at the bivariate level, it is possible that the findings may "exploit chance patterns in the sample at hand, leading to conclusions that do not apply to other samples or to the population" (Hamilton 1992:83).

A series of diagnostic tests were conducted prior to entering these variables into a multivariate analysis. To test for problems with multicollinearity, a correlation matrix of independent and control variables was examined to see if there were any high correlations. This analysis suggested that only victim/offender age and relational distance (r. 538) were moderately correlated. As a more definitive test, these two independent variables were regressed on each other (Hamilton 1992). The R^2 of .2456 suggests that these two variables are related, but it appears that each variable does contribute independently to explaining variations in these dependent variables.

Although multicollinearity does not seem to be an issue with this data, it does appear that high discrimination is a problem with at least one sociological variable (Hamilton 1992). Diagnostic tests revealed that offender age does not vary across arrest outcomes and therefore cannot be included in all multivariate analyses. One-way discrimination was problematic when offender age was included in multivariate analyses with arrest and high legal involvement, since none of the OBSTACLES cases involved minor offenders.

Multivariate analyses can yield unstable models if there are not enough cases in each combination of values (Long 1997). The graphic image production variable was dropped from logistic regression analyses because no graphic child pornography was produced in cases with upward vertical direction, non-White victims, or offenders under 18. One case involving a male victim and one case in which there was no prior relationship involved the production of graphic child pornography.

In addition, there was not enough variation in "limited offender information" to include that variable in a multivariate analysis. Specifically, offender information was available in all cases with upward vertical direction, all cases involving prior victim/offender relationships, and all cases in which an offender produced graphic child pornography. These are not surprising findings, but make it impossible to include *limited offender information* as a control variable in multivariate analyses.

Nevertheless, these analyses provide a statistical overview of the relationships between sociological variables suggested by Black (1976), the legal context of the crime, and measures of legal action in Internet Sex Crimes Against Minors. Table 11 includes a summary of these results. Since the incidence of all legal outcomes examined here was over 10%, odds ratios over 2.5 and under 0.5 may be inaccurate estimates (Zhang and Yu 1998). As suggested by Zhang and Yu (1998), relative risk ratios were calculated to correct odds ratios.

Offender age

These logistic regression analyses find that the age of the offender is a statistically significant predictor of search and seizure (and did not vary across arrest or overall legal involvement outcomes). Law enforcement agents were almost 11 times more likely to conduct a search if the offender was an adult, taking into consideration the relationship between victim and offender and the nature of the criminal act.

If a case involved an adult offender, law enforcement investigators were about seventeen times more likely to seize a computer, taking into consideration whether the victim and offender had a prior relationship, the nature of the act, and whether or not an investigator had specialized training.

Victim race

The race of the victim was not a statistically significant predictor of any of the legal actions examined here.

Prior relationship

The relationship between the victim and the offender was a statistically significant predictor of law enforcement searches, computer seizure and overall legal involvement. Law enforcement agents were 1.03 times more likely to conduct a search if victims and offenders had a prior relationship. Family/acquaintance cases were 1.04 times as likely to yield a computer seizure and 1.11 times more likely to involve high legal involvement (if other variables stay the same).

Victim-offender income

The relation between victim and offender income was not a statistically significant predictor of any type of legal involvement.

Preparatory acts

Whether or not a case involved an actual meeting or an illegal sexual activity predicted arrest and overall legal involvement. The odds that an arrest was made in a case were two times higher if a case involved a meeting between a victim and offender or an illegal sexual act, all other factors being equal. Cases in which a victim and offender met or that included illegal sexual acts were 2.27 times more likely to lead to high legal involvement, controlling for other variables.

Investigator training

Investigator training was not a statistically significant predictor of any type of legal action in this analysis.

Table 11: Logistic Regression of Arrest, Search, Seizure, & Legal Involvement

Variables	**Arrest (88%)**	**Search (86%)**	**Seizure (84%)**	**High Legal Involvement (78%)**
Sociological Variables				
Adult offender	---	10.85[a†]***	17.25[a†]***	---
White victim	2.22[a]	---	---	---
Family/acquaintance relationship	1.71	1.03[a]*	1.04[a]***	1.11[a]*
Victim income equal/less than offender	1.00[a††]	1.15	----	.94
Legal Context Variables				
Actual meeting or illegal sexual act	2.01[a]*	2.14	.85	2.27*
Investigator completed training	---	.99	.99	.99
Model Chi-square	X^2=29.45***	X^2= 40.40***	X^2=51.77***	X^2= 21.53***
Pseudo R^2	.21	.22	.27	.09
Correctly classified	91%	88%	88%	80%

[a] Odds ratio corrected to more closely approximate relative risk.

[†] Missing data more than 5% - comparison dummy variable examined and found to be non-significant.

[††] Missing data more than 5% - comparison dummy variable examined and found to be significant.

* $p \leq .05$, ** $p \leq .01$, *** $p \leq .001$

Summary

Bivariate and multivariate analyses show that offender age, family/acquaintance relationships, and the occurrence of meetings or illegal sex acts are related to legal involvement in Internet sex crimes against minors. Some of these relationships are in the direction predicted by Black's theory, and others suggest alternative explanations of legal action.

Offender age

These results suggest that Internet sex crime against identified minors are more likely to receive most types of legal attention if the offender is an adult than if the offender is a minor. The age of the offender was significantly related to search and seizure in both bivariate and multivariate analyses. As predicted by Black (1976) the young are less subject to most types of legal attention. Law enforcement agents were less likely to conduct a search or seize a computer in cases with minor offenders. It may be that legal actions such as search and seizure are less likely with minors, who may still live at home with a parent or guardian. In such instances, police may be able to collect information and case evidence from parents, teachers, or other social control agents in the minor's life, and may be less apt to pursue a search or computer seizure. The small number of minor offenders may have contributed to these results.

Relational distance

This analysis finds that cases involving strangers, or individuals who had no relationship prior to their Internet interaction, are less likely to result in law enforcement search, computer seizure and overall legal involvement. Multivariate analyses suggest that arrest is less likely in cases involving strangers, but that relationship is not statistically significant. The finding that less law is involved in cases where victims and offenders are strangers contradicts Black's proposition that "the more intimacy, the less law" (1989:100) and research showing an inverse relationship between intimacy and legal response. There is at least one possible explanation for this discrepancy; it may be that the nature of the Internet impacts the direction of relational distance.

Perhaps online "strangers" are actually too far removed to be subject to police involvement. In cases in which an adult sexually solicits a minor online, for example, it may be that offenders are practically unidentifiable and socially invisible to law enforcement. Interactions online generally lack visual cues, descriptive features, and other characteristics that may help law enforcement agencies identify offenders in crimes committed by online "strangers." As with some assault victims, police may be more likely to take legal action if victims can identify the offenders (Felson and Ackerman 2001). In some of these Internet sex crimes against minors, "strangers" met online may be impossible for victims or law enforcement to identify.

While these analyses show that offender age and relational distance predict legal action, it should be noted that Black's predictions are based on a premise that crimes occur in legally similar environments. As Cooney notes, social factors "can explain only so much of the variation in case outcomes" (1999:183). It is likely that there is notable legal variation in these Internet crimes with identified victim cases. It appears that these investigations do vary according to the legal seriousness of the crime and the amount of offender information available to law enforcement.

Preparatory acts

Whether or not an act could be considered preparatory was a predictor of all four types of legal action in bivariate analyses. Multivariate analysis shows that whether or not a case involved preparatory acts was a statistically significant predictor of arrest and high legal involvement. Online solicitations and other cases with no actual meetings or sexual acts were less likely to end in arrest than cases in which meetings or illegal sexual acts occurred.

Insignificant variables

This study finds that four sociological variables (victim gender, victim race victim respectability, and relation between victim and offender income) are not related to the legal outcomes examined here. Cases involving White victims, female victims, victims with prior criminal or run away history, and those victims with incomes higher than offenders were no more likely to receive legal attention than other cases. In part, this may be a function of the Internet-nexus. If some social characteristics are "invisible" or hidden online, it is unlikely that they would impact arrest or other legal actions. Investigators may question the veracity of some social characteristics, realizing that they could have been "created" by an offender or victim as a part of an online persona.

Four of the five legal context variables included in the initial bivariate analyses are not related to these legal outcomes. Investigator training was related to search, seizure, and overall legal action in bivariate analyses. However, multivariate analyses did not find training in Internet sex crimes against minors to be a predictor of any type of legal action. Two other legal context measures, the production of graphic images and limited offender data were significant at the bivariate level, but could not be included in multivariate analyses due to insufficient case variation yielding unstable models. Victim cooperation did not differ significantly for any type of legal action taken in these cases.

Conclusion

These findings provide some support for sociological theories that social structural characteristics are predictors of law enforcement action if legal context factors are held constant, but also suggest some contradictions. These results support predictions that young offenders are less likely to attract legal attention (Black 1976; Cooney 1992). Such findings may point to legal discrimination based on social characteristics in the manner predicted by Black (1989).

This study also finds that the relationship between victims and offenders predicts legal action, but not in the way the sociology of law hypothesizes. The sociology of law suggests that cases involving intimates are less likely to attract legal attention than cases between strangers (Black 1976). Cases in this study were more likely to involve most types of legal action if the victim and offender had a prior relationship. However, gaps in evidence rather than social discrimination seem to explain these findings. It appears that there may not enough evidence to move ahead with a case if the offender is a stranger in some Internet sex crimes against minors.

The findings suggest that whether or not a case is preparatory is a better predictor of arrest than the offender's age, the victim's race or the victim-offender relationship. Internet crimes against identified victims are more likely to involve a search if the offender is an adult and if the victim is a family member or acquaintance of the offender. Perhaps adult offenders are seen as more "dangerous" than minor offenders, and are therefore less likely to be subject to legal action. Legal guidelines for adult/minor crimes may also be more defined or clear than those related to offenses between minors.

These findings show that whether or not a computer is seized is a function of offender age and the victim/offender relationship. It may be that law enforcement can more easily access computer evidence if the victim and offender have a prior face-to-face relationship. Again, these results do not support Black's proposition that more intimate relationships attract greater amounts of law (1976). In fact, it appears that seizure of a computer is more likely if the victim and offender knew each other prior to their Internet communication. Higher levels of legal involvement were found in cases with actual meetings or illegal sex acts.

In conclusion, these results suggest that both the social structure and the legal context of Internet sex crimes against minors predict legal action. Some of the relationships presented here are in the predicted direction and others are not.

CHAPTER 6

DISCUSSION

This analysis finds that law enforcement agents face multiple dilemmas in investigations of Internet crimes against minors. Specifically, there are challenges related to defining child pornography, determining the criminality of preparatory acts, identifying offenders, some victim or offender characteristics, and collaboration between law enforcement agencies. These findings have both practical and theoretical implications.

Implications for Law Enforcement

Child pornography images

These findings suggest that at least two dilemmas, the nature of child pornography images and the age of children depicted in the images, present challenges for law enforcement. Investigator case summaries and case characteristics provide evidence that graphic child pornography images and those depicting minor victims are more likely to lead to legal action. Cases involving less graphic images, such as those depicting nude or partially clothed children in sexually suggestive poses, are less likely to end in arrest. Similarly, images of adolescents are less likely to be categorized as child pornography.

This finding should be considered within the ongoing debate regarding the nature of child pornography. Child pornography has been described as a misnomer (Edwards 2000) for what are generally considered to be evidence of an illegal sexual act involving a minor. At the same time, some argue that creating overly broad definitions of child pornography will infringe on civil liberties (Peron 2003). These findings suggest that some law enforcement investigators are cautious in their interpretations of child pornography.

Implications related to defining child pornography. Two primary implications are evident from this analysis. First, investigators charged with ascertaining whether or not to proceed in a child pornography case need clear guidelines regarding what constitutes illegal images. This analysis identifies a need for clarification regarding child pornography definitions and dissemination of that information. Ideally, uniform definitions could be created, so that images identified by one jurisdiction as child pornography would be recognized by other jurisdictions as illegal.

A related implication is that law enforcement agencies could reinforce existing infrastructure, such as the emerging database of child pornography images or the use of expert witnesses, to support child pornography investigations. Given the number of child pornography images thought to be replicated and shared online (Lemmey and Tice 2000) it is probable that law enforcement agencies have already certified that some images can be defined as child pornography. The development of a centralized law enforcement database of images should assist law enforcement agents in their efforts to assure that specific images meet definitions of child pornography.

As an adjunct to such a database, additional consideration should be given to the use of expert witness testimony in child pornography cases. Currently, some law enforcement agencies use expert witness testimony to support allegations that an image meets definitions of child pornography. Such witnesses may testify as to the age of children depicted in images, the nature of sexual acts depicted, or other issues. Once experts certify images, they could be submitted to the centralized database. Such expert witness testimony may not be financially feasible for some smaller law enforcement agencies. Therefore, federal resources could be allocated for expert witness assistance, realizing that images certified as child pornography by smaller agencies could be entered into the national database to become supporting evidence for investigations in other jurisdictions.

Future research on child pornography. Future research could provide additional information regarding the use of expert witness testimony in these cases. Little empirical evidence exists regarding the use of expert witness testimony across law enforcement jurisdictions or the nature of such testimony. Given the current controversy regarding use of the Tanner scale to ascertain child age in child pornography images (Rosenbloom and Tanner 1998), research could identify a revision or modification of the Tanner scale designed to address current limitations.

Additional research could also explore challenges related to identifying victims in child pornography images. At this time, a primary emphasis is on identifying offenders suspected of possessing or distributing child pornography. In concert with those efforts, research could examine strategies currently being used in and outside of the United States to identify victims depicted in child pornography.

Identifying offenders

This study suggests that identifying offenders can be problematic in some Internet sex crimes against minors investigations. In Internet child pornography cases, investigators may locate an image, but be unable to identify the person who posted or sent the image. Clearly, some offenders can be tracked online, by obtaining a subpoena for Internet service provider information or other methods. In Internet crimes with identified minor victims, email correspondence can provide some offender information as well. However, there are a number of issues that complicate offender identification in cases with identified victims.

As noted here, there are challenges related to obtaining information from Internet service providers, either due to time delays or other problems. Even if investigators are able to contact a victim in these crimes, it may not always be possible to identify a specific offender. These results find that this is particularly problematic if the victim and offender were strangers prior to their Internet communication. In fact, each type of legal action examined here was less likely if victims and offenders were strangers prior to any online communication.

Implications related to identifying offenders. A primary implication is that if a victim and offender know each other prior to an Internet sex crime, it is easier for investigators to identify suspects and take legal action. If victims and offenders are "strangers" except for their online communication, ascertaining the offender's identity can be more challenging. In some instances, an offender sexually solicits a minor, but the minor never actually meets the adult. In such circumstances, investigators may not have any descriptive information about that suspect. Clearly some aspects of digital investigation, such as retrieving email communications or tracing a suspect's Internet service provider account information, can facilitate offender identification. Nevertheless, Internet interaction lacks many of the social and visual cues that could assist investigators in identifying offenders.

Dilemmas related to identifying offenders may not be different from other types of law enforcement investigations, in that cases with missing offender information could present challenges on or offline. However, some features of the Internet, such as anonymous posting of child pornography images or ability to conceal real identities online, do appear to create specific challenges for law enforcement.

Future research on offender identification. Additional research could evaluate what specific improvements could assist law enforcement efforts to identify offenders online. There is a need for insight regarding what specific technical challenges complicate forensic examinations or other Internet investigative strategies.

Criminality of sexual solicitations of minors and other preparatory acts

An additional dilemma relates to the criminality of some preparatory sex acts, including online solicitation of minors. This study finds that arrest was less likely if cases were limited to preparatory acts. It is clear that sexual assaults, meetings between adults and minors, and actual pornography exchanges are, and perhaps should be, priorities for law enforcement. At the same time, there is room for debate regarding the criminality of some attempted or preparatory acts. In particular, it is worth noting that parents and others are encouraged to report incidents such as sexual solicitation to law enforcement agencies or the National Center for Missing & Exploited Children's CyberTipline (National Center For Missing & Exploited Children).

Implications related to preparatory acts. This study illustrates ongoing dilemmas regarding what types of online actions should be criminalized. At this point, there is no consensus regarding whether or not online sexual solicitation of minors should be considered criminal if there is no actual meeting. There may be a need for model legislation regarding sexual solicitations and other Internet-initiated crimes, or improved public education regarding such incidents. Whether or not these incidents are considered illegal acts, there is a need for additional parent education in terms of preventing and reporting these solicitations.

Future research on preparatory acts. Therefore, future research could address outcomes of parent education efforts as well as reporting of these crimes. It is difficult to estimate how often these preparatory acts occur, since existing data collection systems and databases do not address online victimization of juveniles (Finkelhor and Wells 2003). Questions regarding these types of victimizations could be included in the National Crime Victimization Study or other criminal data sources to assess how often these crimes occur and how often they are reported to law enforcement.

Victim/offender characteristics

This study suggests that at least two social characteristics are related to legal actions in Internet sex crimes against minors. In cases in which both victims and offenders were identified, offender age and the relationship between victims and offenders were related to legal outcomes.

Age. Cases that involved minor offenders were less likely to involve a search, lead to a computer seizure, or generally attract high legal involvement. It is possible that cases in which both victims and offenders are minors are seen as less "serious" or problematic than cases with adult offenders and minor victims. For example, if there is a societal reluctance to regulate (Elstein and Davis 1997; Elstein and Smith 2000) sex between minors, it may be that these cases are not a legal priority.

Implications related to offender age. These findings imply that cases with juvenile offenders are less likely to be seen as legally serious. As noted by Black (1976), minors are generally less subject to legal action, in part because they are still largely under the control of family systems. As a result, victims and law enforcement agencies may seek out more informal solutions, and avoid legal actions. From a legal perspective, however, these cases are crimes, regardless of the age of the offender.

Future research on offender age. Therefore, these findings regarding juvenile offenders in Internet sex crimes against minors deserve additional analysis. Future analysis could examine whether sex crimes between minors tend to have less formal sanctions, or informal consequences. Additionally, research could examine whether or not there is justification for the assumption that sex crimes between minors less "serious" than those between adults. Such research could examine victim outcomes, commission of repeat offenses, or other measures that could inform this debate.

Victim/offender relationship. These findings indicate that cases in which victims and offenders are family members or acquaintances are more likely to result in some types of legal action. It appears that investigations are more apt to lead to legal action if victims knew offenders prior to their Internet communication.

Implications. One implication of this finding is that some online "strangers" may be difficult for law enforcement agents to identify, contact, or otherwise investigate. That legal action is more likely when some relationship existed prior to the Internet may reflect the more general challenges related to identifying offenders. In addition, this finding may highlight current gaps in training for investigators. Perhaps investigations initiated on the Internet require specific investigative skills or forensic techniques not currently available to all law enforcement jurisdictions.

Future research related to victim/offender relationship. While this study suggests that legal action is less likely if victims and offenders were strangers prior to their Internet interaction, additional research is needed to clarify these results. It is unclear, for instance, whether the same dynamic would appear in other computer crimes, or if this finding is specific to Internet sex crimes against minors.

Collaboration, training and resources

This study suggests that the need for collaboration in these investigations poses a problem for some law enforcement agencies. Some agencies clearly benefit from multi-jurisdictional investigations, while such collaboration leads to complications for others. These results also reveal that investigator training can influence whether or not a computer is seized in Internet sex crimes against minors.

Implications for collaboration, training and resources. A primary implication of this study is there is a need to streamline the collaborative nature of these investigations. Some of the dilemmas identified here could likely be minimized if the law enforcement agencies involved shared resources and expertise. For instance, smaller agencies could obtain assistance from Internet Crimes Against Children Task Forces and other specialized units in identifying offenders online. In this way, multi-jurisdictional investigations would benefit from the strengths of the agencies involved. A second implication is that specific types of agencies may struggle during multi-jurisdictional investigations. State and Federal resources could be utilized to offer those agencies assistance or training.

Future research on collaboration, training and resources. Future studies could examine this collaboration between law enforcement agencies to determine what works in these investigations. Additional information is needed regarding the infrastructure of such collaborations and how they could be modified to maximize existing resources.

Implications for the Sociology of Law

This analysis provides insight into at least two sociological questions about Internet sex crimes against minors: 1) *is there variation in the social structure of these cases,* and *2) is the social structure visible in these cases?* These findings suggest that the cases do vary according to social characteristics, although the variation is small. The social structure is visible in some, but not all of these crimes.

There was little variation, for example, in race for victims or offenders. The majority of cases in this study involved white victims and white offenders, making it difficult to examine differences in race relation. This relative lack of variation in Internet sex crimes against minors may be due to uniformity in victims and offenders, or due to the nature of the Internet.

It is possible that online, both offenders and victims can be largely invisible to law enforcement. Offender information was not always visible to investigators in these cases, in part because the Internet can effectively hide some offender characteristics. In some cases, such as those involving anonymous posting of child pornography images, almost no offender information was available to investigators. Even in cases involving actual victims, information about offender income, employment, marital status, and other social factors was not always available.

To the extent that social characteristics influence legal actions such as arrest, these gaps in social information present significant dilemmas. As a result, the sociology of law would propose that features of the legal context would be more likely to predict arrest than the social structure of a case. However, these findings underscore one challenge in identifying the impact of either social or legal factors. In Internet sex crimes against minors, it is virtually impossible to disengage the social and legal context.

While previous studies of sex crimes have found that legal factors are paramount (LaFree 1981) to the social structure of a case, there may be significant overlap between these two types of variables. As noted by Cooney, evidence can be a function of the social structure of a case (1999). For instance, the relationship between victims and offenders can predict what evidence is actually available to investigators. If victims only "know" offenders online, they may not be able to provide law enforcement with as much information about offenders as if the offenders were family members. Similarly, offender information can be related to victim cooperation. If victims are unwilling to provide any information about the suspect in cases where illegal sex acts have occurred, law enforcement may not be able to take action.

Although this study did find statistically significant relationships between several sociological variables and legal outcomes, these findings should be interpreted with caution. There is little variation in the social structure of these cases, and in many instances, social factors were invisible to law enforcement.

Future sociological analyses could use Black's (1976) frame to compare at least two types of crimes. First, comparisons could be made of sex crimes against minors with and without an Internet-nexus. Second, Internet sex crimes against minors could be contrasted with other types of computer crime. These studies could provide evidence regarding the impact of the Internet on social information in these crimes. Such studies should include multivariate analyses that attempt to control for legal context. This may provide some evidence of whether or not social factors can be disentangled from legal context in Internet sex crimes against minors.

Limitations

At least five limitations of this study may affect the validity or the generalizability of these results. First, the sample of OBSTACLES cases in which no arrest was made is small and was selected using quota sampling. Although the original sample of law enforcement agencies was randomly drawn, the actual cases included in the OBSTACLES study were selected using quota sampling. This sampling strategy was used in an effort to obtain equal proportions of cases with and without identified victims, and may mean that cases involving identified victims are over-represented in the OBSTACLES sample. However, the OBSTACLES and N-JOV cases included here had the same proportion of victim cases, likely due to sampling and weighting procedures in N-JOV. Forty-six percent of OBSTACLES cases included identified victims as compared to 44% of N-JOV cases.

Second, cases in which an arrest was made may have been easier for law enforcement agents to remember than non-arrest cases. This may have impacted the initial size of the OBSTACLES sample, as well as the information collected from investigators. In some jurisdictions, no written information is maintained if there is not an arrest, and therefore, investigators based their responses on memory alone. Similarly, since no offender was actually arrest in the OBSTACLES cases, law enforcement investigators often did not know answers to questions about those individuals. These issues likely contributed to gaps in offender information available for analysis, particularly in the OBSTACLES cases.

Third, it should be noted that these cases do not represent the entire population of Internet sex crimes against minors. The cases identified here reflect the cases reported to a sample of law enforcement agencies within a one-year time frame. It is probable that the actual incidence of Internet sex crimes against minors is higher than suggested by these reports.

Fourth, the nature of Internet sex crimes against minors and law enforcement investigations are changing rapidly. Training, advances in forensic capabilities, and novel criminal approaches may mean that some of these dilemmas are obsolete and others have taken precedence.

Finally, this study provides a limited test of Donald Black's propositions. The instruments used here were not designed to capture Black's variables. Ideally, Black's propositions would be tested given cases with similar amounts of evidence, identical legal statutes, or uniformity in terms of witnesses or other third parties involved in the cases. As a proxy here, several variables are included as possible, but clearly imperfect substitutes.

Conclusion

As noted previously, child sexual abuse and child pornography are crimes, regardless of whether they occur with or without a computer nexus. In addition, the emergence of Internet sex crimes against minors has caused some to assert that the Internet is a dangerous place for children (Norland and Bartholet 2001). Future research should provide an assessment of this assertion, and provide an empirical analysis of the impact of the Internet on child sex crimes. The Internet may facilitate the commission of child sex crimes, although it may also provide some protection for child victims (Table 12).

Similarly, the impact of these crimes on law enforcement effectiveness is ambiguous. It is likely that in some ways the Internet has created impediments to online child sex crime investigations, although it has also provided investigators with valuable assets (Table 13).

Internet impact on the commission of sex crimes against minors

The two general crime categories presented here, Internet crimes with identified victims and Internet child pornography cases, may include a range of criminal activities. The Internet may impact these incidents in at least three ways.

Table 12: Possible Internet Impact on Sex Crimes Against Minors

Internet may facilitate criminal offenses by:	*Internet may restrict criminal offenses by:*
1. Allowing offenders mass access to child victims and child pornography consumers, with less initial risk	1. Limiting initial physical access to victims and child pornography consumers by requiring steps beyond initial Internet contact
2. Creating a sense of normative reinforcement among offenders	2. Eliminating the social network and authority factors common in conventional child sex crimes
3. Enabling offenders to deceive victims	3. Younger victims perhaps less likely to be victimized online

First, the ease of Internet access and anonymity of online communication may impact these acts. Online communication is possible for virtually anyone with access to a computer and Internet connection. These social interactions via the Internet are not dependent on familiarity and can be largely anonymous. The Internet has made it possible for individuals to meet, communicate, and develop relationships. In fact, individuals who have never met in person may experience deep and intimate relationships online (Turkle 1995).

This suggests that adult offenders in Internet sex crimes may be able to easily access minors online; potentially developing intimate online relationships with several victims at one time (Brown 2001a). Similarly, child pornography distributors can potentially exchange images with a mass market (Jenkins 2001). Since Internet communications are largely anonymous, an adult who has daily online contact with a number of minors or child pornography consumers may not come to the attention of law enforcement. As a result, the Internet may allow for easier, unregulated access to both child victims and images of child pornography.

Commission of these crimes may also be less risky if the victims or consumers are not physically located in geographic proximity to the offenders. Online, offenders do not need to construct a way to access child victims or physically locate child pornography consumers.

While there is some consensus that the Internet has facilitated access to child pornography (Jenkins 2001), it is unclear whether online interactions have facilitated actual victimizations of minors. It could be argued that the Internet actually minimizes the likelihood of sex crime commission against identified victims, since these anonymous strangers are not generally adults with physical access to the children they meet online. For example, online sexual solicitations are a form of victimization, but generally do not lead to actual sexual assaults without additional steps. The Internet generally requires that offenders make some movement past the initial online contact.

In conventional child sexual abuse cases, for example, an adult could meet and sexually abuse a child in the same interaction. The Internet may provide some form of deterrent for offenders, in that communicating with a minor in a chat room does not necessarily mean that there will ever be a face-to-face meeting.

Second, the Internet may create some sense of normative reinforcement among offenders, who share accounts of child sexual abuse or trade images of child pornography online. Internet communication with others may serve as an informal means of encouragement for child sexual offenders.

Despite the possibility that an offender social network exists online, some computer-mediated child sex crimes may be less likely to involve children and offenders in the same offline social network. These offenders may only "know" a minor through online communication, therefore minimizing issues of power and authority. During online communications, minors may be less likely to yield to social expectations to cooperate with adults or comply with their requests. Minors may realize that sexually explicit comments or requests are abnormal, and choose to end contact with questionable online contacts.

Finally, the Internet may make it possible for adult offenders to act as if they were younger online. Some suggest that the anonymity of the Internet allows offenders to be deceptive about their age, intentions, or other features (Brown 2001a; Stanley 2001). At the same time, younger victims may be less likely to be victimized online, since they are unlikely to engage in ongoing electronic (typing, digital cameras, digital video) communication with offenders. This study and N-JOV results (Wolak et al. 2003a) show that victims who met offenders online were generally adolescents, and are therefore older than many of the victims vulnerable to conventional sexual abuse (Barnett et al. 1997).

Internet Impact on law enforcement investigations of sex crimes against minors

The impact of the Internet on law enforcement effectiveness is equally uncertain. The computer-nexus may pose specific impediments to these investigations, although it is possible that some aspects of the Internet may actually be assets for law enforcement.

Table 13: Possible Internet Impact on Law Enforcement Effectiveness

Impediments to investigations	*Assets for investigations*
1. Crimes may involve multiple law enforcement jurisdictions with different laws and resources	1. Law enforcement agencies can work collaboratively on investigations and maximize resources
2. Investigations require technical expertise in computer forensics and related skills	2. Forensic examinations can provide valuable digital evidence; offenders may underestimate forensic capabilities
3. Victims in these cases may deceive offenders about their age, or could be considered compliant	3. Law enforcement investigators can assume undercover identities online and can unobtrusively observe potential offenders

These investigations generally involve multiple law enforcement agencies and cross over several jurisdictions. Findings from this study suggest that having multiple agencies involved in a case can have mixed effects. Multiple agency involvement may pose challenges for law enforcement, as agencies attempt to identify who should take a primary role in the investigations. On the other hand, law enforcement may benefit from these multi-jurisdictional investigations as agencies maximize collective resources and collaborate on cases.

This collaboration could be particularly valuable in cases that require some form of computer forensic examination. Access to these forensic examinations may pose significant impediments to law enforcement agencies, as crucial evidence in Internet sex crimes against identified victims is often digital. Alternatively, these forensic capabilities can be seen as a tremendous asset to investigators, who can use digital evidence as primary or corroborating evidence in criminal investigations.

The computer nexus also presents some challenges related to online deception and identifying offenders. The anonymity inherent in Internet communication makes it possible for victims and offenders in these cases to be deceptive about ages, genders, or other characteristics. In some Internet sex crimes against identified minors, for example, offenders may believe that they are communicating with an 18-year-old on the Internet, when the victim is really only 15. Alternatively, a 15-year-old victim may believe that an online "friend" is also 15, when in reality the individual is 35 years old. In addition, identifying offenders in Internet sex crimes against identified victims can raise legal complications, as tracing real identities on the Internet may require advanced computer skills or a search warrant for an offender's Internet Service Provider (ISP) address information. Alternatively, anonymity online has proven to be a critical asset in undercover investigations of these crimes. Using computer technology to their advantage, law enforcement agents can investigate Internet sex crimes against minors by assuming undercover identities (such as teenage girls). In online child pornography investigations, law enforcement agents can unobtrusively observe potential offenders.

Continued analysis of the impact of the Internet on both commission and investigation of sex crimes against minors is crucial. While many features of these crimes resemble their offline counterparts, the Internet does appear to present significant challenges for law enforcement. Remedial efforts to minimize these challenges should be considered an essential component of efforts to protect children from sexual victimization on and offline.

REFERENCES

"Child Exploitation Statutes and Legislation." *US Department of Justice*. Retrieved December 6, 2003. (http://www.usdoj.gov/criminal/ceos/statutes.htm).

Aftab, Perry. 2000. *The parent's guide to protecting your children in Cyberspace*. New York, NY: McGraw-Hill.

Allinich, Greg and Susan Kreston. 2001. "Suspect Interviews in Computer-Facilitated Child Sexual Exploitation Cases." *American Prosecutors Research Institute Update* 14:1-2.

Astrowsky, Brad and Susan Kreston. 2001. "Some Golden Rules for Investigating On-line Child Sexual Exploitation." *American Prosecutors Research Institute Update* 14:1-2.

Barnett, Ola W., Cindy L. Miller-Perrin, and Robin Perrin. 1997. *Family Violence Across the Life Span*. Thousand Oaks, CA: Sage Publications.

Bartlett, Richard. 1981. "Of Trains and Torts: A study of the interaction between technology and tort law during the late 19th and early 20th centuries." *Technology in Society* 3:337-347.

Baumgartner, M.P. 1999. "Introduction." Pp. 1-31 in *The Social Organization of Law*. San Diego, CA: Academic Press.

—. 2001. "The Sociology of Law in the United States." *The American Sociologist* 32:99-113.

Berliner, Lucy. 2002. "Introduction: Confronting an uncomfortable reality." *The APSAC Advisor* 14:2-3.

Biegel, Stuart. 2001. *Beyond our control? Confronting the limits of our legal system in the age of cyberspace*. Cambridge, MA: The MIT Press.

Black, Donald. 1976. *The Behavior of Law*. San Diego, CA: Academic Press.

—. 1980. *The Manner and Customs of the Police*. New York, NY: Academic Press.

—. 1989. *Sociological Justice*. New York, NY: Oxford University Press.

—. 1998. *The social structure of right and wrong*. San Diego, CA: Academic Press.

Brown, Duncan. 2001a. "Developing strategies for collecting and presenting grooming evidence in a high tech world." *American Prosecutors Research Institute Update* 14:1-2.

—. 2001b. "Jurisdictional Issues and Internet Service Provider Liability in Computer Facilitated Child Sexual Exploitation Crimes." *American Prosecutors Research Institute Update* 14:1-2.

—. 2002. "Pornography after the fall of the CPPA: Strategies for Prosecutors." *American Prosecutors Research Institute Update* 15:1-2.

Brunker, Mike: 2002. "'Legal child porn' under fire." *MSNBC*. Retrieved September 26. (http://www.msnbc.com/news/default.asp?cp1=1).

Caruso, David B. April 6, 2003. "New catalog will aid in child porn fight." A11 in *Boston Sunday Globe*. Boston, MA

Casey, Eoghan: 2000. "Digital evidence and computer crime: Forensic science, computers, and the Internet." Retrieved April 24, 2002. (http://www.forensic-science.com/decc/decc_forum.html).

Chicago Daily Law Bulletin. 2002. "Criminal law & procedure -solicitation of minors."

Cobb, J Allan. 1996. "An examination of venue issues concerning online crimes against children: What happens when cyberspace is used to lure children into sexual relations-A look at federal venue provisions." *University of Louisville Journal of Family Law* 35:537-554.

Collier, P.A. and B.J. Spaul. 1992. "Problems in policing computer crime." *Policing and Society* 2:307-320.

Cooney, Mark. 1992. "Racial discrimination in arrest." *Virginia Review of Sociology* 1:99-119.

—. 1999. "Evidence as partisanship." Pp. 183-205 in *The Social Organization of Law*, edited by M. P. Baumgartner. San Diego, CA: Academic Press.

Daly, Kathleen. 1999. "Structure and Practice of Familial-Based Justice in a Criminal Court." Pp. 207-226 in *The Social Organization of Law*, edited by M. P. Baumgartner. San Diego, CA: Academic Press.

Davis, Noy S. and Jennifer Twombly. 2000. "State Legislators' Handbook for Statutory Rape Issues." Office for Victims of Crime, U.S. Department of Justice Office of Justice Programs, Washington, DC.

Douglas, Geoffrey 2002. "Jim McLaughlin's Secret War." *Yankee*, pp. 74-82.

Edwards, Susan S.M. 2000. "Prosecuting 'child pornography': Possession and taking of indecent pictures of children." *Journal of Social Welfare and Family Law* 22:1-21.

Elstein, Sharon G and Noy Davis. 1997. "Sexual relationships between adult males and young teen girls: Exploring the legal and social responses." American Bar Association, Washington, DC.

Elstein, Sharon G. and Barbara E Smith. 2000. "Victim-Oriented Multidisciplinary Responses to Statutory Rape: Training Guide." Office for Victims of Crime, U.S. Department of Justice, Office of Justice Programs, Washington, DC.

Farrell, Ronald A. and Victoria Lynn Swigert. 1999. "Prior offense record as a self-fulfilling prophecy." Pp. 389-404 in *The Social Organization of Law*, edited by M. P. Baumgartner.

Felson, Richard B and Jeff Ackerman. 2001. "Arrest for domestic and other assaults." *Criminology* 39:654-675.

Finkelhor, David. 1984. *Child Sexual Abuse: New treatment and research.* New York, NY: Free Press.

—. 1993. "Epidemiological factors in the clinical identification of child sexual abuse." *Child Abuse & Neglect* 17:67-70.

—. 1994. "Current information on the scope and nature of child sexual abuse." *The Future of Children* 4:31-53.

Finkelhor, David and Patricia Y. Hashima. 2001. "The Victimization of Children and Youth: A comprehensive overview." Pp. 49-78 in *Handbook of Youth and Justice*, edited by White. New York, NY: Kluwer Academic/Plenum Publishers.

Finkelhor, David, Kimberly J Mitchell, and Janis Wolak. 2000. "Online victimization: A report on the Nation's youth." National Center for Missing & Exploited Children, Alexandria, VA.

Finkelhor, David and Richard Ormrod. 2001. "Child Abuse Reported to the Police." U.S. Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention, Washington, DC.

Finkelhor, David and Melissa Wells. 2003. "Improving data systems about juvenile victimization in the United States." *Child Abuse & Neglect* 27:77-102.

Grasz, L. Steven and Patrick J. Pfaltzgraff. 1998. "Why and how states may constitutionally regulate the production, possession, and distribution of nude visual depictions of children." *Temple Law Review* 71:609-635.

Hames, Michael. 1993. "Child Pornography: A secret web of exploitation." *Child Abuse Review* 2:276-280.

—. 1994. "A police view of pornographic links." Pp. 197-203 in *Organized Abuse: The Current Debate*, edited by P. C. Bibby. Vermont: Ashgate.

Hamilton, Lawrence C. 1992. *Regression with Graphics: A Second Course in Applied Statistics*. Belmont, CA: Duxbury Press.

Hardy, Richard and Susan S. Kreston. 2002. ""Computers are like filing cabinets..." Using analogy to explain computer forensics." *National Center for Prosecution of Child Abuse Update* 15:1-2.

Holmgren, Brian: 2002. "Translating Science into Law: Lessons from Doctors, Judges, and Lawyers about the Use of Medical Evidence in the Courtroom: The Expert Witness." *Lexis Nexis Academic Universe*. Retrieved June 23, 2003.

Howerton, Amanda. 2002. "The Effects of Victim and Offender Characteristics on the Application of Law." in *Unpublished Master's Thesis*. University of New Hampshire.

Humphreys, Catherine. 1996. "Exploring New Territory: Police organizational responses to child sexual abuse." *Child Abuse & Neglect* 20:337-334.

Itzin, Catherine. 1994. "Pornography and the organization of child sexual abuse." Pp. 167-196 in *Organized Abuse: The Current Debate*, edited by P. C. Bibby. Burlington, VT: Ashgate Publishing Company.

Jenkins, Philip. 2001. *Beyond Tolerance: Child Pornography on the Internet*. New York, NY: New York University Press.

Kelland, Kate: 2003. "Police Hunt Runaway Girl and Ex-U.S. Marine." *Reuters Internet Report*. Retrieved July 15, 2003. (http://www.reuters.com/news.jhtml).

Klain, Eva J, Heather J Davies, and Molly A Hicks. 2001. "Child Pornography: The Criminal-Justice-System Response." American Bar Association Center on Children and the Law for the National Center for Missing & Exploited Children, Alexandria, VA.

LaFree, Gary D. 1981. "Official reactions to social problems: Police decisions in sexual assault cases." *Social Problems* 28:582-594.

Lanning, Kenneth V. 1992. "Child Molesters: A Behavioral Analysis." National Center for Missing & Exploited Children, Washington, DC.

—. 1998. "Cyber Pedophiles: A Behavioral Perspective." *The APSAC Advisor* 11:12-18.

Lanning, Kenneth V and Ann Wolbert Burgess. 1989. "Child pornography and sex rings." Pp. 235-255 in *Pornography: Research Advances and Policy Considerations*, edited by D. Z. J. Bryant. Hillsdale, NJ: Lawrence Erlbaum Associates.

Lemmey, Dorothy E. and Pamela Paradis Tice. 2000. "Two tragic forms of child sexual abuse: Are they often overlooked?" *Journal of Child Sexual Abuse* 9:87-106.

Long, J. Scott. 1997. *Regression Models for Categorical and Limited Dependent Variables*, Vol. 7. Thousand Oaks, CA: Sage.

Lundsgaarde, Henry P. 1999. "Murder in Space City." Pp. 133-156 in *The Social Organization of Law*, edited by M. P. Baumgartner. San Diego: Academic Press.

Maguire, Edward R. 1993. "The Professionalization of Police in Child Sexual Abuse Cases." *Journal of Child Sexual Abuse* 2:107-116.

Marx, Gary T. 1982. "Who really gets stung? Some issues raised by the new police undercover work." *Crime & Delinquency*:165-193.

Mastrofski, Stephen D. 2000. "The police in America." in *Criminology: A contemporary handbook*, edited by J. F. Sheley. Belmont, CA: Wadsworth.

Mastrofski, Stephen D, Robert E Worden, and Jeffrey B Snipes. 1995. "Law enforcement in a time of community policing." *Criminology* 33:539-563.

McCullagh, Declan: 2003. "Supreme Court weighs Net porn law." *CNET News*. Retrieved October 14, 2003. (http://news.com.com).

Medaris, Michael and Cathy Girouard. 2002. "Protecting Children in Cyberspace: The ICAC Task Force Program." U.S. Department of Justice, Office of Justice Programs, Office of Juvenile Justice and Delinquency Prevention, Washington, DC.

Messing, Philip, Angela C. Allen, and Tracy Connor: 2001. "'Kid Porn' Jailer Turned in by Wife." *NYPost.com*. Retrieved 09/06/01.

Mitchell, Kimberly J, David Finkelhor, and Janis Wolak. 2001. "Risk Factors for and impact of online sexual solicitation of youth." *Journal of the American Medical Association* 285:3011-3014.

—. 2003. "The Exposure of Youth to Unwanted Sexual Material on the Internet." *Youth & Society* 34:330-358.

National Center For Missing & Exploited Children: Retrieved September 19, 2003. (http://www.ncmec.org/missingkids/servlet/PublicHomeServlet?LanguageCountry=en_US).

National Center for Prosecution of Child Abuse. 1999. "Child Abuse and Neglect State Statues Elements: Crimes Number 30: Child Pornography." Alexandria, VA.

National Directory of Law Enforcement Administrators. 2001. Stevens Point, WI: National Public Safety Information Bureau.

Norland, Rod and Jeffrey Bartholet 2001. "The Web's Dark Secret." *Newsweek*, March 19, pp. 44-51.

Novak, Kenneth J, James Frank, Brad W Smith, and Robin S Engel. 2002. "Revisiting the decision to arrest: Comparing beat and community officers." *Crime & Delinquency* 48:70-98.

O'Barr, William M. 1999. "Speech styles in the courtroom: Powerful versus powerless speech." in *The Social Organization of law*, edited by M. P. Baumgartner. San Diego, CA: Academic Press.

Perez, Cynthia. 1991. "*United States v. Jacobson:* Are child pornography stings creative law enforcement or entrapment." *University of Miami Law Review* 46:235-261.

Peron, Jim: 2003. "The Claptrap Over Child Porn." *NZ via Europe*. Retrieved May 6. (http://www.freedom.orlingrabbe.com/lfetimes/kiddie_porn1.htm)

Persson, Detective Inspector Anders. 2001. "International Perspectives on Internet Crimes Against Children." in *National Internet Crimes Against Children Training Conference*. New Orleans, LA.

Rosenbloom, Arlan L and James M Tanner. 1998. "Letter to the editor." *Pediatrics* 102:1494.

Ryan, G and S Lane. 1991. *Juvenile sexual offending*. Lexington, MA: Lexington Books.

Schuijer, Jan and Benjamin Rossen. 1992. "The Trade in Child Pornography." *Issues in Child Abuse Accusations* 4:55-107.

Schulz, Dorothy. 1987. "Holdups, Hobos, and Homeless: A brief history of railroad police in America." *Police Studies* 10:90-95.

Smith, Barbara E. 1989. "The multidisciplinary team approach to investigating Out-of-Home child sexual abuse cases." *Response* 22:10-12.

Stanko, Elizabeth Anne. 1999. "The impact of victim assessment on prosecutors' screening decisions: The case of the New York County District Attorney's Office." Pp. 405-416 in *The Social Organization of Law*, edited by M. P. Baumgartner. San Diego, CA: Academic Press.

Stanley, Janet. 2001. "Child abuse and the Internet." *Child Abuse Prevention Issues* 15:1-19.

Taylor, Max, Ethel Quayle, and Gemma Holland. 2001. "Child pornography, the Internet and offending." *The Canadian Journal of Policy Research* 2:94-100.

Taylor, Stuart 2001. "Is it sexual exploitation if victims are 'virtual'?" *Newsweek*, March 19, 2001, pp. 44-51.

The Associated Press: 2002. "Witness: Massachusetts sex abuse victim said she was 18." *The Boston Globe Online*. Retrieved November 24. (http://www.boston.com/).

Turkle, Sherry. 1995. *Life on the Screen: Identity in the Age of the Internet*. New York: Simon & Schuster.

Tyler, R.P. Toby and Lore E Stone. 1983. "Child Pornography: Perpetuating the Sexual Victimization of Children." *Child Abuse & Neglect* 9:313-318.

U.S. Department of Commerce. 2002. "A Nation Online: How Americans are Expanding their use of the Internet." Economics and Statistics Administration, National Telecommunications and Information Administration, Washington, D.C.

U.S. Department of Justice. 2000. "Use of Computers in the Sexual Exploitation of Children." U.S. Department of Justice, Office of Justice Programs, Washington, DC.

United States Court of Appeals for the First Circuit: 1998. "United States, Appellee, v. Paul George Gamache, Defendant, Appellant." *Lexis-Nexis Academic Universe.* Retrieved February 26.

United States Department of Justice. 2000. "Use of Computers in the Sexual Exploitation of Children." U.S. Department of Justice, Office of Justice Programs, Washington, DC.

Wasik, Martin. 1991. *Crime and the Computer.* Oxford: Clarendon Press.

Whitcomb, Debra and Julie Eastin. 1998. "Joining forces against child sexual exploitation: Models for a multijurisdictional team approach." U.S. Department of Justice Office of Justice Programs, Newton, MA.

Wolak, Janis, Kimberly J Mitchell, and David Finkelhor. 2003a. "Internet Sex Crimes Against Minors: The Response of Law Enforcement." National Center for Missing & Exploited Children, Washington, DC.

—: 2003b. "National Juvenile Online Victimization Study (N-JOV): Methodology Report." *Crimes Against Children Research Center.* Retrieved October 19, 2003. (http://www.unh.edu/ccrc/).

Wolak, Janis, Kimberly J Mitchell, and Melissa Wells. 2002. "Impact of the Internet on Crimes Involving Child Sexual Assault and Exploitation." in *Victimization of Children & Youth: An International Conference.* Portsmouth, NH.

Zhang, Jun and Kai F. Yu. 1998. "What's relative risk? A method of correcting the Odds Ratio in cohort studies of common outcomes." *Journal of the American Medical Association* 280:1690-1691.

APPENDIX A

OBSTACLES TELEPHONE SURVEY

OBSTACLES SECTION

CASE ID# **AGENCY ID#**

O1.

We are also interested in the actual investigation of this case. Could you tell me more about the steps in your investigation? **(PROBE FOR INVESTIGATION STRATEGIES)** I'm particularly interested in knowing about any problems that arose during the investigation.

JURISDICTIONAL ISSUES

O2. **Were there any challenges related to jurisdiction?**

97 DK 98 NA/REF 99 NOT APP

O3a. **(IF APPROPRIATE)** You said that ______ other agencies were involved in this case. How would you rate your working relationship with federal agencies (FBI, Postal, Customs, Secret Service)?

1 NOT A GOOD WORKING RELATIONSHIP
2 SOMEWHAT GOOD WORKING RELATIONSHIP
3 VERY GOOD WORKING RELATIONSHIP
4 EXTREMELY GOOD WORKING RELATIONSHIP
97 DK 98 NA/REF 99 NOT APP

O3a1. **Can you tell me a bit about that working relationship?**

97 DK 98 NA/REF 99 NOT APP

O3b. How would you rate your working relationship with the ICAC task force?

1 NOT A GOOD WORKING RELATIONSHIP
2 SOMEWHAT GOOD WORKING RELATIONSHIP
3 VERY GOOD WORKING RELATIONSHIP
4 EXTREMELY GOOD WORKING RELATIONSHIP
97 DK 98 NA/REF 99 NOT APP

O3b1. **Can you tell me a bit about that working relationship?**

97 DK 98 NA/REF 99 NOT APP

O3c. How would you rate your working relationship with other city, county, or state police?

1 NOT A GOOD WORKING RELATIONSHIP
2 SOMEWHAT GOOD WORKING RELATIONSHIP
3 VERY GOOD WORKING RELATIONSHIP
4 EXTREMELY GOOD WORKING RELATIONSHIP
97 DK 98 NA/REF 99 NOT APP

O3c1. **Can you tell me a bit about that working relationship?**

97 DK 98 NA/REF 99 NOT APP

RESOURCE ISSUES

O4. Were there any problems related to resources for investigation in this case?

97 DK 98 NA/REF 99 NOT APP

O5. How would you rate your agency's ability to do forensic examinations of computers?

1 NON EXISTENT
2 POOR
3 FAIR
4 EXCELLENT
97 DK 98 NA/REF 99 NOT APP

O6. I'm going to read a short list of things that are required in some investigations. Were there any problems related to access to any of the following resources?

	YES	NO	DK	NA/REF	NOT APP
O6a. Computer forensic exam DESCRIBE BELOW					
O6b. Additional search warrants DESCRIBE BELOW					
O6c. Expert opinion or witness DESCRIBE BELOW					
O6d. Anything else? **DESCRIBE BELOW**					

____

EVIDENTIARY ISSUES

O7. Were there any problems related to collecting evidence (physical or forensic) or obtaining other information to build this case? **(IF SO, PLEASE DESCRIBE)**

____

____

97 DK 98 NA/REF 99 NOT APP

O8. Does your agency have written protocols specifically for seizing computers?

1 YES
2 NO
97 DK 98 NA/REF 99 NOT APP

O9. Does your agency have written protocols specifically for searching computers?

1 YES
2 NO
97 DK 98 NA/REF 99 NOT APP

LEGAL/ PROSECUTORIAL ISSUES

O10. How closely would you say that you worked with your prosecutor during the investigation of this case?

1 NOT AT ALL
2 SOMEWHAT CLOSELY
3 VERY CLOSELY
4 EXTREMELY CLOSELY
97 DK 98 NA/REF 99 NOT APP

O11. Did you need prosecutor approval for any aspect of this investigation?

1 YES
2 NO
97 DK 98 NA/REF 99 NOT APP

O11a. **(IF YES)** Please describe what prosecutor approval was required.

____

____

97 DK 98 NA/REF 99 NOT APP

O12. In this case, did you need to get an indictment before you could make an arrest?

1 YES
2 NO
97 DK 98 NA/REF 99 NOT APP

O12a. **(IF YES)** Was that because **(MARK ALL THAT APPLY)**

1 ALLEGATION WAS NOT SPECIFIC ENOUGH
2 NEEDED AN EXPERT WITNESS
3 REQUIRED BY LAW IN YOUR JURISDICTION
4 OTHER REASON (SPECIFY) _________
97 DK 98 NA/REF99 NOT APP

O13. Did the prosecutor have specific problems with the case?

____

____

97 DK 98 NA/REF 99 NOT APP

EXPERTISE ISSUES

O14. Has your agency had a similar kind of case in the past, I mean an Internet-related case with a victim who was a juvenile (or I mean an Internet-related child pornography case, etc)?

1 YES
2 NO
97 DK 98 NA/REF 99 NOT APP

O14a. (IF YES) How long ago did your agency have its first case involving an Internet-related crime with a juvenile victim (as far as you know)?

_____ DAYS ______ WEEKS ____ MONTHS ____ YEARS
97 DK 98 NA/REF99 NOT APP

O15. Has your agency/department made arrests in other cases of Internet-related crimes against children (as far as you know)?

1 YES
2 NO
97 DK 98 NA/REF 99 NOT APP

O16. Does your agency have specific protocols for investigating Internet-related child sexual assault or child pornography crimes?

1 YES
2 NO
97 DK 98 NA/REF 99 NOT APP

O17. How long have you (THE INVESTIGATOR) been working on these cases (I mean Internet-related crimes with juvenile victims)?

_____ DAYS ______ WEEKS ____ MONTHS ____ YEARS
97 DK 98 NA/REF99 NOT APP

O18. How would you rate the priority of this case as compared to others in your caseload?

1 NOT A PRIORITY
2 MODERATE PRIORITY
3 HIGH PRIORITY
4 EXTREMELY HIGH PRIORITY
97 DK 98 NA/REF 99 NOT APP

O19. What is your typical caseload size? _____________

O20. How many people are in your unit (or agency if no units)? ______________

O21. How did this case get assigned to you?

____

____

____

97 DK 98 NA/REF 99 NOT APP

Social Status

O22. Was there anything about the offender, such as his/her personal connections, credibility, or willingness to cooperate that impacted the investigation of this case?

1 YES
2 NO
3 OFFENDER NOT IDENTIFIED
97 DK 98 NA/REF 99 NOT APP

O22a What about the offender impacted the investigation? **DESCRIBE BELOW**

____

____

97 DK 98 NA/REF99 NOT APP

O23. **(IF CASE INVOLVED AN ACTUAL VICTIM)** Was there anything about the victim, such as his/her personal connections, credibility, or willingness to cooperate that impacted the investigation of this case?

1 YES
2 NO
3 VICTIM NOT IDENTIFIED
97 DK 98 NA/REF 99 NOT APP

O23a. What about the victim impacted the investigation? **DESCRIBE BELOW**

____

____

97 DK 98 NA/REF99 NOT APP

Child Pornography subsection

O24. **(ASK QUESTIONS ONLY IF CASE INVOLVED CHILD PORNOGRAPHY)** I have a few questions about the investigation and prosecution of child pornography cases in your jurisdiction. (In general) Are there any obstacles to investigating child pornography cases in your jurisdiction?

O25. **(IF NOT ANSWERED ABOVE)** (In general) Are there any legal obstacles to prosecuting child pornography cases in your jurisdiction?

O26. How would you rate the general priority of cases involving the possession (distribution) of child pornography in your agency?

1	NOT A PRIORITY				
2	MODERATE PRIORITY				
3	HIGH PRIORITY				
4	EXTREMELY HIGH PRIORITY				
97	DK	98	NA/REF	99	NOT APP

O27. How would you rate the general priority of cases involving the possession (distribution) of child pornography by your prosecutor?

1	NOT A PRIORITY				
2	MODERATE PRIORITY				
3	HIGH PRIORITY				
4	EXTREMELY HIGH PRIORITY				
97	DK	98	NA/REF	99	NOT APP

CONCLUSION

OCONC 1. Just to clarify, in this case, there were problems involving .... **(OR JUST COMPLETE LATER)**

	YES	NO	DK	NA/REF	NOT APP
OC1a. Things like working with other agencies (Jurisdictional issues)					
OC1b. Time, personnel, equipment (Resource issues)					
OC1c. Warrants, evidence collection (Evidence and case follow up)					
OC1d. Legal/Prosecution issues					
OC1e. Training, access to forensics (Expertise)					
OC1f. Child pornography obstacles?					
OC1g Other obstacle					

OCONC2. Is there anything else that would be important to know about problems that came up in this case that we have not discussed?

____

____

____

____

APPENDIX B

HUMAN SUBJECTS APPROVAL LETTER

UNIVERSITY OF NEW HAMPSHIRE

Office of Sponsored Research
Service Building
51 College Road
Durham, New Hampshire 03824-3585
(603) 862-3564 FAX

PI LAST NAME	*Wolak*	**PI FIRST NAME**	*Janis*
CO-PI or ADVISOR	*Kimberly Mitchell, Co-Investigator*	**APP'L DATE**	*9/5/2000*
DEPT	*CACRC - Family Research Lab - 126 Horton SSC*	**IRB #**	*2402*
OFF-CAMPUS ADDRESS (if applicable)	*Crimes Against Children Research Center, 126 Horton SSC*	**REVIEW LEVEL**	*EXE*
		TODAY'S DATE	*12/6/2002*
PROJECT TITLE	*Survey of Criminal Justice System Responses to Online Victimization*		
MODIFICATON	*Addition of Melissa Wells to Research Personnel*		

The Institutional Review Board (IRB) for the Protection of Human Subjects in Research has reviewed and approved your modificaton and/or addition to this protocol, as indicated above.

The protection of human subjects in your study is an ongoing process for which you hold primary responsibility. **Further changes in your protocol must be submitted to the IRB for review and approval prior to their implementation. If you experience any unusual or unanticipated results with regard to the participation of human subjects, please report such events to this office promptly as they occur.** If you have questions or concerns about your project or this approval, please feel free to contact this office at 862-2003.

Please refer to the IRB # above in all correspondence related to this project. The IRB wishes you success with your research.

For the IRB,

Julie F. Simp

Julie F. Simpson
Regulatory Compliance Manager

Modification entered: *12/6/2002*

cc: File
Kimberly Mitchell, Co-investigator
Melissa Wells, Research Assistant