Sex Offender Law Report

Vol 5 No. 4 | ISSN 1529-0697 | Pages 37 - 52 | June/July 2004

Editor's Note

Child sexual abuse in the Catholic Church is an issue that has come to the forefront of public attention in the past two years. Though reportage of cases increased throughout the 1990s, it was only two years ago, after it was discovered that Father John Geoghan of Boston had allegedly molested more than 100 boys, that it emerged as a "crisis." Various victims' organizations and media outlets claimed that child sexual abuse was occurring in epidemic proportions, while the church claimed that although there were some priests who abused children, this was not an endemic problem. No one really knew how widespread the problem actually was.

In order to better understand the nature and scope of the problem of child sexual abuse by priests, the church commissioned a study by John Jay College of Criminal Justice. Though not intended to be a definitive study on the causes and context of the abuse, this study aimed to determine:

- How many priests had abused victims between 1950 and 2002;
- How many victims had made allegations; and
- How much money the church paid as a result of abuse allegations.

This study, now complete, provides answers. To some, these numbers are shockingly high; to others, too low. Since no other institutions have examined the same issue with the same level of depth, there is no comparable context in which to judge these numbers.

Now that we have the numbers, we need to think about the implications of what is, by any standards, a significant problem. This issue is the basis of two multipart articles in SLR. The first describes the study conducted by John Jay College. (Karen J. Terry, "The Nature and Scope of Child Sexual Abuse in the Catholic Church: The

See EDITOR'S NOTE, page 52

Sex Abuse in the Church, Part I

Charging the Catholics

by Jack S. Furlong*

Editor's Note: *This is the first in a series by Jack Furlong assessing the legal reaction to the sexual abuse crisis in the Catholic Church. This series is inspired by the recent spate of litigation in California following its temporary raising of the statute of limitations. This installment discuses the basis of the issue. The next will explain why raising a statute of limitations is harmful, and an overview of the nature and scope of the problem of child sexual abuse over the last 50 years.*

Perhaps no scandal has raised the bar for community outrage more than the specter of priests abusing their positions of trust by having sex with those in their charge. Since canon law prohibits any form of sexual contact between priest and parishioner or student, every scenario reported brings more opprobrium on the church and its supporters. Sometimes these cases turn out to be trysts with teenaged boys who may have indulged in a little exploration of their own, while others involve taking advantage of women in distress. Disturbing claims have ranged from intimidation-induced sex to the extreme of a drugging and awakening to the amateur pharmacist's fondling.

Competing Interests Affect Attempts to Redress the Assaults

Definition of "Redress." What to do to redress these horrendous, but lamentably no-longer-shocking assaults? Well, it depends on what you mean by "redress." Webster lists several variations, including:

> [T]o set right; rectify or remedy, often by making compensation for . . . SYN[NONYM]. Reparation–redress the balance...see that justice is done.[

Most thinking folk seek an end to predatory priest misconduct. Do you accomplish that end by prosecuting the crime, suing the church, defrocking the priest, or all of the above? Understanding the distinctions in remedies and the social policies driving them is central to crafting a way out of this morass, hopefully with a view to restoring the church to its role as moral compass.

Here is one way to put the competing interests in perspective. Whenever a client walks into my office to describe the complaint against him, I rattle off the list of sanctions he faces if found to have committed the crime alleged. Simply put, every person charged with wrongful conduct faces three avenues of liability simultaneously:

1. Criminal;
2. Civil; and
3. Administrative.

Example From Outside the Realm of Sexual Misconduct. Suppose a teacher gets drunk and drives in a school parking lot, killing a student on his way out. He faces criminal prosecution for manslaughter, drunk driving, and related offenses, facing years of imprisonment in a case entitled something like **People v. Jones**, **State v. Jones**, or even **Commonwealth v. Jones**, in jurisdictions that still use quaint nomenclature,

See CATHOLICS, next page

ALSO IN THIS ISSUE

Crimes Against Children Research Center, University of New Hampshire

Law Enforcement Challenges in Internet Child Pornography Crimes

by Melissa Wells, David Finkelhor, Janis Wolak, and Kimberly Mitchell*

Law enforcement agencies have been investigating child pornography crimes since the mid-1970s. Until the emergence of the Internet, it was believed that police were a step ahead of child pornography offenders. (See P. Jenkins, Beyond Tolerance: Child Pornography on the Internet (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. (See e.g., S. Biegel, Beyond Our Control? Confronting the Limits of Our Legal System in the Age of Cyberspace (2001); P. Jenkins, J. Wolak, K.J. Mitchell, and M. Wells, Impact of the Internet on Crimes Involving Child Sexual Assault and Exploitation (paper presented at Victimization of Children and Youth: An International Conference, Portsmouth, NH, 2002).)

Online sources for child pornography include the following:

- UseNet Newsgroups;
- Bulletin Board Systems (BBS);
- Internet Relay Chat (ICR); and
- The World Wide Web (www).

Types of Internet Child Pornography Cases

This analysis examines challenges related to identifying offenders in 34 Internet child pornography possession and distribution investigations in which law enforcement agents did not make an arrest.

Motivations. Child pornography possessors may collect child pornography for any of the following reasons:

- To validate their sexual interest in children;
- To groom children and lower their inhibitions; or
- To blackmail victims or other offenders. (See, e.g., E.J. Klain, H.J. Davies, and M.A. Hicks, Child Pornography: The Criminal-Justice System Response, Am. Bar Assn Ctr. on Children and the Law for the Natl. Ctr. for Missing and Exploited Children (2001); R.P.T. Tyler and L.E. Stone, "Child Pornography: Perpetuating the Sexual Victimization of Children," 9 (3) Child Abuse and Neglect 313 (1983).)

Others may be motivated to collect child pornography out of curiosity, for sexual arousal, or for similar reasons. Distribution of child pornography involves the dissemination or trading of child pornography images. (See Klain et al., supra, 2001.) 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., supra, 2001.) No cases of child pornography production are included here, as those cases appear to be qualitatively different in terms of offender identification. Offenders in child pornography production crimes may appear in the images, facilitating identification and subsequent arrest. 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.

Variations Among Cases. Although all of the cases included in this study involved a suspect alleged to have collected, traded, or distributed Internet child pornography, the cases varied in several ways. The cases include a range of incidents, such as 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 undercover law enforcement investigations of suspected child pornography offenders.

Internet has Increased Availability. There is some agreement that the Internet has made child pornography available to a wider range of offenders. (See Jenkins, supra, 2001; R. Norlan and J. Bartholet, "The Web's Dark Secret," Newsweek 44 (Mar. 19, 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. (See M. Taylor, E. Quayle, and G. Holland, "Child Pornography, the

See INTERNET, next page

Melissa Wells is an assistant professor of social work at the University of New Hampshire. Her research interests include child victimization, Internet safety, child welfare, and program evaluation. She can be contacted at: 239 Pettee Hall, Department of Social Work, University of New Hampshire, Durham, NH 03824; (603) 862 0076; melissa.wells@unh.edu.

David Finkelhor is the director of the Crimes Against Children Research Center, and also co-director of the Family Research Laboratory and professor of sociology at the University of New Hampshire. He has been studying the problems of child victimization, child maltreatment, and family violence since 1977. He is well known for his conceptual and empirical work on the problem of child sexual abuse, reflected in publications such as the Sourcebook on Child Sexual Abuse (Sage, 1986) and Nursery Crimes (Sage, 1988). In this work, he developed some of the earliest estimates about the prevalence and characteristics of child sexual abuse.

Janis Wolak is a research assistant professor at the Crimes Against Children Research Center of the University of New Hampshire. She is the author and coauthor of several articles about child victimization and the director of the Youth Internet Safety Survey and the Survey of Barriers to Police Reporting and Help-Seeking Among Families of Child Assault Victims.

Kimberly Mitchell is a research assistant professor of psychology at the Crimes Against Children Research Center located at the University of New Hampshire. She received her Ph.D. in experimental psychology in 1999, with concentrations in quantitative methods, women's health, and family violence. Dr. Mitchell's research interests include youth Internet victimization, exposure to violence, and fear of crime. She is coauthor of Online Sexual Solicitation of Youth: Risk Factors and Impact (2001); Online Victimization: A Report on the Nation's Youth (2000); and Risk Of Crime Victimization Among Youth Exposed To Domestic Violence (2001), and has written several other collaborative papers about the incidence, risk, and impact of child victimization.

The authors can be contacted at the Crimes Against Children Research Center, University of New Hampshire, 126 Horton Social Science Center, Durham, NH 03824; David.Finkelhor@unh.edu; Janis.Wolak@unh.edu; Kimberly.Mitchell@unh.edu.

INTERNET, from page 41

Internet and Offending," 2 (2) Canad. J. Pol. Res. 94 (2001).) The nature of the Internet can minimize physical barriers to child pornography trading, for instance, and may facilitate communication between geographically distant offenders.

Law Enforcement Investigations of Internet Child Pornography

It is difficult to gauge the impact of the Internet on law enforcement effectiveness in child pornography investigations. 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 pornography crimes. Investigations of Internet child pornography generally require specific technical expertise and computer forensic examinations, which are not available to all law enforcement agencies. However, computer technology can provide law enforcement with powerful weapons and forensic evidence often lacking in conventional child sex crimes. (See Norland and Bartholet, supra, 2001.) Much of what takes place on the Internet leaves a digital trail, allowing law enforcement agencies with access to computer forensic equipment to collect valuable digital evidence.

Nevertheless, law enforcement investigators run into challenges when attempting to identify distributors and collectors of online child pornography. Clearly, initial detection and subsequent investigation of these crimes is complicated by the fact that individuals can post, access, download, and save images of child pornography from a private computer. Additionally, the Internet can allow opportunities for offenders to be deceptive about intentions, personal history, and even their true identities. Turkle suggests that the Internet allows individuals to try out multiple identities and selves. Online, offenders may conceal their true identities, explore identities online, or modify personal information in an effort to present an alternative persona. (See S. Turkle, Life on the Screen: Identity in the Age of the Internet (1995).)

Methodology

This study examines specific law enforcement dilemmas in 34 investigations of Internet child pornography in which no offender was arrested. Qualitative analysis of data collected as a component of the National Juvenile Online Victimization Study (NJOV) provided insight into specific complications in these investigations. This research 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.

Two-Phase Data Collection Process. The current research 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. One component of this mail survey asked law enforcement agencies if they had investigated any significant—defined as investigations in which the law enforcement agency invested considerable energy and resources—Internet-related child pornography cases in which they were unable to make an arrest because of technical, legal, evidentiary, or other obstacles between July 1, 2000 and June 30, 2001. The initial stratified sample included three frames in order to collect information from agencies specializing in Internet sex crimes against minors, those with training in these investigations, and from a random sample of all U. S. law enforcement agencies. In Phase 2 of the data collection process, interviewers conducted telephone interviews with law enforcement investigators about the sample of the nonarrest cases reported in the mail survey.

By definition, cases in this sample did not end in an arrest. Therefore, those cases may not have involved substantiated criminal activities or "offenders" in a criminal sense. These cases may be called "crimes" instead of "investigations" in this analysis and the term "offender" may be used instead of "suspect" for convenience here.

Challenges in Offender Identification

Law enforcement agents reported that Internet child pornography offenders were difficult to identify for at least three reasons. For example:

1. First, verifying online identities can be challenging in these cases;
2. Second, multiple computer users in some cases made it impossible to prove who had downloaded, distributed, or collected the child pornography; and
3. Finally, delay in case processing impacted law enforcement agents' abilities to identify offenders.

Verifying Online Identities. Law enforcement investigators may find images of child pornography online, but have no idea who posted them on the Internet. Some suspects used rotating Internet Service Provider (ISP) accounts that change address information, WebTV connections, or other technologies that made it difficult for some agencies to track individual offenders. This was the primary dilemma 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.

The Internet allows offenders to be deceptive about intentions, personal history, and even their true identities.

In the previous Internet child pornography case, law enforcement agents received reports and discovered images of child pornography online, but were unable to trace ownership back to one offender. There may be a multitude of reasons why investigators run into difficulty determining who was using a computer. For example, in another case, an investigator learned that a suspect was located outside of the United States. An investigator in an undercover investigation 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

See INTERNET, page 49

INTERNET, from page 42

suspect lived in Europe. The investigator did forward the case on to U.S. Customs in hopes that they could identify the suspect.

Obviously, law enforcement investigators cannot make arrests if no offender can be identified. In some Internet child pornography cases, offenders cannot be traced online due to technical challenges, changing identities, or other computer issues. In addition, law enforcement agents were never able to contact some suspects who fled the country or resided outside of the United States.

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. The main challenge for investigators in these investigations is to prove that the suspect was the person who downloaded or saved child pornography images found on a computer. (See G. Allinich and S. Kreston, "Suspect Interviews in Computer-Facilitated Child Sexual Exploitation Cases," 14 (7) Am. Prosec. Res. Inst. Upd. 1 (2001).) 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 downloaded them.

Cases in which a third party, such as a computer repair shop, finds images on a computer may be more vulnerable to this multiple user dilemma than other investigations. In cases when 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.

Staleness Hinders Identifying Perpetrators. An additional dilemma in identifying offenders in these Internet crimes is "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 Internet service provider (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 printouts 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 specialized 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. 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 (See B. Astrowsky and S. Kreston, "Some Golden Rules for Investigating Online Child Sexual Exploitation," 14 (1) Am. Pros. Res. Inst. Upd. 1 (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 received information from 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.

Implications Related to Identifying Offenders

Increasingly, aspects of digital investigation, such as retrieving email communications or tracing a suspect's Internet service provider account information, can facilitate offender identification. At the same time, such electronic investigations are largely dependent on digital evidence or accessing information from ISPs. In addition, Internet interaction lacks many of the social and visual cues that could assist investigators in identifying offenders.

Dilemmas related to identifying online offenders might 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.

It may be that longer-term retention of ISP records would assist law enforcement agents' efforts to identify suspects, in case offenders frequently change online identities or create new ISP accounts. In cases with multiple computer users, investigators may need to rely on more traditional investigative methods to determine who committed online crimes. Examining patterns of use, determining who had computer access during identified time periods, or other approaches could assist in resolving dilemmas related to multiple users.

Internet Perpetrators Leave a Trail

Clearly, 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. Law enforcement agencies that have the technical skills or forensic resources to examine computer evidence in these cases may be able to retrieve otherwise "invisible" evidence. ■