Child Protection, Exploitation, and Obscenity

March 2004
Volume 52
Number 2

United States
Department of Justice
Executive Office for
United States Attorneys
Office of Legal Education
Washington, DC
20535

Guy A. Lewis
Director

The United States Attorneys' Bulletin is published pursuant to 28 CFR § 0.22(b).

The United States Attorneys' Bulletin is published bi-monthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201. Periodical postage paid at Washington, D.C. Postmaster: Send address changes to Editor, United States Attorneys' Bulletin, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Technical Editor
Nancy Bowman

Intern
Courtney Kane

Internet Address
www.usdoj.gov/usao/reading_room/foiamanuals.html

Send article submissions to Managing Editor, United States Attorneys' Bulletin, National Advocacy Center, Office of Legal Education, 1620 Pendleton Street, Columbia, SC 29201.

In This Issue

Prosecuting Web-based Obscenity Cases

Benjamin Vernia
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

David Szuchman
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

I. Introduction

The pornography industry has capitalized on the growth and popularity of the Internet, and particularly the World Wide Web, as have few other businesses. Although estimates of the volume of Internet pornography are often unreliable, a study from one reputable source estimates that "adult" online pornography generates approximately $1 billion per year in revenues, an amount which is expected to grow to between $5 and $7 billion by 2007. YOUTH, PORNOGRAPHY, AND THE INTERNET, 72 Computer Science and Telecommunications Board, National Research Council (Thornbugh and Lin, eds. 2002). One of the factors contributing to the explosion of pornography on the Internet is the relative anonymity that the Internet affords to producers and consumers alike. Equally appealing to distributors is the ease and low cost of mass distribution afforded by the Internet.

Opposing these forces are concerned parents, with little or no computer savvy, who lack the tools to supervise their children's use of the Internet and exposure to pornography and obscenity. Often, these same parents are unwilling recipients of "porn spam" themselves. Indeed, offensive material that was once largely unavailable to average citizens and children is now largely unavoidable. Finding obscene material on the Internet is as easy as a click of the mouse, and even persons seeking to avoid the material find themselves confronted with it. It is this situation that has led to the Attorney General's call for obscenity enforcement. The Internet's porous borders call for federal prosecution.

While the Internet poses many challenges to obscenity prosecutions, the challenges faced by prosecutors in this area are not very different from the challenges faced in other areas where the Internet is used to commit the offense. Additionally, existing obscenity laws, once developed to address brick-and-mortar retailers, apply equally well to retailers in cyberspace. The recent addition of new legal tools by Congress to specifically target Internet-based offenders complement those existing laws nicely.

II. Overview of the business

Pornographic Web sites can be classified generally by their content and manner of conducting business. In terms of content, Web sites may offer explicit heterosexual or homosexual conduct, or may specialize in a fetish which appeals to a small segment of the population. These include "scat" (depicting the use of feces or urine in sexual conduct), bestiality, sadomasochism, necrophilia, and real or simulated rape. Although child pornography, as that term is defined in 18 U.S.C. Chapter 110, is subject to obscenity laws as well, this article addresses only "adult" pornographic Web sites. There is, however, much overlap in the prosecution of child and adult pornography cases.

Fetish-centered Web sites are often small enterprises, run by one or two individuals (the "webmasters"). Typically, the webmasters of these sites deal in third or fourth-hand pirated copies of material originally collected for their personal use. Although some non-fetish Web sites, particularly online video catalog sites, are also "mom-and-pop" operations, they are more often part of a larger enterprise that includes production operations and parallel retail distribution of their products. These latter organizations are more likely to share the features of a legitimate business, such as operation from a location separate from the webmaster's residence, and the use of a corporate bank account.

Web sites also differ widely in the manner in which they conduct business. A Web site may be little more than an online catalog, providing users with a convenient mechanism for ordering magazines or videos which the retailer then mails or ships to the customer. Conversely, a Web site may offer only online content, pictures, videos, or "chat," and charge by the item or through a subscription fee. Some Web sites offer only advertising space to other pornographic Web sites. Organized as a ranking service of the "best" or

most frequently visited Web sites, they permit advertisers to display sexually explicit "banner ads" that occupy a small portion of the web page.

Marketing and sales practices of pornographic Web sites also differ widely. Many magazines and video producers have established Web sites as an adjunct to, and sales vehicle for, their hard copy products. Other Web sites attract business through the use of "spam" (unsolicited bulk e-mail), or they may trick customers, including children, into visiting their sites through the use of common misspellings of otherwise innocuous domain names. Frequently, Web sites place terms likely to be entered into search engines (such as Google.com) in "metatags," codes stored in the web page but invisible to the user. These terms cause the search engines, which periodically index Web sites, to falsely identify the pornographic Web site as one responsive to the user's innocuous search request.

III. Laws applicable to Web sites

Most of the provisions of 18 U.S.C. Chapter 71, created in response to the brick-and-mortar obscenity trade, are fully applicable to web-based obscenity cases. Those laws include 18 U.S.C. §§ 1461 (mailing obscene matter), 1462 (importation or transportation of obscene matters), 1465 (transportation of obscene matters for sale or distribution), and 1466 (engaging in the business of selling or transferring obscene matter).

Numerous prosecutions have been brought against persons distributing obscenity through computers. In *United States v. Thomas*, 74 F.3d 701 (6th Cir. 1996), a case involving a commercial computer "bulletin board," the Sixth Circuit specifically rejected the defendants' arguments that 18 U.S.C. § 1465 did not apply to intangible objects such as computer image files, and that Congress had not intended to regulate computer transmissions. Subsequent to this decision, Congress amended 18 U.S.C. §§ 1462 and 1465 specifically to prohibit the use of an "interactive computer service" to distribute obscenity.

Congress' frustration with Web sites with names calculated to mislead Internet users to pornographic Web sites (such as whitehouse.com) led to the passage of 18 U.S.C. § 2252B in the PROTECT Act. This provision, enacted on April 30, 2003, creates two related crimes for the misleading use of a domain name (a Web site's "address" that a user enters into a Web browser). The first criminalizes the knowing use of a misleading domain name to deceive any person into viewing obscene material. The second makes it illegal to use a misleading domain name to deceive a minor into viewing material that is harmful. (The Child Obscenity and Exploitation Section (CEOS) has issued guidance for United States Attorneys' Offices describing this law and its application, which is available on USABook).

Forfeiture for obscenity cases is covered under 18 U.S.C. § 1467. Criminal forfeiture is authorized under this section, but civil forfeiture is not. The following is subject to forfeiture under § 1467: (1) any obscene material produced, transported, mailed, shipped, or received; (2) any real or personal property constituting or traceable to gross profits or other proceeds; and (3) any real or personal property that facilitates the offense. Facilitating property is subject to forfeiture if the court, in its discretion, determines the property should be forfeited, taking into consideration the nature, scope, and proportionality of the use of the property in the offense. *Id.*

It is critical to consider using seizure warrants and orders to seize bank accounts and funds associated with the illegal enterprise. As in any "white collar" investigation, money that is potentially forfeitable should be seized at the time of indictment or arrest to avoid potential disposal of proceeds of the crime by the target of the investigation. In addition, if property was used to facilitate the crime, it should be seized for forfeiture pending conviction so that the target does not dispose of it. Furthermore, plea agreements should address forfeiture where possible, including forfeiture of the domain name itself and related ownership interests in and related to the Web site, as well as forfeiture of any and all property and equipment used to facilitate the offenses.

IV. Investigating web-based cases

A. Targets

Obscene Web sites are referred for prosecution from a variety of sources. These include, among others, citizen complaints registered with private groups such as ObscenityCrimes.org and the National Center for Missing and Exploited Children, or those sent directly to U.S. Attorneys' Offices. Leads are also developed by law enforcement and the Criminal Division's Child Exploitation and Obscenity Section, and particularly its High Tech Investigative Unit.

It is crucial, early in the investigation, for a law enforcement agent to visit the Web site in question and preserve its publicly-accessible content using a tool such as Teleport Pro or

Adobe Acrobat. Both programs can create a copy of the Web site's Hypertext Markup Language (HTML) and graphic files, in essence duplicating the Web site on a law enforcement computer's file system. This work should be performed on an undercover computer with proper backstopping (including the use of an untraceable Internet Protocol, or IP address), and should be carefully documented.

Identifying the webmaster is the first, and often, insurmountable hurdle. The Web site's public registration information is the first source to check, because it is free and does not risk notifying the webmaster of law enforcement interest. Typically, a Web site acquires a domain name or address, such as "usdoj.gov," through private companies, known as registrars, which have been delegated the authority to register unique names for a fee. The information provided by the webmaster to the registrar can be retrieved using an Internet "whois" query available on a variety of Web sites, including hexillion.com and samspade.org.

Many pornographic webmasters provide genuine information to the domain name registrars. More devious webmasters, however, can easily provide false information, because the only verification most registrars undertake is of the credit card used to pay for the service. The practice of providing false or fictitious registration information is likely to increase in frequency as more webmasters are prosecuted for obscenity. If the registrar's information on the webmaster is false or fictitious, additional investigation may be necessary to make an identification. Despite a bogus registration, a webmaster may be located by tracing the webmaster's payment method, typically a check, credit card, or wire transfer, to either the registrar or the Internet service provider (ISP) for the hosting services. Conversely, an identification may result from tracing the webmaster's method of receiving payment for goods or services. For example, checks or credit card accounts used to buy videotapes, DVDs, or subscription access to a Web site, can be examined for information leading to the recipient of the funds.

When the agent performs the "whois" query to identify the webmaster, he or she should also perform a "traceroute" query (using the publicly-available resources provided above) to identify the owner of the Web site's IP address. Most pornographic Web sites are operated using the facilities of an ISP and are housed at an ISP, in order to obtain communication speeds faster than those typically available at homes and small businesses.

As with Web sites, ISPs provide Internet connectivity in many different ways. The two primary Web site "hosting" models are server leasing and collocation. In server leasing, the ISP owns the server (a computer with specialized software for receiving and transmitting web pages) and leases it, or a portion of the space available on it, to the webmaster operating the Web site. The webmaster typically never even sees the server but administers the site from a remote location by logging into the machine over the Internet with a password supplied by the ISP. A collocated server is also remotely administered, but the machine is usually provided by the webmaster to the ISP which places the server in its facility and connects it to power and communication lines.

Although many ISPs provide web hosting services to Web sites regardless of subject matter, others specialize in hosting pornography. By visiting the ISP's own Web site, an investigator may develop a sense for whether the ISP is a large, diverse company, or a specialist. Large firms are likely to have significant experience in, and standard procedures for, responding to subpoenas and search warrants, and their size and diversity makes it unlikely that they would inform the webmaster if they are contacted by law enforcement. "Adult" hosting companies, on the other hand, should be approached with suspicion, and it should be assumed that even informal inquiries, as well as compulsory process, will result in the subject's becoming aware of the investigation.

Title 18 U.S.C. § 2703(f) provides a means by which ISPs can be instructed to preserve the contents of web servers for a period of ninety days, pending the issuance of a search warrant. As with other contacts, however, care should be taken in determining whether the ISP receiving this request is likely to notify the subject of the investigation.

The information provided in these steps is also significant in determining the appropriate venue for prosecuting the webmaster and for opposing a possible motion to transfer. (Venue issues are discussed in more detail below.) The location of the webmaster and the Web site's server are two important venues to be considered. Identifying the physical location of the server, however, may require contacting the ISP. Many ISPs operate server facilities in several cities or states, and the traceroute information will identify the company, but not the location, where the

server is operating. Notably, Web sites selling obscene materials are frequently located in foreign countries. If both the Web site and the webmaster are overseas, the case is unlikely to merit further investigation.

B. Evidence gathering

With the Web site's content captured, and the registration and ISP of the Web site identified, investigators can proceed to place undercover purchases through the Web site and preserve the evidence. A software program such as Camtasia can preserve the ordering process so that a jury can view the images seen by the agent as they listen to the agent's description of the ordering process.

The undercover purchases can then be used to gain insight into the subject's banking practices and finances. Cancelled checks or money orders will provide the subject's bank and account number, and undercover credit card statements can provide similar information on the ultimate recipient of the funds. Grand jury subpoenas directed at the subject's financial institutions will provide access to the subject's account records.

The full range of investigative techniques employed in other criminal cases is also useful in Web site obscenity investigations. These include mail covers, surveillance of businesses and residences, and interviews of witnesses such as former employees. Although Web site cases begin in cyberspace, they must, in the end, result in real-world investigations of individuals and the businesses they operate.

C. Searches

The final investigative step typically employed in a Web site obscenity case is to search the business, residence, and computers of the webmasters. As in any case, the investigative agent prepares an affidavit describing the investigation to date and the locations to be searched. When either a computer server, or personal computers at the enterprise's physical location (used for bookkeeping, e-mail, and remotely managing the Web site) are searched, the affidavit should describe the nature of the search and assert that pre-publication materials, if any are found, will be protected under the Privacy Protection Act, 42 U.S.C. § 2000aa. This Act forbids a government officer or employee, in connection with the investigation of a criminal offense, from searching for or seizing any work product or documentary materials reasonably believed to be intended for dissemination to the public, a newspaper, book, broadcast, or other form of public communication.

Despite the challenges of searching the Web site's servers, they are potentially quite useful in investigating and prosecuting online obscenity. First, the server is likely to provide additional evidence of both the content alleged to be obscene and the webmaster's use of the Internet to distribute it. In addition, File Transfer Protocol (FTP) logs maintained by the web server can provide useful information regarding the webmaster's remote administration of the Web site, and the webmaster's transmission of obscenity between the business location and the server. However, the evidentiary opportunities presented by the web server and the other computers cannot be exploited without obtaining the assistance of computer forensic technicians familiar with duplicating and investigating Web sites.

Prosecutions will often require the government to obtain search warrants in jurisdictions other than where the prosecution is venued. In these instances, the question will arise as to which community standard the reviewing magistrate should apply in evaluating probable cause. The magistrate may inquire whether he or she should apply the community standards of the jurisdiction where the business is located and where the search warrant will be executed or of the community where the case will be prosecuted.

This issue was addressed in *United States v. Levinson*, 991 F.2d 508 (9th Cir. 1993). The district court held that the community standards of the district in which the alleged obscene materials are located, which in this case was Los Angeles, generally govern a probable cause determination. However, where the government expresses an intent to prosecute in a different jurisdiction, the community standards of that district should control. Because the government intended to prosecute in Las Vegas, the district court found that probable cause did not exist because the government had not proven the community standards of that district. The Ninth Circuit reversed, holding that the district court could have applied the community standards of Los Angeles because the government could have prosecuted the case there. *See also Multi-media Distributing Co. v. United States,* 836 F. Supp 606 (N.D. Ind. 1993) (district court where alleged obscene materials were located could make probable cause determination based on that community's standards).

V. Grand jury practice

Most Web site indictments are presented using a single agent who describes the results of the investigation. Although the grand jury may

issue a valid indictment based solely on an agent's description of the material alleged to be obscene, *see, e.g., United States v. Manarite*, 448 F.2d 583 (2d Cir. 1971), the grand jury must be provided the opportunity to view the material if it wishes and to do so in its entirety to meet the test for obscenity in *Miller v. California*, 413 U.S. 15 (1973).

By presenting at least a portion of the material, the prosecuting attorney will have the opportunity to observe the grand jurors' reactions, and thereby gain some insight into the community standards that the petit jury will likely employ in evaluating the material. In practice, booklets of photographs or short clips of videos may be prepared which can be shown to the grand jury in the context of the agent's description of the purchases. In cases in which the Web site content itself is alleged to be obscene, the captured version of the Web site can be provided on a computer to demonstrate the contents to the grand jury.

VI. Pretrial motions

When defendants are charged in the jurisdiction to which materials were sent or downloaded, they may file motions to change venue to where they reside or where their business is located. These arguments have been tried and rejected in several cases. In *United States v. Espinoza,* 641 F.2d 153 (4th Cir. 1981), a case involving the shipment of child pornography under 18 U.S.C. § 1465, the Fourth Circuit rejected the defendant's claim that he had a constitutional right to be tried in the jurisdiction of his residence. Similarly, in *United States v. Slepicoff*, 524 F.2d 1244 (5th Cir. 1975), in a prosecution for mailing obscene materials under 18 U.S.C. § 1461, it was held that the multivenue provisions contained in 18 U.S.C. § 3237 allow for enforcement in selected districts. In view of the contemporary community standards requirement of the *Miller* test, the *Slepicoff* court found that it was logical to try a defendant in a jurisdiction to which obscene materials had been mailed. *Id.* Furthermore, a defendant's choice to do business throughout the nation limited his right to be tried in the locality where he lives and bases his operations. *Id.*

The principles of broad venue under 18 U.S.C. § 3237 have even been held to apply in obscenity conspiracy prosecutions. *United States v. Cohen*, 583 F.2d 1030 (8th Cir. 1978). In the *Cohen* decision, the Eighth Circuit rejected the defendants' claims that the government should have been required to introduce evidence of the community standards of the Central District of California, where the defendants formed the conspiracy and performed the overt acts in furtherance of that conspiracy, instead of the Northern District of Iowa where the materials were distributed. The Eighth Circuit stated that the same principles of venue under 18 U.S.C. § 3237 apply to a charge of conspiracy, and "it is well settled that the offense of conspiracy may be tried not only in the district where the agreement was made, but also in the district where an overt act was committed." *Id.* at 1041-42.

Defendants may also file motions to dismiss the indictment, arguing that the government allegedly manufactured jurisdiction or venue. The defense will argue that the government lured the defendant into a pro-government district and that the defendant was merely an operator of a Web site located in a distant jurisdiction. The government can counter that the defendant created the interstate nexus by sending the material in interstate commerce, or used a facility of interstate commerce or interactive computer service for the purpose of distribution, and thus accepted the possibility of prosecution in the district to which the material was sent. Several analogous cases support the view that in Web site cases, the government may charge a defendant in the district from which the materials originated or where the materials were received. *See, e.g., United States v. Bagnell*, 679 F.2d 826 (11th Cir. 1982) (interstate shipment of obscenity); *Reed Enterprises v. Clark*, 278 F. Supp. 372 (D.D.C. 1967) (mailing of obscenity); *see also United States v. Thomas*, 74 F.3d 701 (6th Cir. 1996) (Internet bulletin board with restricted membership).

VII. Trial issues

A. Community standards and the internet

Many of the prosecutions for violations of obscenity statutes will involve crimes committed via the Internet. While the *Miller* test established a three-part test for obscenity which incorporates "the average person applying contemporary adult community standards," this test was devised before the advent of the Internet. *Miller v. California*, 413 U.S. 15, 24 (1973). Therefore, the question as to what the community standard is on the Internet has not yet been answered. Is the standard that of the community in the jurisdiction where the case is brought? Should the community standard be that of the district where the material is produced, distributed, or sold? Or should there be a national community standard because the Internet is available in each and every jurisdiction in the country?

Although the Supreme Court has yet to weigh in on the forum shopping issue in the context of Internet obscenity, its recent analysis regarding the constitutionality of applying local community standards to material distributed on the Internet suggests at least some agreement with the notion that the community standards of the district of receipt should be applied. In *Ashcroft v. American Civil Liberties Union*, 535 U.S. 564 (2002), a plurality held that the Child Online Protection Act's (COPA's) reliance on community standards to determine what was "harmful to minors" over the Internet did not, by itself, render COPA unconstitutionally overbroad. The plurality stated:

> If a publisher chooses to send its material into a particular community, this Court's jurisprudence teaches that it is the publisher's responsibility to abide by that community's standards. The publisher's burden does not change simply because it decides to distribute its material to every community in the Nation.

Id. at 583. In reaching this conclusion, the plurality relied on *Hamling v. United States*, 418 U.S. 87 (1974), in which the Court upheld the application of varying community standards to obscenity in an obscenity mail distribution case, and *Sable Communications v. FCC*, 492 U.S. 115 (1989), in which it held that the application of local community standards to "dial-a-porn" telephone communications was constitutional. *Ashcroft*, 535 U.S. at 580-81. *Ashcroft*'s language also implies that the Court would view venue in any district a necessary consequence of choosing to distribute obscenity over a far-reaching medium like the Internet.

All of this is not to suggest that the broad distribution aspect of the Internet has not caused apprehension among some courts, with regard to both venue and the appropriate community standards to be applied. Recent rumblings in the Supreme Court and elsewhere suggest that the breadth of the Internet's reach is elevating concerns about broad venue and the concomitant applicability of varying community standards. Despite the plurality's holding in *Ashcroft*, the concurring opinions suggest that *Hamling* and *Sable* might not be applicable to the Internet because it is a broader medium with necessarily unlimited distribution, unlike the mail or the telephone. *Id.* at 587 (O'Connor, J. concurring) ("adoption of a national standard is necessary in my view for any reasonable regulation of Internet obscenity"); *Id.* at 594-97 (Kennedy, J. concurring, joined by Souter and Ginsburg, JJ.) (recognizing the burden on Internet speech based on the varying national community standards); *Id.* at 590-91 (Breyer, J., concurring) (stating that legislative history of Child Online Protection Act made clear that Congress intended a national standard). This point has not been lost on at least one lower court considering the overbreadth of other Internet-related statutes. *See Nitke v. Ashcroft*, 253 F. Supp. 2d 587, 603-05 (S.D.N.Y. 2003) (in discussing appropriate community standard for Internet, court distinguished *Hamling* and *Sable*, stating that "because the Internet content providers cannot control the geographic distribution of their materials, Internet obscenity statutes restrict protected speech"). *Id.* at 604.

This emerging view that distributors on the Internet are helpless to control the vast extent of distribution could precipitate an unfavorable judicial attitude toward the government's selection of venue in judicially conservative districts. While a national community standard has not yet been created, it appears from the opinions discussed above that it is at least being considered by some members of the judiciary. Following this type of reasoning, a lower court could try to impose a national standard, which could greatly impact any obscenity prosecution. For example, that national standard could be that of a restrictive community, a permissive community, or something in between. This concern will be mitigated where the distributor exercises increased control over distribution, such as by mailing into a district. In any event, the appropriate community standard is an issue that requires thought and preparation in advance of trial.

B. Scienter

When prosecuting obscenity cases, many defendants will claim lack of knowledge that the material they were distributing was obscene. However, a defendant does not need to know that the material is obscene to sustain a guilty verdict. For example, under 18 U.S.C. § 1461, the knowledge requirement has been deemed satisfied if the defendant "knew the character and nature of the materials," so that the government does not have to prove that the defendant knew that the materials were legally obscene. *Hamling v. United States*, 418 U.S. 87, 123 (1974). Rather, proving scienter only requires a showing of "general knowledge that the material is sexually oriented." *United States v. Linestsky,* 533 F.2d 192, 204 (5th Cir. 1976). One court has held that books, magazines, and other films seized from the defendant can be used to prove the defendant's knowledge of the nature of the films that are the subject of the prosecution. *United States v. Hurt,* 795 F.2d 765 (9th Cir. 1986).

In addition, in a prosecution for conspiracy to violate 18 U.S.C. §§ 1461 and 1462, it was held that scienter was established where, among other things, the record contained evidence that the defendants attempted to conceal their personal involvement in the scheme by evasive tactics, including the use of fictitious corporate names, changes of address filed by persons using aliases, and the use of various locations as mail drops for return mail consisting of orders and payments from customers. *United States v. Cohen,* 583 F.2d 1030 (8th Cir. 1978). In another conspiracy case, the court held that knowledge that materials were sexually explicit was the only scienter requirement under 18 U.S.C. § 1462, and therefore, the defendants could be convicted of conspiring to violate the statute even if they did not know that the videos in question would be distributed to a community in which they would be deemed obscene. *United States v. Investment Enterprises, Inc.,* 10 F.3d 263 (5th Cir. 1994).

VIII. Sentencing

Offenses committed under 18 U.S.C. §§ 1461, 1462, and 1465 fall under the purview of United States Sentencing Guideline (USSG) § 2G3.1, Mailing or Transporting Obscene Matter. The base offense level is 10 for this violation and includes enhancements based on the content of the material (sadistic and masochistic conduct), whether or not a computer was involved in the commission of the crime, and whether the distribution was for pecuniary gain. If the distribution was for pecuniary gain, then the loss table located in USSG § 2B1.1 is utilized, corresponding to the retail value of the material. The enhancement increases the offense level by a minimum of 5, and may increase it more, based on the total loss value.

There will also be cases where the general conspiracy statute is charged pursuant to 18 U.S.C. § 371, most often in the context of a conspiracy to use the mails for the mailing of obscene matters and to use an interactive computer service for the purpose of the sale and distribution of obscene matters, in violation of 18 U.S.C. §§ 1461 and 1465. This crime carries a maximum sentence of five years and no specific guideline covers this offense. Therefore, prosecutors are directed to USSG § 2X1.1, Attempt, Solicitation, or Conspiracy Not Covered by a Specific Offense Guideline. This section states that the base level to be used is the base offense level from the guideline for the substantive offense, plus any adjustments from such guideline for any intended offense conduct that can be established with reasonable certainty. Therefore, USSG §2G3.1 (Mailing or Transporting Obscene Matter) is utilized for violations of this statute.

Based on USSG § 3D1.1(a), Procedure for Determining Offense Level on Multiple Counts, when a defendant has been convicted of more than one count, the court shall group the counts resulting in conviction into distinct Groups of Closely Related Counts by applying the rules specified in USSG § 3D1.2. Based on USSG § 3D1.2(a), offenses are grouped when counts involve the same victim and the same act or transaction. In addition, USSG § 3D1.2(b) provides that offenses are grouped when counts involve the same victim and two or more acts or transactions connected by a common criminal objective or constituting part of a common plan or scheme. Finally, although not specifically enumerated, USSG § 3D1.2(d) also provides for the possibility of grouping. Therefore, based on the foregoing sections, it is likely that these offenses will group based on the fact that the same victim, *i.e.*, society, is harmed by commission of these offenses which are based on a common scheme or plan. The offenses are of the same type, and therefore, all counts likely will group together, forming one group. Pursuant to USSG § 3D1.4, there would be no increase in the offense level.

IX. Conclusion

Although web-based obscenity prosecutions present unique challenges, they are a vital component of an overall federal strategy to address an increasingly degradative pornography industry. In addition, effective enforcement of obscenity law on the Internet is critical to reclaiming this important medium as an arena which, while permitting the expression of First Amendment-protected speech, is reasonably safe for children and adults to explore.❖

ABOUT THE AUTHORS

❑**Benjamin Vernia** is a Trial Attorney in the Child Exploitation and Obscenity Section. Prior to joining CEOS in 2002, he was a Trial Attorney in the Fraud Section of the Civil Division for eight years.

❑**David Szuchman** joined the Child Exploitation & Obscenity Section as a Trial Attorney in 2002. Mr. Szuchman was previously employed as a Legislative Attorney for the New York City Council and also served for four years as an Assistant District Attorney for the Manhattan District Attorney's Office in New York.✠

The Aftermath of Free Speech: A New Definition for Child Pornography

Brian Slocum
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

Wendy Waldron
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

I. Introduction

In 2002, a United States Supreme Court decision struck a serious blow to federal child pornography prosecutions. In *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002), the Supreme Court found two of the four then-existing definitions of child pornography to be unconstitutional. The first of these was 18 U.S.C. § 2256(8)(B), which defined "child pornography" to include visual depictions that "appear[] to be" of minors engaging in sexually explicit conduct. This definition, often referred to as the "virtual child pornography" definition, included computer-generated images or images of adults who appeared to be minors. The Court found this provision to be unconstitutionally overbroad. In particular, the Court concluded that the definition extended beyond the traditional reach of obscenity as described in *Miller v. California*, 413 U.S. 15 (1973), that the Court's decision in *New York v. Ferber*, 458 U.S. 747 (1982) could not be extended to support a complete ban on virtual child pornography, and that the government's arguments in favor of the prohibition were insufficient under the First Amendment. *Ashcroft,* at 246-52, 256. The aftermath of this portion of the Court's decision is the focus of this article.

By invalidating these important features of the Child Pornography Prevention Act of 1996, *codified at* 18 U.S.C. §§ 2251-2260, the Court's decision left the government in an unsatisfactory position that warranted a prompt legislative response. As a result of the *Free Speech* decision, defendants frequently contend that there is "reasonable doubt" as to whether charged images, particularly digital images on a computer, were produced with an actual child, or as a result of some other process. Occasionally, there are experts who are willing to testify to the same effect on the defendants' behalf. Without a provision that covers highly-realistic computer-generated images, it is difficult to meet the burden of proof when images are of real, but unidentified, children. This problem has the potential to grow increasingly worse as trials devolve into confusing battles between experts arguing over the method of generating images that look like, and probably are, real children. Even in cases involving identified victims of child pornography, it is very difficult for prosecutors to arrange for one of the few law enforcement witnesses who have met the child to be available for any given child pornography trial.

II. The need for a "*Free Speech* fix"

Congress sought to remedy these concerns with the enactment of the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today Act of 2003 (PROTECT Act), Pub. L. No. 108-066, 117 Stat. 650, on April 30, 2003. The PROTECT Act greatly enhances federal child pornography law by, among other things, replacing with a new provision the prior definition of "child pornography" in 18 U.S.C. § 2256(8)(B) that was struck by the *Free Speech* court. Title V, Subsection A of the PROTECT Act directly responded to the *Free Speech* decision by creating a new provision in § 2256(8)(B) that defines child pornography to include computer-based depictions that are indistinguishable from those involving real children. The PROTECT Act also expands the affirmative defense applicable to cases brought under § 2256(8)(B) in response to the Supreme Court's criticism of the prior law.

The PROTECT Act child pornography provisions more narrowly focus federal child pornography law on the government's core interest: preserving its ability to enforce laws proscribing child pornography produced using real children. To further this interest, the PROTECT Act makes fundamental changes with respect to the "virtual" child pornography ban in § 2256(8)(B), and the corresponding affirmative defense in 18 U.S.C. § 2252A(c). Thus, the PROTECT Act includes in the definition of child pornography images that, to an ordinary observer, could pass for the real thing. At the same time, the PROTECT Act provision gives a defendant the ability to escape conviction under the child pornography statutes if he can establish that the image was not produced using a real child.

The changes brought about by the PROTECT Act are intended to address the Supreme Court's concerns that legitimate expression might improperly fall within the scope of the child pornography laws. The provision is therefore narrowly tailored in four ways to advance the government's compelling interest, without casting a broad net over protected speech. First, the proscription of virtual images is limited to digital, computer or computer-generated images. Second, the images must genuinely look like they depict real children. Third, the sexual content must be particularly explicit. Fourth, the defendant can escape conviction through an affirmative defense by establishing that the images were produced without the use of a real child. As set forth in more detail below, the new provision provides an important response to the Supreme Court's concerns in *Ashcroft v. Free Speech Coalition*.

III. The details of the new child pornography provisions

The centerpiece of the PROTECT Act's response to the *Free Speech* decision was to amend § 2256(8)(B) to read as follows:

> such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct;

18 U.S.C. § 2256(8)(B) (2003).

Among other changes, the new definition substitutes the phrase "indistinguishable from [] that" of a minor for the "appears to be" phrase struck down by the Court in *Free Speech*. A new provision, § 2256(11), explains the meaning of "indistinguishable" as follows:

> the term "indistinguishable," used with respect to a depiction, means virtually indistinguishable, in that the depiction is such that an ordinary person viewing the depiction would conclude that the depiction is of an actual minor engaged in sexually explicit conduct. This definition does not apply to drawings, cartoons, sculptures or paintings depicting minors or adults.

18 U.S.C. § 2256(11) (2003).

The definition thus clarifies that only the most convincing depictions of child pornography, which are indistinguishable from those depicting real children, are proscribed.

Further narrowing the scope of the virtual child pornography definition, § 2256(8)(B) is now explicitly limited to "digital image[s]," "computer image[s]," and "computer-generated image[s]." This limitation implicitly acknowledges the power of computer imaging technology both to alter actual child pornography and to generate simulated child pornography. Because the use of computers and digital technology to traffic images of child pornography implicates the core of the government's practical concern about enforceability, "drawings, cartoons, sculptures, or paintings," which cannot pass for the real thing, are specifically excluded from the scope of § 2256(8)(B).

Along with narrowing the definition of child pornography, the PROTECT Act limits the scope of sexual conduct depicted that is actionable for virtual child pornography under § 2256(8)(B). (Note that this new definition does *not* affect prosecutions under either § 2256(8)(A) or (C)). Thus, a new provision, § 2256(2)(B), contains a definition of sexually explicit conduct specific to § 2256(8)(B):

> (B) For purposes of subsection 8(B) of this section, 'sexually explicit conduct' means–
>
> (i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse, where the genitals, breast, or pubic area of any person is exhibited;
>
> (ii) graphic or lascivious simulated;
>
> (I) bestiality;
>
> (II) masturbation; or
>
> (III) sadistic or masochistic abuse; or
>
> (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person;

18 U.S.C. § 2256(2)(B) (2003).

This provision, in turn, relies upon a new definition in 18 U.S.C. § 2256(10), which defines "graphic":

> 'graphic', when used with respect to a depiction of sexually explicit conduct, means that a viewer can observe any part of the genital area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted[.]

Notably, the new provision requires a simulated image to be lascivious to constitute child pornography under § 2256(8)(B). Thus, child pornography that simulates sexually explicit conduct (as opposed to depicting actual sexually explicit conduct) must be lascivious, as well as meet the other requirement of the definition. The

combined effect of these changes is to narrow the definition of sexually explicit conduct in cases involving virtual child pornography under § 2256(8)(B). In such cases, sexually explicit conduct must be graphic or, if simulated, also lascivious.

The PROTECT Act also significantly amends the affirmative defense in 18 U.S.C. § 2252A(c). Previously, the affirmative defense was available in cases involving transportation, distribution, receipt, and reproduction of child pornography if the defendant could prove that the alleged child pornography was produced using an actual adult, and was not pandered in such a manner as to convey the impression that it was child pornography. In *Free Speech*, the Court criticized the affirmative defense on the grounds that it incompletely protected defendants' First Amendment rights. Specifically, the Court observed that the affirmative defense was not available to a defendant who could prove that real children were not involved in the production of the images, but who had pandered the material as child pornography. 535 U.S. at 256. The Court was also concerned that the defense did not extend to possession offenses. *Id.*

The new affirmative defense eliminates both of the problems identified by the Court. First, the affirmative defense now includes possession offenses. Second, while prior law only granted an affirmative defense for productions involving youthful-looking adults, and only allowed the defense if the defendant did not pander the material as child pornography, a defendant can now prevail simply by showing that no children were used in the production of the materials. In other words, a defendant can now prevail by establishing that the images do not depict actual children. The defendant must, however, provide notice to the government of an intention to assert the affirmative defense no later than ten days before trial.

IV. Application of the new provisions and alternative charges

Since the enactment of the PROTECT Act, prosecutors have several options to consider in child pornography cases. The Department of Justice (Department) expects that the "virtual porn" provision of the PROTECT Act will face constitutional challenges. Because it is possible that those challenges will ultimately be heard by the Supreme Court, Assistant United States Attorneys (AUSAs) considering charges under the new child pornography definition in § 2256(8)(B) should be mindful that their cases are just as likely as any other to serve as the vehicle for a challenge. Prudence dictates that, until the challenges are finally resolved by the Supreme Court, prosecutors should carefully evaluate and scrutinize their use of the new provisions, and include "safe harbor" or back-up charges in their indictments to the extent such charges are available.

Several aspects of the images should be considered before a charging decision is made. The images should be of good quality, appear to show real children, and depict sexually explicit conduct, if possible. In addition, given the Supreme Court's emphasis on the potential literary and artistic merit of materials exploring teenage sexuality, images of prepubescent children should be given preference over those of older children.

In all cases, prosecutors and law enforcement should continue their efforts to identify children depicted in the images. The identification of known victims is essential in determining which victims of child pornography have not yet been identified and protected from further harm. Prosecutions under § 2256(8)(B) will also be in a stronger position against any constitutional challenge if some of the charged images depict known victims. In cases brought under the old child pornography statutes, the identification of known victims is useful even if it is not feasible to introduce evidence regarding the child's identity at trial. The identification of known victims can often lead to plea agreements or to stipulations that charged images depict actual minors engaged in sexually explicit conduct.

Prosecutors considering charging under the pre-existing child pornography provisions, rather than the new § 2256(8)(B), should keep in mind that the identification of known victims is by no means the only way to meet the government's burden of proving that charged images depict real children engaging in sexually explicit conduct. Indeed, there is support for the position that simply entering the images into evidence can meet the government's burden.

The three circuits that have addressed the issue in light of the *Free Speech* decision have concluded that the jury can make its decision by simply viewing the images themselves. *See United States v. Kimler*, 335 F.3d 1132, 1142 (10th Cir. 2003) (holding that juries are capable of distinguishing between "real and virtual images" and that neither expert testimony nor evidence of victim identity is required by the *Free Speech* decision); *United States v. Deaton*, 328 F.3d 454, 455 (8th Cir. 2003) (per curiam) (holding that images alone were sufficient to prove that production of charged images involved use of a

real minor); *United States v. Hall*, 312 F.3d 1250, 1260 (11th Cir. 2002) (holding that despite unconstitutional jury instruction, examination of charged images showed that no reasonable jury could have found that images depicted virtual children as opposed to actual children). Prosecutors in child pornography cases may also want to support their proof that images depict real children by presenting the testimony of a physician that characteristics such as the proportions, body fat distribution, and skin tone of the children depicted are consistent with those of real children. *See United States v. Bender*, 290 F.3d 1279 (11th Cir. 2002).

In cases that proceed under the new 18 U.S.C. § 2256(8)(B), charging some images under one of the obscenity provisions, 18 U.S.C. §§ 1460-70, is also an effective way to ensure that convictions will stand in the event that § 2256(8)(B) is struck down as unconstitutional. The new obscenity statute enacted as part of the PROTECT Act, § 1466A, is one of the possible backup charges. This statute is directed to the obscene visual representation of the sexual abuse of children. *See* 18 U.S.C. § 1466A (2003). When possession, as opposed to receipt or distribution, of the images is all that can be shown, the new § 1466A(b) is the only available federal obscenity provision because it is the only one that includes possession within its prohibitions. When receipt or distribution can be shown, however, obscenity provisions other than § 1466A can be used. In addition, while § 1466A(a)(1) is likely to be a safe charge, § 1466A(a)(2) should be used with caution as a backup charge due to the likelihood that it will be challenged.

Finally, care should be taken to develop a strong record when accepting pleas to child pornography charges. First, to the extent the record supports it and the defendant agrees, the plea colloquy should unequivocally reflect that the defendant is pleading to child pornography involving real minors. If the government has evidence suggesting that one or more of the charged images depicts an identified minor, the fact that such evidence exists should be part of the colloquy.

V. Conclusion

The situation before the enactment of the PROTECT Act was unacceptable, as many meritorious cases involving child pornography were not being brought, or were creating an unnecessarily heavy drain on law enforcement and prosecutorial resources. The Supreme Court's decision in *Free Speech* made enforcement of the child pornography laws substantially more difficult and threatened to reinvigorate this pernicious traffic and harm more children. While the Department was disappointed with the Court's decision, any legislation must necessarily respect it and endeavor, in good faith, to resolve the constitutional deficiencies in the prior law that were identified by the Court. The Department believes that the PROTECT Act has succeeded in doing so.❖

ABOUT THE AUTHORS

❑**Brian Slocum** is a Trial Attorney in the Child Exploitation and Obscenity Section (CEOS). Prior to joining CEOS in 2002, Mr. Slocum was hired through the Honors Program as an attorney in the Civil Division in 2000.

❑**Wendy Waldron** joined the Child Exploitation and Obscenity Section through the Honors Program as a Trial Attorney in 2001. Ms. Waldron spent six months on detail in the United States Attorney's Office for the District of Columbia, specializing in child sexual and physical abuse cases.✠

Sex Trafficking of Minors: International Crisis, Federal Response

Sara L. Gottovi
Trial Attorney
Child Exploitation Obscenity Section
Criminal Division

For most Americans, the word "slavery" invokes thoughts of shameful practices abolished long ago. Unfortunately, however, modern day slavery not only exists, but is a thriving industry in countries throughout the world. U.S. Department of State, *Trafficking in Persons Report, 2003, available at* http://www.state.gov/g/tip/rls/tiprpt/2003 [hereinafter TIP Report]. The business of human trafficking is a problem of global proportions, with potentially devastating consequences not only for the individual victims, but for entire nations as well. *Id.* at 10-11. This article examines the United States' approach to the crime of human trafficking, with a focus on sex trafficking of children.

I. Introduction

Although there is no worldwide consensus on the appropriate definition for "trafficking in persons," Francis T. Miko & Grace Park, *Trafficking in Women and Children: The U.S. and International Response*, at 2 (Updated July 10, 2003), *at* http://www.usembassy.it/pdf/other/RL30545.pdf, United States legislation defines "severe forms of trafficking in persons" as:

> sex trafficking in which a commercial sex act is induced by force, fraud, or coercion, or in which the person induced to perform such an act has not attained 18 years of age; or
>
> the recruitment, harboring, transportation, provision, or obtaining of a person for labor or services, through the use of force, fraud or coercion for the purpose of subjection to involuntary servitude, peonage, debt bondage, or slavery.

TIP Report, *supra* at 12.

Using that definition, the United States Department of State estimates that approximately 800,000-900,000 people are trafficked annually. *Id.* at 7. Approximately 18,000-20,000 of those victims are trafficked into the United States. *Id.*

The human trafficking business is a lucrative one, generating approximately $7-10 billion annually for traffickers. *Id.* at 9. Trafficking is a particularly alluring crime because many nations punish trafficking victims more harshly than the traffickers, thus allowing a high level of income to be generated with a low level of risk. Kara C. Ryf, Note, *The First Modern Anti-Slavery Law: The Trafficking Victims Protection Act of 2000,* 34 CASE W. RES. J. INT'L L. 45, 48 (2002). Because "there is less overhead cost than in the drug and arms smuggling industries, and humans are a reusable commodity that can be sold and resold. . . . large and well-established organized crime rings" including the Russian Mafia, have become involved in the market of human trafficking. *Id.* at 50.

Although United States citizens are not immune from the crime of trafficking, residents of nations plagued by poverty, war, or other political unrest, are particularly vulnerable. These conditions fuel the residents' desire to migrate. Tal Reviv, *International Trafficking in Persons: A Focus on Women and Children—The Current Situation and the Recent International Legal Response*, 9 CARDOZO WOMEN'S L.J. 659, 661 (2003). In some cases, victims are sold by their families. Kara C. Ryf, Note, *supra* at 49. In others, tantalizing promises of lucrative employment or marriage into an affluent family may be used to lure victims. TIP Report, *supra*, at 7. It is also a common scenario for traffickers to use threats, force, violence, or even kidnapping, to procure victims. *Id.* at 6-7.

International traffickers generally transport victims to foreign and unfamiliar countries to increase their vulnerability and susceptibility to manipulation. *Id.* at 6. After reaching their intended destination, traffickers may strip the victim of all identification and other documents needed for travel. *Id.* Traffickers may also charge grossly inflated fees for their "immigration services," which can result in a lifetime of debt bondage. Miko *supra,* at 4.

Victims of trafficking are then used to provide cheap labor for a variety of industries. Some of the most common sites of "employment" include, but are not limited to: houses of prostitution or other forms of sexual exploitation, farms, residences (victims forced into domestic

servitude), sweatshops, the military (victims utilized as child soldiers or in other military positions), and the streets (victims forced to beg or steal). TIP Report, *supra*, at 9, 26, 38, 45, 59, 97. In the United States, approximately one-half of all trafficking victims are forced into prostitution and the sex industry. Miko, *supra*, at 7.

All genders, races, and ages are subject to human trafficking. The majority of trafficking victims, however, are women "under the age of 25, many in [their] mid to late teens." *Id*. at 4 (noting that "[t]he fear of infection with HIV and AIDS among customers has driven traffickers to recruit younger women and girls, some as young as seven, erroneously perceived by customers to be too young to have been infected."). *Id.* Internationally, the majority of trafficking victims are believed to come from South and Southeast Asia, while the former Soviet Union "may be the largest new source of trafficking for prostitution and the sex industry." *Id.* at 2. After being trafficked, "most of the victims are sent to Asia, the Middle East, Western Europe, and North America. They usually end up in large cities, vacation and tourist areas, or near military bases, where demand is highest." *Id*. Victims who come to the United States "most often end up in the larger cities of New York, Florida, North Carolina, California, and Hawaii . . . [although] the problem is also migrating to smaller cities and suburbs." *Id*. at 7.

In addition to addressing the influx of international victims of sex trafficking, the United States has its own homegrown problem of interstate sex trafficking of minors. Although comprehensive research to document the number of children engaged in prostitution in the United States is lacking, it is estimated that about 293,000 American youth are currently at risk of becoming victims of commercial sexual exploitation. Richard J. Estes & Neil Alan Weiner, *Commercial Sexual Exploitation of Children in the U.S, Canada and Mexico*, UNIVERSITY OF PENNSYLVANIA, EXECUTIVE SUMMARY at 11-12 (2001) (available at http://caster.ssw.upenn.edu/~restes/CSEC.htm) [hereinafter Estes Report]; *see also* Mia Spangenberg, *Prostituted Youth in New York City: An Overview* (available at http://www.ecpatusa.org/child_prosti_us.asp). The majority of American victims of commercial sexual exploitation tend to be runaway or thrown away youth who live on the streets. Estes Report, at 11-12. These children come from homes where they have been abused, or from families that have abandoned them, and often become involved in prostitution as a way to support themselves financially or to get the things they want or need. *Id*. at 3.

Other young people are recruited into prostitution through forced abduction, pressure from parents, or through deceptive agreements between parents and traffickers. Miko, *supra*, at 7. Once these children become involved in prostitution, they are often forced to travel far from their homes and, as a result, are isolated from their friends and family. *Id*. Few children in this situation are able to develop new relationships with peers or adults other than the person who is victimizing them. *Id.* The lifestyle of such children revolves around violence, forced drug use, and constant threats. *Id*.

Among children and teens living on the streets in the United States, involvement in commercial sex activity is a problem of epidemic proportions. Approximately 55% of street girls engage in formal prostitution. Estes Report at 7. Of the girls engaged in formal prostitution, about 75% worked for a pimp. *Id.* Pimp-controlled commercial sexual exploitation of children is linked to escort and massage services, private dancing, drinking and photographic clubs, major sporting and recreational events, major cultural events, conventions, and tourist destinations. *Id.* About one-fifth of these children become entangled in nationally organized crime networks and are trafficked nationally. *Id.* at 8. They are transported around the United States by a variety of means, including cars, buses, vans, trucks or planes, *Id*., and are often provided counterfeit identification to use in the event of arrest. *Id*. The average age at which girls first become victims of prostitution is twelve to fourteen. *Id.* at 92. It is not only the girls on the streets that are affected; for boys and transgender youth, the average age of entry into prostitution is eleven to thirteen. *Id.*

II. Recent U.S initiatives to curb sex trafficking of minors

The United States has declared its firm commitment to combat the scourge of trafficking in persons and to protect the "victims who fall prey to traffickers." TIP Report, *supra*, at 169. Numerous policy directives and statutory enactments, both international and domestic in scope, have resulted from this commitment to eradicate human trafficking. Miko & Park, *supra* at 8-19. These initiatives are designed to target various aspects of the trafficking epidemic and rely on a cooperative approach by, among others, the Departments of Justice, Labor, State, Homeland Security, and the Federal Bureau of Investigation. *Id.* at 8-10.

"The U.S. government-wide anti-trafficking strategy is one of (1) prevention, (2) protection and support for victims, and (3) prosecution of traffickers." *Id.* at 8. Numerous initiatives have emerged from this strategy. A Workers' Exploitation Task Force was created to investigate and prosecute human trafficking and exploitation cases. *Id.* at 9. Internationally, "[t]he Department of State funded the creation of a database on U.S. and international legislation on trafficking." *Id.* An Interagency Council on Women was created to increase awareness of the problem and to develop strategies for solutions. The United States urged other countries to take strong action to address the problem of human trafficking, including passage of necessary legislation and cooperation with non-governmental organizations (NGOs) dedicated to eradicating trafficking. *Id.*

As a result of this initiative, the U.S. Congress passed the Victims of Trafficking and Violence Protection Act in 2000. Pub. L. 106-386, 114 Stat. 1466 (Oct. 28, 2002) [hereinafter TVPA]. Among its key provisions, the TVPA directs the Department of State to submit an annual report identifying countries that do and do not comply with minimum standards for the elimination of trafficking. The report must also provide, on a country-by-country basis, a description of the nature and extent of severe forms of trafficking in persons in each country, and an assessment of the efforts by governments to combat trafficking. *See* 22 U.S.C. § 2151n(f). Another important aspect of the TVPA was the authorization to grant up to 5,000 non-immigrant visas per year to victims of severe forms of trafficking who are in the United States, who have been in the United States for at least three years, who agree to assist in a trafficking investigation and/or prosecution, and who would face a significant possibility of retribution or other harm if they were removed from the United States. *See* 8 U.S.C. §§ 1101, 1184; 22 U.S.C. § 7105. The TVPA also amended the federal criminal sex trafficking provisions, discussed in detail below in Section III, to enhance prosecutors' abilities to bring sex traffickers to justice. *See* 18 U.S.C. § 1591.

The strong anti-trafficking initiative begun in the last administration has carried through with equal force to the current administration. Miko, *supra*, at 10. In March 2001, the Department of Justice (Department) announced that the effort to combat trafficking would be a top priority for the administration and that U.S. law enforcement agencies would cooperate closely to upgrade their efforts to combat trafficking. *Id.* at 9. On January 24, 2002, the Attorney General announced the implementation of the special "T" visa program, mandated in the TVPA, for international victims of trafficking in the United States who cooperate with law enforcement officials. In addition to providing the non-immigrant "T" visa for those individuals recently victimized by traffickers, the Attorney General made clear that individuals in "T" status would have an opportunity to seek permanent residency after three years in "T" status, and that their spouses and children living in the United States could apply for non-immigrant visa status.

In early 2003, the FBI announced Operation Innocence Lost, a nationwide initiative focusing on child victims of interstate sex trafficking in the United States. The FBI initiative first identified several urban areas that are known to be hubs for interstate sex trafficking of minors. Federal and state prosecutors and investigators, along with FBI special agents from these geographic areas, have been targeted for special training at the National Center for Missing and Exploited Children on issues related to identifying, investigating, and prosecuting cases involving child victims of prostitution. Starting in 2004, this training program will be expanded to include individuals from areas not initially targeted in Operation Innocence Lost. In addition, as part of Operation Innocence Lost, the FBI has committed additional investigative resources to work cases of child prostitution in the targeted field offices. Overall, Operation Innocence Lost is committed to a task force approach, joining local, state, and federal resources to solve these horrific crimes against children.

III. Federal statutory tools for prosecutors combating sex trafficking of minors

The federal prosecutor's tool kit in cases of sex trafficking of minors contains four primary statutes: 18 U.S.C. § 1591 and 18 U.S.C. §§ 2421-2423. Most are familiar only with 18 U.S.C. §§ 2421–2423, which have their origins in the Mann Act of 1910. Prosecutors are less familiar with 18 U.S.C. § 1591, which was amended by the TVPA in 2000, and only since that time has become a truly effective tool to address cases of child sex trafficking.

Title 18, United States Code, Section 1591, as amended in 2000 by the TVPA, provides:

> (a) Whoever knowingly –
>
> (1) in or affecting interstate commerce, recruits, entices, harbors, transports, provides, or obtains by any means a person; or
>
> (2) benefits financially or by receiving anything of value, from participation in a

> venture which has engaged in an act described in violation of paragraph (1), knowing that force, fraud or coercion . . . will be used to cause the person to engage in a commercial sex act, or that the person has not attained the age of 18 years and will be caused to engage in a commercial sex act, shall be punished as provided in subsection (b).
>
> (b) The punishment for an offense under subsection (a) is –
>
> (1) if the offense was effected by force, fraud or coercion or if the person transported had not attained the age of 14 years at the time of such offense, by fine under this title or imprisonment for any term or years or for life, or both; or
>
> (2) if the offense was not so effected, and the person transported had attained the age of 14 years but had not attained the age of 18 years at the time of such offense, by a fine under this title or imprisonment for not more than 40 years, or both.

In summary, the statute makes it illegal to recruit, entice, obtain, provide, move, or harbor a person, or to benefit from such activities, knowing that the person will be caused to engage in commercial sex acts where the person is under eighteen **or** where force, fraud, or coercion exists. As written, this statute can be applied to both the pimp, who recruits or provides the minor, and to the customer who obtains the minor for sex. This statute does not require that either the defendant or the victim actually travel. The federal jurisdictional hook in the statute uses the language "in or affecting interstate commerce." This provision makes the jurisdictional reach of this statute broader than the older Mann Act derived statutes described below, which require actual travel. Although there is no case law interpreting the appropriate reach of the jurisdictional hook in the specific context of 18 U.S.C. § 1591, analogous provisions are included in 18 U.S.C. § 922(g) (criminalizing, *inter alia*, possession of a firearm "in or affecting interstate commerce"); 18 U.S.C. § 844(i) (criminalizing use of fire or explosives to damage or destroy any building, vehicle or other property used in, or affecting, interstate or foreign commerce); and 18 U.S.C. § 1951(a) (The Hobbs Act) (criminalizing acts which "in any way or degree obstruct[], delay[] or affect[] commerce…"). These statutes have a significant volume of case law interpreting the jurisdictional language.

The statute defines "Commercial Sex Act" as any sexual act for which something of value is given or received. 18 U.S.C. § 1591(c)(1). "Coercion" is defined as:

1) actual threats of harm;

2) any scheme intended to cause the victim to believe harm would result; or

3) threats of legal repercussions against the victim.

18 U.S.C. § 1591(c)(2). Statutory penalties for violating § 1591 are quite severe. In instances where no force, fraud, or coercion is used, and in which the victim is between fourteen and eighteen years of age, the statutory maximum penalty is forty years imprisonment. If the victim has not attained the age of fourteen, or in instances when force, fraud, or coercion can be proved, the statutory maximum penalty is any term of years or life imprisonment. It is important to note that 18 U.S.C. § 1591 includes an attempt provision.

A prosecutor with a case of international or interstate sex trafficking of minors may also charge violations of 18 U.S.C. §§ 2421-2423. Each of the statutes requires that the government show actual travel in interstate commerce, or a specific use of the channels of interstate commerce for illegal sexual activity.

Although these statutes have been refined over the years, they have their origins in the 1910 Mann Act. In this case, age has some advantages as there is extensive case law interpreting the Mann Act and working out any Constitutional kinks. See, for example, *Hoke v. United States*, 227 U.S. 308 (1913) (holding Mann Act constitutional under commerce power); *Caminetti v. United States*, 242 U.S. 470 (1917) (holding that Congress' authority under the Commerce Clause to keep the channels of interstate commerce free from immoral or injurious uses is unquestioned).

Passage of the PROTECT Act has made significant changes designed to enhance the effectiveness of 18 U.S.C. §§ 2422 and 2423. Title 18, Section 2421 of the United States Code provides:

> Whoever knowingly transports any individual in interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such individual engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title or imprisoned not more than 10 years, or both.

The statute really needs no summary or explanation, but there are two important points to make about 18 U.S.C. § 2421: (1) it applies to transportation of *any individual*; and (2) of the three statutes (18 U.S.C. §§ 2421, 2422 and 2423), it has the lowest potential statutory maximum sentence. These two points lead to the natural conclusion that, in instances when minors are being trafficked for sex, the prosecutor should look first to one of the other applicable statutes with sentencing structures that reflect the involvement of underage victims.

Title 18, Section 2422 of the United States Code applies to defendants who coerce or entice either adults or minors to engage in illegal sexual activity:

> (a) Whoever knowingly persuades, induces, entices or coerces any individual to travel in interstate or foreign commerce, or in any Territory or Possession of the United States, to engage in prostitution or in any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title or imprisoned not more than 20 years, or both,
>
> (b) Whoever, using the mail or any facility or means of interstate or foreign commerce or within the special maritime and territorial jurisdiction of the United States knowingly persuades, induces, entices, or coerces any individual who has not attained the age of 18 years, to engage in prostitution or any sexual activity for which any person can be charged with a criminal offense, or attempts to do so, shall be fined under this title and imprisoned not less than 5 years and not more than 30 years.

The PROTECT Act raised the maximum sentence under section 2422(a), and both established a mandatory minimum sentence and raised the maximum sentence under section 2422(b). Notably, in *United States v. Bailey*, 228 F.3d 637 (6th Cir. 2000), the court held that a conviction under 18 U.S.C. § 2422(b) required a finding only of intent to persuade or attempt to persuade, and not of intent to perform a sexual act following persuasion.

Congress extensively amended 18 U.S.C. § 2423, the statute addressing interstate or international transportation of minors for illegal sexual activity, in the PROTECT Act. The newly revised statute provides:

> (a) Transportation with intent to engage in criminal sexual activity. – A person who knowingly transports an individual who has not attained the age of 18 years in interstate or foreign commerce, or in any commonwealth, territory or possession of the United States, with the intent that the individual engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, shall be fined under this title and imprisoned not less than 5 years and not more than 30 years.
>
> (b) Travel with intent to engage in illicit sexual conduct. – A person who travels in interstate commerce or travels into the United States, or a United States citizen or alien admitted for permanent residence in the United States who travels in foreign commerce, for the purpose of engaging in any illicit sexual conduct with another person shall be fined under this title or imprisoned not more than 30 years, or both.
>
> (c) Engaging in illicit sexual conduct in foreign places. – Any United States citizen or alien admitted for permanent residence who travels in foreign commerce, and engages in any illicit sexual conduct with another person shall be fined under this title or imprisoned not more than 30 years, or both.
>
> (d) Ancillary offenses. – Whoever, for the purpose of commercial advantage or private financial gain, arranges, induces, procures, or facilitates the travel of a person knowing that such a person is traveling in interstate commerce or foreign commerce for the purpose of engaging in illicit sexual conduct shall be fined under this title, imprisoned not more than 30 years, or both.
>
> (e) Attempt and Conspiracy. – Whoever attempts or conspires to violate subsection (a), (b), (c), or (d) shall be punishable in that same manner as a completed violation of that subsection.
>
> (f) Definition. – As used in this section the term "illicit sexual conduct" means (1) a sexual act (as defined in section 2246) with a person under 18 years of age that would be in violation of chapter 109A if the sexual act occurred in the special maritime and territorial jurisdiction of the United States; or (2) any commercial sex act (as defined in section 1591) with a person under 18 years of age.
>
> (g) Defense. – In a prosecution based on illicit sexual conduct as defined in subsection (f)(2), it is a defense which the defendant must establish by a preponderance of the evidence, that the defendant reasonably

believed that the person with whom the defendant engaged in the commercial sex act had attained the age of 18 years.

18 U.S.C. § 2423.

The PROTECT Act amendments enhance the statute in several ways:

(1) in the area of sex tourism, a new provision 2423(c) makes it sufficient to show that a United States citizen or lawful permanent resident traveled abroad and engaged in any illicit sexual conduct with a minor, regardless of what his intentions may have been when he left the United States;

(2) the addition of 2423(d) specifically reaches any person who knowingly "arranges, induces, procures, or facilitates the travel" of an individual they know is traveling for the purpose of engaging in illicit sexual conduct, when they engage in facilitating the travel for the purpose of commercial advantage or private financial gain (*i.e.*, sex tour operators);

(3) new provision 2423(e) punishes an attempt or conspiracy to violate any of the provisions in 2423;

(4) the definitions contained in 2423(f) broaden the prohibited conduct under the statute to include commercial sex acts (as defined in 18 U.S.C. § 1591(c)(1)) with persons under 18; and

(5) for defendants charged under the sex tourism provision, 2423(c), an affirmative defense was added for defendant who "reasonably believed" that person who had engaged in the commercial sex act was eighteen. The defendant bears the burden of proving the affirmative defense by a preponderance of the evidence.

The PROTECT Act also changed the sentencing scheme for 18 U.S.C. § 2423. For 18 U.S.C. § 2423(a)(traveling for criminal sex act), the maximum sentence was upgraded to thirty years imprisonment. Formerly, the equivalent provision had a maximum sentence of fifteen years. A mandatory minimum sentence of five years was also enacted. In the revision to section 2423(b), the maximum sentence was also upgraded from fifteen to thirty years imprisonment.

IV. *United States v. Quinton Williams*, CR-S-03-0046-KJD-RJJ (D. Nev. 2003)

Recently, AUSAs Howard J. Zlotnick and Justin J. Roberts successfully prosecuted a case of interstate sex trafficking under 18 U.S.C. § 1591, and other violations, in the District of Nevada. Following a three-day jury trial, Quinton Williams was convicted of transporting a minor for prostitution, transporting an adult for prostitution, sex trafficking of children, money laundering, and interstate travel in aid of racketeering. Williams, a Chicago resident, operated a prostitution business in which he transported women, including minors, across state lines for the purposes of prostitution or other illegal sexual activity. During 2001, Williams transported a sixteen-year-old juvenile and an adult prostitute by automobile from Chicago to Portage, Indiana, Houston, Texas, Phoenix, Arizona, and Las Vegas, Nevada. In those cities, the defendant supervised the prostitution activities of the adult and minor female, and he collected and kept all of their earnings. The defendant had no source of income other than from the illegal prostitution activity. For approximately the last ten years, the defendant filed only one federal individual income tax return with total reported earnings of less than $500. Williams has prior felony convictions for attempted robbery and narcotics trafficking. The case was investigated by IRS Criminal Investigation Unit and the Las Vegas Metropolitan Police Department. This case represents the first jury trial on an 18 U.S.C. § 1591 charge since the statute was amended by the TVPA in 2000.

Although the United States Attorney's Office in the District of Nevada ultimately achieved a successful result, this case was not without a challenge that often occurs in interstate sex trafficking cases. Both the adult and juvenile, who had been transported by Williams, disappeared and were not available to testify at trial. Originally, a criminal complaint was filed in the Fall of 2002, but it had to be dismissed because the witnesses vanished. The adult prostitute Williams had transported to Nevada was later arrested on new charges in Las Vegas. At that time, the prosecutors were able to make out a new criminal complaint against Williams based upon his money laundering activity. After filing the complaint, they compelled a deposition of the adult prostitute as a material witness under FED. R. CRIM. P. 15. Although the prosecutors were never able to locate the adult witness for further testimony after the deposition, they were able to use the deposition testimony at pretrial proceedings and at trial. Contents of the deposition were corroborated by police reports from all of the cities to which the defendant and witness had traveled.

In addition, the prosecutors presented the juvenile witness to the grand jury at the earliest possible opportunity after locating her. This proved to be a very important and smart strategy

because the juvenile witness became less cooperative, ultimately disappeared, and was not available as a trial witness. The grand jury testimony was admitted at trial and it corroborated information about the defendant's dates and locations of travel contained in the adult witness' deposition. Further, since the juvenile witness was not available to testify, certain hearsay statements she made to her mother, implicating the defendant, were admitted at trial.

Quinton Williams was sentenced to 125 months in prison, the high-end of the sentencing guideline range. Williams has filed an appeal, which is currently pending in the United States Court of Appeals for the Ninth Circuit.

V. Conclusion

The heinous crime of interstate and international trafficking of children for sex in the United States is on the rise. Thousands of minors are exploited within our own borders for prostitution and other illicit sexual activities and, by all reports, the numbers are increasing. Recent amendments to several federal statutes significantly enhance prosecutors' abilities to seek justice for children. Whether those children are from the United States or abroad, it is beyond question that they are the most vulnerable victims of the business of illegal sex.❖

ABOUT THE AUTHOR

❑**Sara L. Gottovi** joined CEOS as a Trial Attorney in 2002. Prior to joining the Justice Department, Ms. Gottovi was in private practice for three years at Covington & Burling. She has previously published *United States v. Lopez: Theoretical Bang and Practical Whimper? An Illustrative Analysis Based on Lower Court Treatment of the Child Support Recovery Act*, 38 WM.& MARY L. REV. 677 (1997).✠

Establishing the Interstate Nexus in Child Pornography Cases

Paul Almanza
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

I. Introduction

Establishing a federal jurisdictional nexus in child pornography cases is critical to success, yet can easily be taken for granted until the eleventh hour. Because federal jurisdiction in the child pornography statutes rests on the Commerce Clause, the statutes, including 18 U.S.C. §§ 2251, 2252, and 2252A, contain jurisdictional elements that the prosecution must prove in order to obtain a conviction. These elements generally are that: (1) the defendant knew or had reason to know that the child pornography would be transported in interstate or foreign commerce (*e.g.*, 18 U.S.C. § 2251(a)); (2) the child pornography was produced using materials that had traveled in interstate commerce (*e.g.*, 18 U.S.C. § 2252(a)(4)(b)); or (3) the child pornography had traveled in interstate commerce (*e.g.*, 18 U.S.C. § 2252A(a)(2)(b)). Unfortunately, some courts are unwilling to rely on the second element to establish an interstate nexus.

Indeed, in two recent cases in which the interstate nexus was based solely on the fact that the child pornography was produced using materials that had traveled in interstate commerce, two circuit courts of appeal reversed child pornography convictions, concluding that the prosecution failed to prove a sufficient nexus to interstate commerce to confer federal jurisdiction under the Commerce Clause. This article first outlines Supreme Court jurisprudence concerning the nexus to interstate commerce that prosecutors must establish in child pornography cases under 18 U.S.C. §§ 2251, 2252, and 2252A. It then

explores the analysis underlying the recent adverse circuit court decisions in order to fully explain the nature of the problem prosecutors may face, while pointing out that the majority of circuits to consider the issue have found in the government's favor. Finally, this article outlines ways that prosecutors can meet their burden of establishing a sufficient nexus to interstate commerce.

The current controversy surrounding the interstate nexus for child pornography produced using materials that traveled in interstate commerce can be summarized as follows. In essence, the fact that child pornography was produced using materials that traveled in interstate commerce is a statutory element of the offense. Two circuit courts have held that even when the government proves that statutory element, it must still establish through competent proof that, under the facts of the particular case, Congress did not exceed its authority under the Commerce Clause. This means that, in addition to the statutory element, the government must prove that the offense conduct impacted interstate commerce, *i.e.*, a nexus to interstate commerce. Using this analysis, the Ninth and Sixth Circuits held that while the government proved the statutory element, the offense conduct did not have a sufficient nexus to interstate commerce. In similar circumstances, however, other courts have found that a sufficient nexus was proven. The latter courts base their conclusions on the fact that Congress determined (in the legislative history of the statutes) that the purely intrastate possession of child pornography affects interstate commerce.

II. Supreme Court jurisprudence requires a sufficient impact on interstate commerce to confer federal jurisdiction under the Commerce Clause.

In *United States v. Lopez*, 514 U.S. 549 (1995), the United States Supreme Court held that the Commerce Clause allows Congress to regulate: (a) "the channels of interstate commerce," (b) "the instrumentalities of interstate commerce, or persons or things in interstate commerce," and (c) "those activities having a substantial relation to interstate commerce, *i.e.*, those activities that substantially affect interstate commerce." *Id.* at 558-59. In cases involving child pornography that actually traveled in interstate commerce, prosecutors generally have little difficulty in establishing a nexus to interstate commerce.

Prosecutors may have to work harder to establish this nexus, however, in cases involving child pornography that was produced using materials that had traveled in interstate commerce. Typically, prosecutors rely on this jurisdictional element when they cannot prove the child pornography, itself, traveled in interstate commerce, but can prove the materials used to produce the child pornography did. Commerce Clause jurisdiction in such cases depends on the third *Lopez* category, governing activities that have a substantial effect on interstate commerce. In *United States v. Morrison*, 529 U.S. 598 (2000), the Supreme Court established a four part test used to determine whether an activity "substantially affects" interstate commerce: (a) whether the statute regulates commerce or economic activity; (b) whether the statute contains a jurisdictional element that limits its application; (c) whether the statute or its legislative history contains congressional findings that the activity affects interstate commerce; and (d) whether there is an attenuated link between the activity and a substantial effect on interstate commerce. *Id.* at 610-12. Against this backdrop, several courts have considered whether child pornography that was produced using materials that traveled in interstate commerce, but that remained intrastate itself, creates a sufficient interstate nexus for federal jurisdiction. While a majority of courts have found this nexus sufficient, two circuits have not.

III. Though taking a minority view, the Ninth and Sixth Circuits have found a lack of sufficient nexus to interstate commerce where materials used to produce child pornography traveled in interstate commerce.

In two rather troubling opinions, the Ninth and Sixth Circuit Courts of Appeal have reversed convictions on the grounds that the prosecution failed to prove a sufficient nexus between the defendant's actions and interstate commerce. In neither case did the courts find the statutes unconstitutional on their face. Rather, in both cases, the courts found the statute unconstitutional as applied to the facts before them.

In *United States v. McCoy*, 323 F.3d 1114 (9th Cir. 2003), the Ninth Circuit reversed a conviction for the possession of child pornography in violation of 18 U.S.C. § 2252(a)(4)(B). The court held that intrastate possession of child pornography cannot be prohibited if the images themselves have not traveled in interstate commerce, or if there was no other economic connection to interstate commerce. *Id.* at 1131-33. *McCoy* involved a conditional guilty plea to one count of possession of child pornography in the Southern District of California. *Id.* at 1115-16. Defendant's husband had taken one photograph of her and her ten year

old daughter, partially unclothed, with their genitals exposed. *Id.* The photograph was taken in defendant's home in San Diego, and was discovered and reported to police by the photo developers, also in San Diego, to whom defendant had taken the film for developing. *Id.* Defendant's husband was charged with four counts of production of child pornography, but was acquitted of all counts after a jury trial. *Id.* As part of the plea, the parties stipulated that the camera and film used to take the photograph were manufactured outside California. *Id.* at 1116. These were the only facts that conferred jurisdiction, as there was no evidence that the photograph itself was transported in interstate commerce, or that the defendant intended to sell or otherwise distribute the photograph in interstate commerce. *Id.*

Defendant argued on appeal that 18 U.S.C. § 2252(a)(4)(B) is unconstitutional in that it permits a conviction for possession of child pornography if the materials used to make the child pornography traveled in interstate or foreign commerce. *Id.* After a lengthy discussion of the Supreme Court's Commerce Clause jurisprudence, focusing on *Lopez* and *Morrison*, the Ninth Circuit agreed with the defendant, finding the statute unconstitutional as applied to those "whose noncommercial, noneconomic possession of a prohibited photograph is entirely intrastate in nature." *Id.* at 1131, 1133.

In its analysis, the Ninth Circuit considered several recent cases interpreting whether what it called the "jurisdictional hook" of 18 U.S.C. § 2252(a)(4)(B) (materials used to produce child pornography traveled in interstate commerce) passes muster in light of *Lopez* and *Morrison*. *Id.* at 1124-26. The Ninth Circuit noted that given today's realities, the jurisdictional element will apply to virtually all cases because the materials used to produce child pornography will almost always be produced outside of the state in which a defendant is prosecuted. *Id.* at 1124. The Ninth Circuit declined to follow cases that found the statute constitutional, such as *United States v. Angle*, 234 F.3d 326 (7th Cir. 2000), *cert. denied*, 533 U.S. 932 (2001), *appeal after remand*, 315 F.3d 810 (7th Cir. 2003); *United States v. Kallestad*, 236 F.3d 225 (5th Cir. 2000); and *United States v. Rodia*, 194 F.3d 465 (3d Cir. 1999), *cert. denied*, 529 U.S. 1131 (2002). Instead, it followed the Sixth Circuit in *United States v. Corp*, 236 F.3d 325 (6th Cir. 2001) (*see infra*), in finding the statute unconstitutional as applied. *Id.* at 1119-26, 1131-33.

The court concluded that, under the facts before it, there was no "substantial connection between ... [appellant's] conduct and *any* interstate commercial activity.... The kind of demonstrable and substantial relationship required between intrastate activity and interstate commerce is utterly lacking here." *Id.* at 1132 (emphasis in original). The Ninth Circuit noted that it expressed no opinion as to whether the statute applies "to wholly intrastate possession [of child pornography] of a commercial or economic character." *Id.*

In *United States v. Corp*, 236 F.3d 325 (6th Cir. 2001), the Sixth Circuit reversed a conviction for possession of child pornography produced using materials that had traveled in interstate commerce in violation of 18 U.S.C. § 2252(a)(4)(B) because, as applied to the facts of the case, the statute exceeded Congress' power under the Commerce Clause. The Sixth Circuit found that there was an insufficient nexus between Corp's intrastate possession of child pornography and interstate commerce. *Id.* at 325-26.

Corp involved a conditional guilty plea to one count of possession of child pornography in the Western District of Michigan. *Id.* at 326-27. Defendant had taken sexual photographs of a seventeen-year-old girl, months away from her eighteenth birthday. There was no indication that he distributed these pictures or that he intended to do so, nor was there any sign that the pictures had traveled in interstate commerce. *Id.* at 326. Federal jurisdiction was thus predicated on the fact that the photographic paper used to produce the photographs was made in Germany. *Id.*

The Sixth Circuit did not find § 2252(a)(4)(B) unconstitutional on its face, although it noted that it had "serious questions" about whether the statute passed constitutional muster. *Id.* at 332. Rather, the court found that, as applied to defendant, whose activity "was not of a type demonstrated *substantially* to be connected or related to interstate commerce," (emphasis in original), the statute exceeded Congress' power under the Commerce Clause. *Id.* The court then listed several factors it believed relevant to a determination as to whether a defendant's activity has a substantial effect on interstate commerce:

> Was the activity ... related to explicit and graphic pictures of children engaged in sexual activity, particularly children about fourteen years of age or under, for commercial or exploitive purposes? Were there multiple children so pictured? Were the children otherwise sexually abused?

> Was there a record that defendant repeatedly engaged in such conduct or other sexually abusive conduct with children? Did defendant move from place to place, or state to state, and repeatedly engage in production of such pictures of children?

Id. at 333.

The factors set forth in *Corp* are somewhat disjointed. Certain of them would confer an independent jurisdictional basis, such as asking if the defendant moved from state to state and repeatedly engaged in production of child pornography. In such a case, there likely would be jurisdiction based on interstate travel. Other factors are not particularly germane to a child pornography possession case, such as asking whether the children depicted in child pornography were otherwise sexually abused. Whether the children were or were not otherwise sexually abused does not impact the defendant's conduct in possessing the child pornography. The factors enumerated by the court read more like prosecution guidelines than jurisdictional elements. It is likely that the court was troubled by the exercise of prosecutorial discretion under the facts of this case. Nevertheless, in the Sixth Circuit, prosecutors must now consider these factors when evaluating a case where jurisdiction will be based on the out-of-state origin of the materials used to produce the child pornography.

IV. The majority of circuits have found a sufficient nexus to interstate commerce in cases where the materials used to produce child pornography traveled in interstate commerce.

In addition to the Third, Fifth, and Seventh Circuit cases cited above, upholding federal jurisdiction in cases where the materials used to produce the child pornography had traveled in interstate commerce (*Rodia*, *Kallestad*, and *Angle*, respectively), the First and Eighth Circuits have upheld federal jurisdiction relying, in large part, on the mere proof of the statutory element. *United States v. Robinson*, 137 F.3d 652 (1st Cir. 1998); *United States v. Bausch*, 140 F.3d 739 (8th Cir. 1998). Additionally, in two recent cases, the Second and the Ninth Circuits have upheld prosecutions in which federal jurisdiction was based on the out-of-state origin of the materials used to produce the child pornography at issue. *United States v. Holston*, 343 F.3d 83 (2d Cir. 2003) (upholding 18 U.S.C. §2251(a)); *United States v. Adams*, 343 F.3d 1024 (9th Cir. 2003) (upholding 18 U.S.C. § 2252(a)(4)(B) and distinguishing *McCoy* because the defendant in *Adams*, unlike the defendant in *McCoy*, possessed "commercial" child pornography). Taken together, these opinions from seven circuits indicate that courts are reluctant to follow *McCoy* and *Corp* in finding this jurisdictional basis unconstitutional.

Kallestad, *Rodia*, *Angle, Holston*, and *Adams* adopt the view that federal jurisdiction is permissible under the Commerce Clause because there is a nexus between the intrastate possession of child pornography and interstate commerce. *See Kallestad*, 236 F.3d at 230 ("Congress could rationally determine that banning purely local possession [of child pornography] was a necessary adjunct to its effort to ban interstate traffic"); *Rodia*, 194 F.3d at 479 ("Congress rationally could have believed that child pornography that did not itself travel in interstate commerce has a substantial effect in interstate commerce, and is thus a valid subject of regulation under the Commerce Clause"); *Angle*, 234 F.3d at 338 ("there is a nexus, via a market theory, between interstate commerce and the intrastate possession of child pornography"); *Holston*, 343 F.3d at 90 (Congress has the power to "prohibit local production that feeds the national market and stimulates demand, as this production substantially affects interstate commerce"). While these cases discuss the jurisdictional element in the relevant statutes, they do not ascribe much importance to it in their Commerce Clause analysis.

Robinson and *Bausch*, on the other hand, appear to conclude that proof of the statutory element (*i.e.*, that the image was produced using material that traveled in interstate commerce) *necessarily* establishes a sufficient nexus. Accordingly, in the First and Eighth Circuits, prosecutors should have little difficulty establishing a nexus to interstate commerce because they only need show that the bare requirements of the statutory element are met. Note that *Robinson, Bausch*, and *Rodia* predate the Supreme Court's opinion in *Morrison*. However, *Morrison* does not compel a different result than that reached by those courts because other post-*Morrison* courts have upheld the constitutionality of the statute. Specifically, the Eighth Circuit followed *Bausch* in *United States v. Hampton*, 260 F.3d 832 (8th Cir. 2001), *cert. denied*, 535 U.S. 1058 (2002) and in *United States v. Hoggard*, 254 F.3d 744 (8th Cir. 2001), while the Third Circuit reaffirmed the vitality of *Rodia* in *United States v. Galo*, 239 F.3d 572 (3d Cir. 2001) and *Doe v. Chamberlin*, 299 F.3d 192 (3d Cir. 2002).

V. Prosecutors can prove a nexus to interstate commerce in a variety of ways.

A. The image traveled in interstate commerce.

The cleanest way for a prosecutor to establish the interstate commerce nexus in a child pornography case is to show that the image at issue actually traveled in interstate commerce. If the image in photograph or video form physically was transported across state lines, or if the image in digital form crossed state lines via the Internet, prosecutors should have no problem establishing a nexus to interstate commerce.

The physical transportation of an image was discussed in *United States v. Tampico*, 297 F.3d 396 (5th Cir. 2002). *Tampico* involved a violation of 18 U.S.C. § 2252A(a)(2), in that the defendant distributed child pornography to his next door neighbor in Texas. The child pornography had traveled in interstate commerce because Tampico had brought it from California when he moved to Texas. *Id.* at 398. The Fifth Circuit upheld Tampico's conviction because the interstate commerce nexus was established by the child pornography having moved in interstate commerce before Tampico distributed it to his next door neighbor. *Id.* at 400.

Another case involving physical transportation of an image is *United States v. Schaffner*, 258 F.3d 675 (7th Cir. 2001), *cert. denied*, 534 U.S. 1148 (2002), a case involving a violation of 18 U.S.C. § 2251(a). Schaffner took a sexually explicit picture of a fifteen-year-old girl in Minnesota and then took the picture to Wisconsin, where authorities discovered it. *Id.* at 677. The Seventh Circuit found that the movement of the photograph across state lines impacted interstate commerce and implicated Congress' "concern that this evil not be spread or encouraged through the use of the channels of interstate commerce." *Id.* at 683. Moreover, the court reasoned that "Congress could have determined that the most effective way of curbing . . . [child pornography's] spread was to sanction the producer whenever his product crossed a state line and had the opportunity to fuel the demand for such material in another locale." *Id.*

When the basis for jurisdiction is that the image traveled in interstate commerce, prosecutors should take care to show that *each* charged image, in fact, traveled in interstate commerce. In *United States v. Runyan*, 290 F.3d 223 (5th Cir. 2002), *cert. denied*, 537 U.S. 888 (2002), an Internet case involving violations of 18 U.S.C. §§ 2251 and 2252A, jurisdiction on the § 2252A count was predicated on the fact that the images defendant received and possessed had traveled in interstate commerce. *Id.* at 240. In affirming the government's use of circumstantial evidence to show that the images at issue were obtained from the Internet (such as the fact that one image retrieved from defendant's computer had a Web site address and language describing the child pornography available at that site embedded on it), the Fifth Circuit emphasized that "the Government must make a specific connection between the images introduced at trial and the Internet to prove the requisite jurisdictional nexus." *Id* at 242. Although the court affirmed most of defendant's convictions, it reversed his conviction for distribution in violation of § 2252A on the grounds that the government presented no evidence that he actually distributed the images he produced to anyone, or that he actually transported these images in interstate commerce. *Id.* at 243.

Similarly, in *United States v. Ellyson*, 326 F.3d 522 (4th Cir. 2002), a case involving possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), a number of the images contained Internet addresses of European child pornography Web sites or logos of particular Web sites. *Id.* at 533. The court followed *Runyan* in concluding that this kind of evidence, when verified and explained by an experienced agent, "is sufficient evidence, albeit circumstantial, to establish an interstate nexus...." *Id.*

Of course, images that actually travel across state lines via the Internet confer federal jurisdiction. In *United States v. Kimler*, 335 F.3d 1132 (10th Cir. 2003), a case involving various violations of 18 U.S.C. § 2252, defendant received and transmitted child pornography "over the Internet across state lines via telephone wires." *Id.* at 1139. The Circuit found there was more than sufficient evidence to support the interstate commerce element of the statute. *Id.* at 1140.

B. The defendant intended that the image travel in interstate commerce, or knew or had reason to know that the image would so travel.

Prosecutors can also establish the requisite nexus to interstate commerce by showing that the defendant intended that the image travel in interstate commerce or that he knew or should have known that it would. When a defendant's knowledge or intent is at issue, prosecutors should be attuned to using circumstantial evidence or statements by the defendant to show the fact finder what was in the defendant's mind.

Circumstantial evidence of intent was sufficient in *United States v. Buculei*, 262 F.3d

322 (4th Cir. 2001), *cert. denied*, 535 U.S. 963 (2002), a case involving a violation of 18 U.S.C. § 2251(a). Federal jurisdiction was premised on the defendant's intent to produce child pornography in Maryland and to transport that child pornography to New York, his state of residence. *Id.* at 330 (the evidence of intent appears to have been purely circumstantial). Although defendant was unsuccessful in actually producing child pornography because he had not fully rewound the videotape he used to record his sexual activity with the minor in Maryland, the Fourth Circuit affirmed his conviction because he induced the minor to engage in sexually explicit conduct for the purpose of making a visual depiction of that conduct. *Id.* at 328. In response to defendant's claim that the statute could not be constitutionally applied to him, the court explained that Congress "rationally determined that eliminating such pernicious activity [the intent to transport child pornography in interstate commerce] will reduce the enormous interstate market in child pornography." *Id.* at 330. The court thus affirmed, finding the application of the statute to defendant within Congress' Commerce Clause authority. *Id.*

The defendant's statements were sufficient to prove his intent that the images travel in interstate commerce in *Runyan*, a case involving violations of 18 U.S.C. §§ 2251 and 2252A. Federal jurisdiction on the Section 2251 violation was premised on defendant's statements to the victim that he would use the Internet to solicit people to buy the sexually explicit pictures he took of her, and that he planned to sell those pictures to people in another country. *Runyan*, 290 F.3d at 238-39. The Fifth Circuit rejected defendant's argument that planning to sell images over the Internet was not sufficient to establish a nexus to interstate commerce, finding that "transmission of photographs by means of the Internet is tantamount to moving photographs across state lines and thus constitutes transportation in interstate commerce." *Id.* at 239 (*quoting United States v. Carroll*, 105 F.3d 740, 742 (1st Cir. 1997) (internal marks omitted).

C. The materials used to produce the image traveled in interstate commerce.

Despite the cases cited above in section III, there is authority for the proposition that Commerce Clause jurisdiction attaches when the materials used to produce the child pornography at issue travel in interstate commerce. Prosecutors should be aware that this jurisdictional element, while called into question by the highly-publicized cases of *McCoy* and *Corp*, is still alive and well.

The out-of-state origin of computer disks can be sufficient to confer Commerce Clause jurisdiction. In *United States v. Guagliardo*, 278 F.3d 868 (9th Cir. 2002), *cert. denied*, 537 U.S. 1004 (2002), a case involving possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), the Ninth Circuit upheld a conviction where jurisdiction was premised on the defendant having copied child pornography onto computer disks that had been made overseas. *Id.* at 870-71. Interestingly, this case was not cited by the Ninth Circuit panel in *McCoy*, perhaps because the *Guagliardo* panel did not engage in Commerce Clause analysis.

Similarly, the foreign origin of a computer hard drive can establish the necessary nexus to interstate commerce. In *United States v. Anderson*, 280 F.3d 1121 (7th Cir. 2002), *cert. denied*, 537 U.S. 1176 (2003), a case involving possession of child pornography on defendant's hard drive in violation of 18 U.S.C. §2252A(a)(5)(B), jurisdiction was predicated on the hard drive having been made overseas. *Id.* at 1123. The Seventh Circuit, citing *Angle* for the proposition that images are "produced" for purposes of the statute when computer equipment is used to copy or download them, found that the government had established the jurisdictional element by introducing evidence that the hard drive that "produced" the images had previously traveled in interstate commerce. *Id.* at 1125. Similar arguments could be made in regard to cameras, video equipment, photographic paper, or video tape.

VI. Conclusion

Although the Ninth and Sixth Circuits in *McCoy* and *Corp*, respectively, have called into question whether Congress has the authority under the Commerce Clause to prohibit intrastate activities with respect to child pornography, the majority of the Circuits have found that Congress can do so. Prosecutors should be aware, *McCoy* and *Corp* notwithstanding, that they can still establish a sufficient nexus to interstate commerce in most cases, even where the child pornography images themselves did not cross state lines.❖

ABOUT THE AUTHOR

❑**Paul Almanza** is a Trial Attorney in the Child Exploitation and Obscenity Section (CEOS). Prior to joining CEOS in 2002, Mr. Almanza practiced white collar criminal defense with McKenna Long & Aldridge and served on active duty in the U.S. Army JAG Corps.✠

Making a Child Exploitation Case with Computer Forensics

James Fottrell
Manager, High Tech Investigative Unit
Child Exploitation and Obscenity Section
Criminal Division

Michelle Morgan-Kelly
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

I. Introduction

A target's computer has been seized after he e-mailed an image of child pornography to an undercover agent. However, the computer forensic examiner is inexperienced, with little knowledge of the child exploitation statutes and the type of evidence needed to support every element of each crime. If the AUSA is new to Internet child exploitation crimes or computer forensics, supervising a complete evaluation of a computer hard drive may seem like a daunting task. Yet there may be substantial evidence, within the target's computer, of crimes far in excess of the single distribution count already on the table. Approaching the evaluation of computer evidence methodically and with common sense will ensure that all critical evidence is obtained and the best possible case is mounted against the target.

Before understanding how the target uses his computer, it is a must to consider how the target thinks. Individuals who trade child pornography generally have several common characteristics. Viewing child pornography is most often symptomatic of the ultimate desire to molest children. Photographs serve to validate these intentions, and sharing photographs and stories with others enhances this validation. Therefore, the deviant activity of child exploitation offenders tends to start small and increase significantly and compulsively. Prosecutors and investigators must begin with an appreciation of the fact that no true pedophile will be satisfied with just one image of child pornography. Thus, pedophiles may begin by "merely" viewing child pornography on free Web sites without downloading any images. They may then graduate to paying for Web site subscriptions, downloading images, joining newsgroups dedicated to pedophilia, trading files through e-mail, peer-to-peer networks or Internet relay chat, and even trolling for minor victims in chat rooms, eventually engaging in private e-mail conversations intended to lure victims into sexual encounters. At the most extreme end of the spectrum, they will photograph or videotape their victims, or even use Web cams for "live feeds," to memorialize and post on the Internet their sexual abuse of the children they victimize. Offenders tend to maintain their collections in a well-organized manner, perhaps by the victims' names, ages, or physical characteristics. Seasoned collectors often seek "new" images (those not previously available on the Internet) and "extreme" images (including, for example, very young children, torture, and bondage). Understanding these behavioral characteristics at the outset can significantly assist a computer forensic investigation.

II. Initial examination of the computer

As a precursor to any child exploitation computer forensic investigation, the accuracy of the computer's Bios date and time stamp must be verified. Through this memory chip, the computer automatically tracks and stores date and time information, and any evidence that is obtained from the computer will be based on the accuracy of the Bios date and time stamp as compared with

the actual time. This memory chip operates on a battery and, therefore, does not lose information when the computer's power is off. It is important to assess the accuracy of the date and time stamp and preserve this information as soon as the computer is seized because the battery will lose its power after a period of time.

The forensic examiner's first step should be to find the actionable child pornography on the target's computer. Thus, he should search the entire hard drive for .jpg (image) files, .mpg or .avi (video) files, and compressed archives, such as zip files, to identify any child pornography. Obtaining the directory structure or path names, for each of these files will indicate where the file was obtained and provide additional support for the case. Accordingly, the AUSA should ask the examiner to identify where these images or videos are located on the computer. In addition, some images or videos may be part of a known series, which also will be helpful for the case. The examiner should flag these.

In searching for child pornography, the examiner should also check external storage media, such as floppy disks, CDs, DVDs, and zip disks, if seized in conjunction with the computer, as well as Web cams and digital cameras. Offenders often save images on these types of storage media that they can relocate or hide and delete the images from their hard drives, in the hopes that their unlawful activities will go undetected by other family members who might use the computer. The volume of images present on the computer and related storage media may provide an indication of the target's preferences regarding children, as well as the length of time that he has been involved in collecting child pornography. It should be noted, however, that broad band connections such as Digital Subscriber Line (DSL) or cable modem allow traders to increase their collections quickly despite having collected for a relatively short period of time.

In addition, though unpleasant, it is critical for prosecutors to view the images retrieved from the computer and storage media. New investigators, in particular, may not have a clear understanding of what constitutes "child pornography" under the statutory definition. The investigator may fail to bring to the AUSA's attention images that meet the definition, including images that reflect the lascivious exhibition of the genitals (as opposed to more graphic sexual conduct) or that appear to be older minors. Nevertheless, such images may very well constitute child pornography. Moreover, the images may reveal essential clues that the target has not only possessed, received, or distributed child pornography, but also produced child pornography. For this reason, it is critical to examine the images on the target's computer in conjunction with photographs taken at his home or other location from which the seizure occurred, whenever possible. Items in the background of an image, such as an unusual bedspread or a unique poster, have been traced to targets and have brought about the rescue of victimized children on numerous occasions. The powerful potential of such details should never be overlooked.

Perhaps the most common mistake among inexperienced agents and prosecutors is to assume that once the child pornography is located and possession has been established, the computer forensic examination is over. Nothing, however, could be further from the truth. Locating child pornography on the target's computer is only the first step in building a strong child exploitation case. A thorough examination of every potential channel of Internet communication available to the target is essential in determining where, when, and for how long the target has been possessing, receiving, distributing, or even producing, child pornography.

III. Tracking the source of the child pornography

The first step in tracing the source of the target's child pornography collection is determining the target's mode of Internet connectivity. Is it:

- broadband, *e.g.*, DSL or cable?
- dial-up via modem?
- dedicated access (such as at a university)?
- or is it through one of the new, cutting-edge wireless networks?

The type of connectivity can be determined by examining the hard drive configuration files, which can be analyzed in conjunction with a picture taken at the scene of the search that depicts wires from the computer connected to a jack in the wall. Connectivity must be established as part of the proof that the defendant distributed one image of child pornography to the undercover agent, and is critical to proving any other Internet-related illegal conduct, including establishing an interstate nexus.

Once it has been established how the target is connected to the Internet, it is necessary to determine how he is communicating with like-minded individuals. In addition to explaining the potential source of the target's collection of child pornography, his methods of computer

communication will demonstrate his knowledge, criminal intent, and pattern of behavior over a period of time. He may be accessing Web sites, obtaining images through e-mail, participating in newsgroups, sharing files through Internet relay chat (IRC) or peer-to-peer networks, or using instant messaging. All of these possible channels of access should be explored.

In each investigation it is best to begin with the technology that spawned the investigation. Thus, because the hypothetical case began with an undercover e-mail exchange, begin by analyzing the target's e-mail use. As a general matter, the target may be communicating via e-mail with individuals whom he already knows or whom he met in Internet chat rooms dedicated to pedophilia, or perhaps even with children. His e-mail use may include not only written communication, but the exchange of images containing child pornography. The forensic examiner should first determine what type of e-mail program is installed. E-mail applications can be either client-based or Web-based. Client-side e-mail programs, such as Outlook, Outlook Express, Netscape Communicator, and Eudora, store the user's e-mails on the user's computer. Thus, if the target uses client-based e-mail, the examiner should thoroughly check the "sent," "inbox," "deleted," and "trash" folders. All of these may contain evidence of child exploitation crimes, including images, written communications, stories (either real or fantasy-driven) about child molestation, and even registration or confirmation e-mails for Web site subscriptions or mail orders of child pornography. The "sent" folder should be examined to locate and verify the particular e-mail message that the undercover agent received, which would clearly document criminal distribution. Another good source of information may be the user's address book, which will identify persons with whom he is corresponding. If the target is instead using Web-based e-mail, such as Yahoo!, Hotmail, or America Online, there will be no program on the hard drive containing content. In such cases, the examiner must instead conduct a generic Web analysis, described in more detail below. This will consist primarily of a search for hypertext markup language (.html) pages in unallocated space, which will show fragments of e-mail messages sent or received on the target's computer.

The next step is to analyze the target's Web use. Nearly everyone explores the Internet using a Web browser, and some individuals utilize the Internet to view and obtain child pornography. Indeed, offenders who are relatively new to computers, or new to their deviant interests in children, may initially rely exclusively on the World Wide Web for child pornography. The examiner's first task is to determine which browser the target is using, *e.g.*, Internet Explorer, Netscape Navigator, Mozilla, or others. The examiner should seek evidence of the target's Web use, which may lie in a variety of areas on the computer. For example, the browser may contain "favorites," or Web sites that the user has specifically saved as preferred sites. Selecting child porn Web sites as "favorites" suggests knowledge, intent, and a pattern of behavior by the target, and is therefore helpful evidence. All "favorites" should be examined even if they appear innocuous, as users can easily change the names of the favorites from the Web site's actual uniform resource locator (URL) to a name that will not raise any suspicion.

Another potentially fruitful area for analysis is recently-visited sites, or cache files located in the temporary Internet files folder. These are physically stored on the hard drive and show the .html pages and associated graphics with recently-accessed Web pages. The examiner should also explore the history, or index.dat, file. This file shows the date, time, and location of every step of the target's Web-browsing activity. In addition to showing downloads of images by the user, it will also reflect any search terms that the user entered when visiting various search engines, such as Google or Yahoo! (*e.g.*, "preteen sex" or "lolita"). The history may also show registration or confirmation screens for Web site subscription activity. While the history does include redirects (URLs arrived at by virtue of unwanted pop-up ads), they are clearly identifiable, precluding an argument by a defendant that his access to such a site was an "accident." The history also includes typed URLs, *i.e.*, URLs that the target actually typed, precluding the defendant's argument that he was redirected to these sites.

The history may also include cookies, which are files used by Web sites to uniquely identify each visitor and consist of text files that the user's computer automatically stores about the Web sites visited. Thus, cookies generally reflect the user's preferences or interests. They may indicate that a target is subscribing to a certain site, or may reflect access to Web-based communities that distribute child pornography, through the presence of URLs associated with groups such as Yahoo! Groups and Microsoft Communities. Cookies, however, have some characteristics that diminish their evidentiary value, including the fact that:

- they can be disabled;

- a user can receive redirected cookies, *e.g.*, from pop-up ads in which the user is not interested; and
- most child pornography Web sites do not create cookies.

Newsgroups are another popular method for accessing child pornography. Newsgroups consist of a protocol that facilitates the distribution of text and images relating to a specific topic of interest, such as cooking, hockey, and even child pornography. Newsgroups are similar to e-mail, except that the messages are sent to a specific topic, rather than to a specific person. To determine if a target is using newsgroups, the forensic examiner should look for programs that facilitate newsgroups access, such as Outlook, Outlook Express, or Netscape Communicator, or commercial programs such as Forte's Agent. The examiner should also determine from which newsgroups' server the target's computer was configured to access newsgroups. Newsgroups access is usually bundled as a service through the user's Internet service provider (ISP), but many ISPs filter or limit access to sexual newsgroups. In such circumstances, there may be configuration settings to reflect that the user is accessing a commercial newsgroups provider, such as EZNews, which offers unlimited or unfiltered newsgroups access for a fee. If such activity is identified, the case agent can verify commercial newsgroups access by employing legal process, for example, by checking credit card statements and recent billing activity, to determine the target's length of service.

The target's configuration file will show if he subscribes to any of the roughly 30,000 existing newsgroups. The target's newsgroups software will be configured to download and store images in a particular directory. The examiner should confirm that this configuration matches the directory from which child pornography was recovered. If it does, this provides additional evidence to support receipt of child pornography through newsgroups. If not, it suggests that the target is getting his child pornography from another source. Finally, the newsgroups application may contain log records showing dates and times when files were received. Most newsgroups software automatically schedules receipt of newsgroups communications on specific dates at specific times, *e.g.*, 3:00 a.m. every Saturday, and downloads all messages in subscribed newsgroups. Prosecutors should be cautioned that such a configuration can negatively impact the ability to prove knowing possession or receipt because it occurs automatically. Nevertheless, newsgroups may contain convincing evidence of the distribution of child pornography where targets post images to newsgroups. Like e-mail, "sent items" may reflect images posted by the target, which will match up with the same postings received by the newsgroups server, creating clear evidence of distribution via newsgroups.

A more sophisticated means of communication is IRC, or "Internet relay chat." IRCs are real-time chat rooms organized by specific subject matter. IRC channels or chat rooms exist that are utilized by offenders for the specific purpose of advertising and trading child pornography. These individuals typically create "rules" associated with the use of their files, for example, requiring the upload of one file in exchange for the download of two files. To determine whether the target is using IRC, the examiner should look for an IRC client software program from a third-party provider, such as MIRC, because Microsoft and Netscape do not sell these programs. IRC programs are coupled with FTP file-servers, which allow for the simultaneous transfer of files. For example, MIRC is usually coupled with FTP file server directories such as Panzer and Sphere, which rely on configuration files associated with MIRC to function properly. The FTP file server directory will contain all of the child pornography images that the target has sent or received via IRC. The file server directory will also contain configuration files and settings for those visitors who have connected to the target's file server, which can often result in spin-off investigations of other individuals.

Offenders may also obtain child pornography through peer-to-peer file sharing, or "P2P." P2P software allows individual computers to communicate with one another directly in real-time in order to share files without the use of a central server. The presence of P2P software such as KaZaA, Morpheus, Limewire, Winmx, Blubster, and KaZaA Lite may indicate the target's use of P2P file sharing. The examiner should analyze the target's "shared folder," which may contain files received by the target and/or files placed there by the target for distribution. P2P investigations, however, can be challenging. Because P2P file sharing occurs in real-time with no central server, there are no log records to indicate previous activity. It is also difficult to show a target's knowledge simply based on the presence of child pornography in his shared folder because last modified and last accessed dates may be altered by virus scanning and indexing software, such as Microsoft Fast-Find.

Accordingly, P2P investigations are best done in real-time by an undercover agent. Nevertheless, if the target's computer contains evidence of P2P use, the presence of child pornography in the shared folder should be buttressed with evidence from the Windows media player reflecting that the files received have been viewed by the target. It is also helpful if the examining agent can identify the presence of the same files from the shared folder elsewhere in the computer.

Another possible means of communication is instant messaging (IM), which consists of real-time communication with a specific person. Targets may use IM to send file attachments containing child pornography or to communicate with potential child victims. Evidence of instant messaging will be reflected in the presence of a software application such as AOL instant messenger, Yahoo! Pager, Microsoft Messenger, or ICQ. Some IM software maintain logs of communications while others do not, unless requested by the user.

If all else fails, a tool of last resort is to search for images in unallocated space. Unallocated space reflects portions of the hard drive that have been deleted, but not yet overwritten. This is the last resort because the files and file fragments in unallocated space have been deleted by the user, making it difficult to document the dates and times when the files existed and what the file names were. Where a case relies solely on images in unallocated space, defendants can more easily argue that they did not want the images and just deleted them (though if there are hundreds of images in unallocated space, that would tend to refute such an argument). While images in unallocated space may correlate to images on other storage media, it is often difficult to ascertain how images got into unallocated space, which also diminishes their evidentiary value.

As a final step in any thorough computer forensic examination, it is always prudent to restore the hard drive, and view the computer as the target would have viewed it. This step often further illuminates the specific interests of the target. By seeing how the target arranged his desktop and icons, and even what type of screen savers and wallpaper he used, the examining agent may obtain additional helpful clues to build the case against the target.

IV. Particularly devious defendants

Computers are rapidly becoming the premiere forum for trafficking in child pornography, and therefore, collectors are becoming increasingly computer savvy. Efforts to disguise illegal activities may take a variety of forms, for which the examiner should be on the lookout. Offenders may change the names of files or favorites from names clearly connoting child pornography to benign names. They may store images in zip files (compressed files on the hard drive), which are less readily accessed. Offenders may also delete Internet cache files or delete images (though as discussed above, an examination of unallocated space may disclose such activity). Another increasingly popular covert tactic is to utilize remote storage, *i.e.*, to upload images to Yahoo! groups and store them there, permitting constant access without local presence of the images.

Perhaps the most blatant method of covering one's tracks is to utilize Evidence Eliminator software. The presence of this tool is detectable on a target's computer, as log records in the Windows directory will indicate when the software was installed. In addition, while the software may successfully remove client-side records, records may still exist on the server side. The software also may not be as thorough as offenders would like in every instance. For example, if Evidence Eliminator erased the sent e-mail from the Internet history and temporary Internet files, it still would not delete .html pages in unallocated space, and the server would likely have a record of the e-mail as well. Moreover, even if a communication is deleted, the presence of Evidence Eliminator software provides at least circumstantial evidence of illegal activity.

V. Thorough computer forensics seal a defendant's fate

The multiple aspects of a thorough computer forensic examination may seem intimidating at first, but it is important to consider the rewards that may be reaped from a good forensic investigation. One child exploitation case from several years ago provides a good example. The case began as a possession case in which the forensic agent identified fifty images of child pornography on the defendant's hard drive and copied them to a CD-Rom for the case agent and attorney to review, without documenting the directory structure. The defendant was indicted for possession but, one month before trial, the prosecutor sought further forensic assistance in order to understand the significance of the date and time stamps associated with certain images. In particular, the prosecutor needed to explain when the defendant possessed the child pornography and why there was a series of images dated sequentially over a short period of time. The prosecutor's inquiry prompted further forensic investigation of the target's computer.

The directory structure proved quite significant because it showed that the defendant had been using a Panzer file server connected to IRC to distribute hundreds of images of child pornography over a six-month period. Log records associated with the Panzer file server not only showed the dates and times when the files were sent and received, supporting distribution and receipt counts, but also identified a dozen other people with whom the defendant had been trading for an extended period of time. In addition, the recent directory of the Windows media player showed that images from the Panzer file server had been viewed, indicating defendant's knowing possession. The Panzer file server was also configured by the defendant to receive files in the "downloads" directory, and the defendant had organized the files and placed them in other directories. Moreover, restoring the defendant's hard drive revealed wallpaper consisting of an actionable child pornography image. This image had been saved with an innocuous filename in bitmap format rather than as a .jpg or .mpg file, and therefore, would never have been revealed without restoring the machine. All of the above evidence resulted in a superceding indictment, which included multiple distribution and receipt counts associated with much higher sentences than mere possession. *United States v. Cundiff*, EV99-029-CR-01 (S.D. Ind. Aug. 16, 2000).

VI. Looking beyond the target's computer

As the above discussion indicates, finding child pornography images on a target's computer is only half of the battle. There are other critical aspects to building a strong computer-based child exploitation case, all of which must be facilitated by early and frequent communication between the case agent, forensic examiner, and prosecutor. In addition, as important as the evidence on the computer itself is, the evidence possessed by ISPs is equally so. Because ISPs may only retain their records for a limited period of time, it is crucial to complete the forensic analysis as quickly as possible so that all relevant evidence in the possession of ISPs, as well as other third parties, can be readily obtained.

The constant education of law enforcement regarding emerging technologies is also essential. Individuals who trade child pornography on the Internet quickly embrace new technologies, the manufacturers of which increasingly tout their ability to provide users with heightened anonymity and quicker access to larger quantities of information. As offenders look ahead to new technological developments, law enforcement must keep pace with them in order to prevail.❖

ABOUT THE AUTHORS:

❑**James Fottrell** is the Manager of the High Tech Investigative Unit of the Child Exploitation and Obscenity Section (CEOS). Prior to joining CEOS in 2002, Mr. Fottrell served for twelve years as a computer consultant for the United States Customs Service, focusing on child exploitation cases. Mr. Fottrell lectures frequently on computer forensic investigations.

❑**Michelle Morgan-Kelly** has been a Trial Attorney in the CEOS since 2002. Previously, Ms. Morgan-Kelly spent four years as an intellectual property litigator at Skadden, Arps, Slate, Meagher & Flom LLP. Ms. Morgan-Kelly has published law review and journal articles regarding international parental kidnaping and various aspects of patent litigation.✠

Rescuing Victims of Child Pornography Through Image Analysis

Damon King
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

Michelle Collins
Program Manager
Child Exploitation and Obscenity Section
Criminal Division

Jennifer Lee
Staff Analyst
National Center for Missing and Exploited Children

I. Introduction

Nearly every prosecutor who has worked on a child pornography case is haunted by the images they have viewed. There is, of course, a sense of relief in knowing that a child, in a given image, has been identified and rescued from the horrific abuse he or she has suffered. However, oftentimes the child depicted is totally unknown, and could be anyone, anywhere in the world. Until very recently, there was insufficient focus placed on accomplishing the critical task of identifying victims of child pornography. "For far too long, law enforcement's focus has been on the image itself–with little consideration for the serious abuse depicted in the images," wrote Assistant Attorney General Michael Chertoff, head of the Department of Justice's Criminal Division, in a February 3, 2003 letter to the General Accounting Office. *See also* Max Taylor, *Child Pornography and the Internet: Challenges and Gaps*, Panel presentation to the 2nd World Congress Against the Commercial Sexual Exploitation of Children (Yokohama, December 2001) ("There needs to be a greater focus on the identification of child victims, rather than trading networks.").

Prompted in large part by a growing consensus among federal law enforcement and prosecutors of the importance of identifying the victims depicted in child pornography, the crucial National Child Victim Identification Program (NCVIP) has emerged. As Assistant Attorney General Chertoff aptly explained:

> [T]he NCVIP is primarily intended to help law enforcement identify and stop current instances of child abuse associated with the production of child pornography. The NCVIP will help stop current child abuse by allowing law enforcement, upon discovering an image of child pornography, quickly to determine whether that image is new or dated. If the image is new, law enforcement can then take steps to identify the victim and the producer with the goal of preventing continued abuse of the victim. . . . NCVIP will be instrumental in focusing law enforcement's efforts on current abuse and ensuring that our focus is not simply limited to the trafficking of child pornographic images, but extends to the investigation and prosecution of the underlying abuse.

Statement of Assistant Attorney General Michael Chertoff , United States Government Accounting Office, *File Sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography*, Report 03-351, Appendix III (2003).

Victim identification requires painstaking Image Analysis. Image Analysis is an investigative technique whereby an investigator looks at the child pornography images at issue and attempts to use the information contained in the images to gather intelligence about the victim, the perpetrator, and the location where the victimization occurred. Successfully capturing and synthesizing all of the information that can be gleaned from each child pornography image, and combining that data with all other information known from the investigation, is the key component of Image Analysis. Although the ultimate goal of Image Analysis is to identify and locate the child depicted, the first goal is to narrow the pool of potential victims and perpetrators to a sufficiently discrete geographic area so that a single law enforcement office or task force is able to take ownership of the investigation. This requires developing sufficient information from the images to establish that the victim and/or perpetrator is within the jurisdiction of a specific law enforcement office or task force, and garnering enough information to enable local law enforcement to locate the victim or perpetrator.

II. Every child pornography image is a crime scene

Each image of child pornography displays some information about the victim, the perpetrator, and the location in which the crime occurred, making every child pornography image a crime scene. Often, a significant amount of information can be gleaned merely from a close examination of images. This examination will entail attempting to determine the ages of the child and perpetrator, as well as any identifying physical characteristics concerning each. However, unless specific information is seen in a broader context, this information alone will be of little value. Items seen in the background, such as unique clothing worn by the victim or perpetrator and other distinguishing indicia, may identify a discrete geographic location and ultimately make the noteworthy physical characteristics of the victim or perpetrator useful. The more images that are available for examination, the more likely it is that the critical mass of detail needed for successful identification will be reached.

The following two examples demonstrate how the application of the principles of Image Analysis can help identify child victims and their abusers. In both of these cases, the National Center for Missing and Exploited Children's (NCMEC) Child Victim Identification Project (CVIP) and law enforcement officials used the Image Analysis technique to successfully locate the unidentified child victims in the pornographic images.

A. Somewhere in America

During the first week of November 2002, Interpol contacted the CVIP to share information regarding a series of photographs that were being widely distributed on the Internet. Although Interpol was unaware of any sexually graphic images of this child, it was highly concerned about the child because her photos were being traded in child pornography newsgroups. In addition, photos of this child were discovered on multiple computers belonging to child pornographers in Europe. Interpol notified the CVIP because various items in the background indicated that the photos originated in the United States.

Interpol provided forty non-pornographic images of the child to the CVIP. The CVIP team scrutinized each image and noticed that the child was holding a school yearbook. By magnifying the text on the book, NCMEC analysts were able to identify the high school and its location. In another image, a television program captured in the background contained the logo "GPTV" which was quickly identified as the acronym for "Georgia Public Television."

The CVIP analysts contacted the European organization COPINE (Combating Paedophile Networks in Europe) to request additional images that might assist in the Image Analysis. The COPINE staff provided approximately 940 additional photos of this child. Further analysis of the images revealed the following distinguishing details:

- The child had a broken left wrist during a previous summer;
- An older model, red Toyota Supra GT with no license plates was in the background;
- Photos were taken in front of a white house with burgundy shutters;
- Shell casings from Remington ammunition were on the floor in some images;
- Two additional children were featured in some images. One child wore a necklace with an unusual name spelled with beads; and
- Many photographs were taken indoors, so that plaques and family photos were visible in the background.

The CVIP generated a detailed report and forwarded it to the Internet Crimes Against Children (ICAC) task force of the Georgia Bureau of Investigation (GBI) to seek their assistance in identifying these children. Upon receiving the CVIP report and images, the GBI created a task force to locate the children and identify the producer of the photographs. Ultimately, law enforcement was able to identify a person seen in a framed photograph in the background of an image. Although the person in the framed photograph turned out to be an innocent third party who was not the producer of the photos, this person was able to quickly lead law enforcement to the three children and perpetrator.

Investigators arrested the perpetrator and charged him with fifty-nine counts of sexual exploitation of a minor after they found dozens of sexually explicit pictures of children in his home. The coordination and cooperation between various law enforcement agencies including the GBI, Bibb County District Attorney's Office, Bibb County Sheriff's Office, Macon Police Department, Twiggs County Sheriff's Office, and the Houston County Sheriff's Office, were instrumental in the success of the investigation.

B. A lifesaving t-shirt

On June 21, 2003, an unknown subject dropped off a disposable camera at a drugstore in Prunedale, California. The photo developer contacted the Monterey County Sheriff's Office upon discovering that the majority of the pictures featured a prepubescent girl being sexually assaulted.

The Sheriff's Office reviewed the store's security video, set up surveillance at the store, and lifted fingerprints from the film. In an effort to promptly rescue the child from the abusive situation, a cropped image of the child's t-shirt was aired on a local news network. After this effort failed to generate any significant leads within Monterey County, the Sheriff's Office contacted NCMEC's CVIP for assistance.

The CVIP obtained the cropped image of the child's t-shirt from the Sheriff's Office for further analysis. The t-shirt featured the text "Pep & Cheer" and a logo of a megaphone with the word "Skyhawks" emblazoned across it. The CVIP ran various queries on the Internet and identified a local elementary school in Clovis, California that had a cheerleading squad whose mascot was the skyhawk. The elementary school also had the same blue and green school colors as the victim's t-shirt.

On July 2, 2003, the CVIP contacted the Clovis Police Department and provided the Image Analysis report and cropped photo of the t-shirt. Detective John Weaver immediately visited the elementary school and learned that the t-shirt worn by the child victim had been issued to approximately sixty girls the prior summer during a cheerleading camp. Clovis police coordinated with the Monterey County Sheriff's Office, and through their joint effort the cropped image of the t-shirt was featured the following day on the six o'clock news, airing over a multi-county geographic area.

The adult offender surrendered to the Fresno Police Department the next day, confessed to abusing the victim, and disclosed the identity of the eight-year old victim.

III. Image Analysis tools

Because most child pornography is now discovered in digital format, a basic set of digital imaging tools is needed in order to successfully apply the Image Analysis technique in most cases. Digital "still" images in formats such as JPEG can be examined using inexpensive digital imaging software such as Paint Shop Pro. Video, for example, .mpg and .avi files, can be examined with a variety of inexpensive media player software packages, such as RealOne Player.

In some cases, however, there is more to a particular image than meets the eye. For example, a digital image that is created by a digital camera will oftentimes be in Exchangeable Image File (Exif) format. Basically, Exif format is the same as a JPEG file format. Exif inserts some image/digicam information data and thumbnail image data to JPEG format in conformity to JPEG specifications. Thus, although a seized image may have a filename with a .jpg extension, there may be Exif data (sometimes referred to collectively as an "Exif header") contained within the image. Because most editing and viewing software simply skips past the Exif header and ignores it, a casual viewer normally will not even be aware of its presence. An investigator employing the specialized software to view the Exif data contained in an image, in which the Exif data is intact, can obtain a wealth of information, including the date and time that the image was created, the make and model of the digital camera, and perhaps even the camera's serial number.

IV. Conclusion

Image Analysis is a powerful investigative tool that can be used to locate and rescue the unidentified children depicted in pornographic images. Law enforcement agents and prosecutors should consider employing this technique in every child pornography case in which seized child pornography contains images of unidentified children.❖

ABOUT THE AUTHORS

❑**Damon King** is a Trial Attorney in the Child Exploitation and Obscenity Section. Mr. King joined the Section in 2001 after serving for seven years as a prosecutor in the U.S. Army JAG Corps. For six of those years, he was a Special Assistant United States Attorney in the Eastern District of Virginia.

❑**Michelle Collins** is the Program Manager for the Exploited Child Unit at the National Center for Missing and Exploited Children, where she has been employed for over five years. Ms. Collins oversees the Child Victim Identification Project.

❑**Jennifer Lee** has been a Staff Analyst with the Child Victim Identification Project at NCMEC for the past two years. ✠

Effective Use of the Medical Expert in Child Pornography Cases

Dr. Sharon W. Cooper
Forensic and Developmental Pediatrician
Associate Professor of Pediatrics
University of North Carolina

Damon King
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division

I. Introduction

While not always required, a forensic medical expert can provide essential assistance in the investigation and prosecution of child sexual exploitation cases. In particular, forensic medical experts are helpful in proving that (1) the person depicted in an image is a minor, not an adult, and (2) the person depicted is a "real" minor, as opposed to a "virtual" minor.

II. Deciding whether to use an expert to establish a child's age

Where both the identity of the child depicted in a suspected child pornography image and the approximate date of the image's creation are known, establishing that the image depicts a person under the age of eighteen years should, in most cases, be relatively straightforward. Notable exceptions to this rule include cases of child sex tourism in which the perpetrator produces images of sexually explicit conduct involving one or more child prostitutes in a foreign country. Although law enforcement officials have been increasingly successful at identifying the children depicted in such cases, often, the child himself does not know how old he is and official documentation establishing the child's date of birth is either unobtainable or nonexistent.

However, if a prosecutor is unable to establish that a particular image depicts a child whose identity and age are known, the prosecutor has two options. Under the first option, the prosecutor can proceed without an expert on the basis that the trier of fact can examine the image and determine, without expert testimony, whether the individual is under the age of eighteen. Secondly, the prosecutor can employ an expert, such as a pediatrician, to analyze the image and give an expert opinion as to the age of the person depicted, to aid the jury in making its determination. The decision to implement one strategy over the other will turn on the particular facts of the case. As the Fifth Circuit explained in *United States v. Katz*, 178 F.3d 368 (5th Cir. 1999):

> The threshold question–whether the age of a model in a child pornography prosecution can be determined by a lay jury without the assistance of expert testimony–must be determined on a case by case basis. As the government correctly points out, it is sometimes possible for the fact finder to decide the issue of age in a child pornography case without hearing any expert testimony. However, in other cases, the parties have been allowed to present conflicting expert testimony. In yet other cases, one party presents expert testimony, while the other does not. A case by case analysis will encounter some images in which the models are prepubescent children who are so obviously less than 18 years old that expert testimony is not necessary or helpful to the fact finder. On the other hand, some cases will be based on images of models of sufficient maturity that there is no need for expert testimony. However, in this case, in which the government must prove that a model, who is post-puberty but appears quite young, is less than eighteen years old, expert testimony may well be necessary to assist the trier of fact to understand the evidence or to determine a fact in issue.

Id. at 373 (internal citations omitted).

"There is no requirement that expert testimony be presented in child pornography cases to establish the age of the children in the pictures." *United States v. Nelson,* 38 Fed. Appx. 386, 392 (9th Cir. 2002); *accord United States v. Gallo*, 1988 WL 46293 (4th Cir., May 12, 1988) (unpublished). In cases involving images of clearly prepubescent children, there may be no need to present expert testimony as to whether the image depicts a person under the age of eighteen. *United States v. Fox,* 248 F.3d 394, 409 (5th Cir. 2001) (no abuse of discretion in admitting photographs without testimony as to subjects' ages where even defendant conceded that "[s]ome of the photos appear to be prepubescent children

who are. . . obviously less than 18"), *vacated on other grounds*, 535 U.S. 1014 (2002). Even in instances where the images are of children who are not clearly prepubescent, the images can sometimes be introduced without expert opinion evidence, if bolstered by other evidence. *United States v. Hilton*, 167 F.3d 61, 75 (1st Cir. 1999) ("Without limiting *a priori* the type of evidence that would be admissible on this question in a given case, the following proof could be offered to establish the apparent age of the person shown: the physical characteristics of the person; expert testimony as to the physical development of the depicted person; how the disk, file, or video was labeled or marked by the creator or the distributor of the image, or the defendant himself. . . and the manner in which the image was described, displayed, or advertised. While this list is hardly exhaustive, it gives a flavor of the ways in which a depicted person's apparent age might be objectively proven."); *United States v. O'Malley*, 854 F.2d 1085 (8th Cir. 1988) (sufficient evidence existed to support district court's factual determination that images depicted persons under the age of eighteen where defendant had described one photograph as a twelve-year-old girl engaging in oral sex with "her mother's boyfriend" and photographs depicted young females, one of whom wore braces, and the other appeared "diminutive in all her bodily proportions"). *Id.* at 1086, 1088 n.3.

A trial court may preclude the introduction of certain photographs which otherwise could have been introduced, had the government presented expert testimony to assist the trier of fact in determining age. For example, in *United States v. Riccardi*, 258 F. Supp. 2d 1212 (D. Kan. 2003), rather than simply admitting all six computer images that the government moved to introduce, the trial court "carefully analyzed each computer file to determine whether a lay jury could determine the age of the models without the assistance of an expert. In the end, the court found that only two of the six computer files contained images of models who were so obviously less than 18 years old that expert testimony was not necessary to assist the fact finder." *Id.* at 1219. Thus, in cases in which the age of the person depicted may be difficult to discern, the prudent course is to offer opinion testimony regarding the child's age.

If a prosecutor intends to offer opinion testimony as to the age of children depicted, it is important to employ a qualified witness. Eliciting lay opinion testimony as to the age of children depicted in a charged image should be done with caution, especially with the amendment of FED R. EVID. 701 in 2000 to exclude testimony "based on scientific, technical, or other specialized knowledge within the scope of Rule 702." *Compare United States v. Hall*, 312 F.3d 1250, 1260 (11th Cir. 2002) (Innocent Images Task Force detective testified that based on his training and experience, images depicted minors); *United States v. Davis*, 41 Fed. Appx. 566 (3d Cir. 2002) (testimony from two postal inspectors who had training and experience in child pornography investigations was properly admitted under version of Rule 701 in effect at time of trial); *and United States v. Stanley*, 896 F.2d 450, 451-52 (10th Cir. 1990) (no abuse of discretion in admitting, over defense objection, lay opinion testimony by postal inspector as to age of children depicted); *with Nelson,* 38 Fed. Appx. at 392 (trial court abused its discretion by admitting lay opinion testimony by probation officer and law enforcement witnesses as to age of children depicted because testimony was not "helpful." Given the fact that the images were available for the jury to review, however, error was harmless since any reasonable juror who reviewed pictures would have determined that some of individuals depicted were under eighteen years old).

Federal courts have long admitted testimony by medical professionals, in the form of expert opinion, as to the approximate age range of children depicted in digital computer images, videotapes, and photographs. *See, e.g., United States v. Rayl*, 270 F.3d 709, 714 (8th Cir. 2001) (experienced pediatrician opined that many of children depicted in digital pictures attached to incoming and outgoing e-mails were under age of eighteen); *United States v. Long*, 1997 WL 130079 (6th Cir., Mar. 19, 1997) (pediatrician and forensic psychiatrist who had been a medical doctor for eighteen years opined that some of individuals depicted on two videotapes were under eighteen); *United States v. Broyles*, 37 F.3d 1314, 1317-18 (8th Cir. 1994) (pediatric endocrinologist opined that one girl and one boy depicted in charged videotape were "definitely under age eighteen, with an estimated age for the girl of from nine to fourteen years and of the boy, who was clearly in a pre-pubertal state, from eight to nine years."); *United States v. Snow*, 1990 WL 171572 (6th Cir., Nov. 7, 1990) (unpublished) (forensic pathologist examined two seized publications containing nude photographs and provided medical opinion that all of the models in one publication were under eighteen, but was unable to state opinion as to whether models in second publication were under eighteen).

Prosecutors should be especially wary, however, of defense attempts to present expert

witness testimony from persons who lack sufficient qualifications to give an opinion as to the age of persons depicted in images. For example, in *United States v. Anderton*, 136 F.3d 747, 750 (11th Cir. 1998), the government presented expert testimony from a medical doctor with expertise in adolescent growth and development. The doctor testified that, in her opinion, the children depicted in the charged videotape were between the ages of eleven and fifteen and a half. The defense presented testimony from a clinical psychologist and sex therapist that, in his opinion, the ages of the individuals depicted in the "videotape could not be determined because the pornography industry is 'notorious for picking young looking people.'" On cross examination by the government, the defense expert admitted that he possessed no medical training or experience evaluating adolescent growth and development. Without commenting directly on the defense expert's lack of qualifications, the Eleventh Circuit affirmed the conviction of the defendant, stating that "[t]he jury was free to evaluate both experts' testimony and conclude that the government's expert was more reliable and credible." *Id.* at 750 (internal citations omitted). Although the government's cross-examination was obviously effective in discrediting the defense's "expert" in *Anderton* by demonstrating his lack of qualifications to testify as to the age of the children depicted, in such situations, it would also be appropriate to move the court for a pretrial hearing to consider whether the proposed expert's testimony meets the standard for admissibility set forth by the Supreme Court in *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), and its progeny.

III. Determining age through Tanner staging

The analysis of computer media, photographs, videos, or other published depictions of child pornography by a forensic medical expert to determine age involves several factors. All aspects of physical maturation are considered in order to determine if the image of the person depicted is consistent with a child who is less than eighteen years of age. Factors deemed important include, but are not limited to:

- Body habitus and musculature;
- Height and weight proportion;
- Signs of sexual maturation (breast development, axillary hair, pubic hair distribution, pigmentation of scrotal sac, elongation of the penis, etc.);
- Hirsuitism or degree of hair distribution over the body, especially to include facial hair and axillary hair;
- Fat distribution;
- Extremity length proportion with respect to torso;
- Dentition; and
- Dysmorphia or the appearance of the face and body, which might be consistent with specific developmental syndromes, which may be associated with an abnormal stature or maturation processes.

One component of the medical expert's analysis is "Tanner staging," which is a helpful tool used by medical experts in forming the basis of their opinion as to the age of a child depicted in an image.

Tanner staging was developed four decades ago by Dr. James Tanner, who completed research in the United Kingdom that established the sequence of pubertal changes seen in children. Dr. Tanner established the original definitions of the stages of sexual maturation by reviewing numerous pictures of the breasts and genitals of boys and girls in the U.K. as they began to enter puberty. These stages, now familiar to health care providers as the "Tanner stages," had correlating ages noted by the original researchers, which varied between boys and girls. Tanner used the letter 'B' to refer to breast development, 'PH' for pubic hair distribution, and 'G' for genital or gonad (testes) development. The designations "1-5" denoted increasing maturation signs, such as the pubic hair changing from fine soft hair to a more dense curling hair of a greater distribution. *See* J.M. Tanner, GROWTH AT ADOLESCENCE (Lippincott 2d ed., 1969) and J.M. Tanner, *Sequence, Tempo, and Individual Variation in Growth and Development of Boys and Girls Aged Twelve to Sixteen,* ADOLESCENT BEHAVIOR AND SOCIETY: A BOOK OF READINGS (Rolf Eduard, Helmut Muuss & Harriet Porton eds., 1998).

It is important to recognize that Tanner staging is only one of many tools that a medical expert can use to arrive at a clinical opinion as to the age of a child. In 1998, an inartfully drafted letter was submitted by Dr. Tanner and Dr. Arlan L. Rosenbloom to the editor of the journal, PEDIATRICS, which generated some controversy. Drs. Tanner and Rosenbloom were apparently concerned about the possibility of Tanner staging being used as the sole basis for an expert witness' opinion as to the age of a child, but the text of the letter was read by some as stating that Tanner

staging should not be used at all by medical professionals who testify as expert witnesses. As explained later in letters subsequently submitted by medical professionals, and in a clarifying letter submitted by Dr. Rosenbloom himself, the purpose of the original letter submitted by Drs. Tanner and Rosenbloom was simply to point out that Tanner staging, while scientifically reliable and of value in forming an expert opinion as to the age of a child, is only one tool out of many that a medical professional should employ when making a clinical judgment as to the age of a child. *See* A.L. Rosenbloom and J.M. Tanner, *Misuse of Tanner Puberty Stages to Estimate Chronological Age*, 102(6) PEDIATRICS 1494 (1998); Timothy J. Kutz, Andrew Sirotnak, Angelo P. Giardino, A.L. Rosenbloom, *Tanner Staging and Pornography*,104(4) PEDIATRICS 995 (1999); and James F. McLaughlin and A.L. Rosenbloom, *Misuse of Tanner Scale*, (Dec. 16, 1998) (unpublished letters, on file at www.ci.keene.nh.us/police/tanner%20scale.htm). The controversy generated by the original letter submitted by Drs. Rosenbloom and Tanner is excellently summarized and analyzed in *United States v. Pollard*, 128 F. Supp. 2d 1104 (E.D. Tenn. 2001), which fully describes the proper employment of the medical expert, the usefulness of Tanner staging, and why testimony from a qualified expert, in part based on the expert's consideration of Tanner staging, is properly admissible under the criteria set forth by the Supreme Court in *Daubert* and its progeny.

While experts can utilize Tanner staging and other methods to help establish the age of a child depicted in an image, it is important to note that there may be pitfalls in this process. Poor image quality and other factors can limit the ability of an expert to render a sufficiently reliable opinion as to the age of a child depicted. For example, in *United States v. Katz*, 178 F.3d 368 (5th Cir. 1999), after conducting a *Daubert* hearing, the trial court found a medical expert's opinion admissible as to some images, but not others. With regard to a set of images of children on a charged videotape that the defendant received from a undercover agent in a controlled delivery, the court stated:

> After hearing testimony, the parties stipulated and the district court found that the Tanner Scale has been subject to peer review and publication, that it is a scientifically valid methodology for determining the age of individuals, and that the Government's expert, Dr. Woodling, was qualified to perform Tanner Scale analysis. . . . At the close of the hearing, the district court concluded there was sufficient ability to visualize the Tanner Scale criteria to permit the expert to express a reliable opinion whether the models were less than 18 years old and preliminarily determined that the videotape and the expert witness testimony were admissible. A second hearing was conducted on December 1-4, 1997, immediately prior to the scheduled trial, to resolve all remaining evidentiary issues. The district court reaffirmed that the videotape and government's expert testimony were admissible.

Id. at 370. However, with respect to five color digital images (the "GIF" images) which were on a computer disk delivered to the defendant in the same controlled delivery as the charged videotape, the district court ruled that those images were inadmissible because the government had provided "only poor quality black and white versions of these images to the defense during discovery." *Id*. As a discovery sanction, the trial court permitted only the use of the black and white images, and then ruled that the black and white images were inadmissible under FED. R. EVID. 403 because "they lacked sufficient clarity to determine the models ages under the Tanner Scale and therefore their probative value was outweighed by their prejudicial effect," and because the uncertainty concerning the ethnicity of the model in one photograph and problems with visibility attributed to the angles of some of the photos further reduced the probity of the exhibits. *Id*. at 371. After an interlocutory appeal by the government, the Fifth Circuit affirmed the exclusion of the color photographs and the subsequent exclusion of the black and white copies, finding that the trial court had not abused its discretion in excluding them under FED. R. EVID. 403. (Interestingly, this case involved the same expert whose testimony was later found admissible in *Pollard*.).

IV. Avoiding *Katz* problems

One way to avoid discovery problems, like those in *Katz,* is to make the child pornography evidence available for the defense to inspect in a controlled environment, such as the secure law enforcement facility where the actual case evidence is maintained, instead of providing copies of child pornography to the defense. At least two circuits and one district court have held that the government is not required to provide copies of child pornography to the defense because it is contraband. *See United States v. Horn*, 187 F.3d 781 (8th Cir. 1999); *United States v. Kimbrough*, 69 F.3d 723 (5th Cir. 1995); *United States v. Husband*, 246 F. Supp. 2d 467

(E.D. Va. 2003). In the event, however, that a trial court orders the government to provide copies of the child pornography to the defense over the government's objection, the government should ensure that the court enters a protective order concerning the handling and preservation of the material. The government must also ensure that the materials provided to the defense are exact duplicates of what the government intends to introduce at trial.

Given that the original Tanner studies were limited to Caucasians, an additional basis for excluding one of the images in *Katz* was the uncertainty of the ethnicity of the model in the photo, prompting the district court to note "that the scientific methodology of the Tanner Scale was not sufficiently verified on non-Caucasian individuals." *Katz* at 371. This basis for exclusion is likely no longer valid due to subsequent studies published after *Katz*, correlating ages of children from various ethnic groups with the Tanner stages. Indeed, in November 2002, the medical journal PEDIATRICS published the results of a study that correlated ages with the Tanner stages of maturation amongst a U.S. sample of 4,263 non-Hispanic white, black, and Mexican-American girls and boys aged eight to nineteen. (*See* Tables 1 and 2). Shumei S. Sun, et al., *National Estimates of the Timing of Sexual Maturation and Racial Differences Among U.S. Children*, 110(5) PEDIATRICS 911-919 (2002). This study, coupled with demographic studies conducted in other countries that correlated the ages of children from varying ethnic groups with the Tanner stages (*see* Table 3), should allow a clinician who has experience with the ethnic group depicted to render a reliable opinion as to the age of a child in an image.

[Table 1]

PUBIC HAIR	NON-HISPANIC WHITE	NON-HISPANIC BLACK	MEXICAN-AMERICAN
PH2	10.57 (10.29-10.85)	9.43 (9.05-9.74)	10.39 (-)
PH3	11.80 (11.54-12.07)	10.57 (10.30-10.83)	11.70 (11.14-12.27)
PH4	13.00 (12.71-13.30)	11.90 (11.38-12.42)	13.19 (12.88-13.52)
PH5	16.33 (15.86-16.88)	14.70 (14.32-15.11)	16.30 (15.90-16.76)
BREAST DEVELOPMENT			
B2	10.38 (10.11-10.65)	9.48 (9.14-9.76)	9.80 (0-11.78)
B3	11.75 (11.49-12.02)	10.79 (10.50-11.08)	11.43 (8.64-14.50)
B4	13.29 (12.97-13.61)	12.24 (11.87-12.61)	13.07 (12.79-13.36)
B5	15.47 (15.04-15.94)	13.92 (13.57-14.29)	14.70 (14.37-15.04)

Table 1. Median Ages at Entry into Each Maturity Stage and Fiducial Limits in Years for Pubic Hair and Breast Development in Girls by Race. Shumei S. Sun, *et al.*, *National Estimates of the Timing of Sexual Maturation and Racial Differences Among U.S. Children*, 110(5) PEDIATRICS 911-919 (2002).

[Table 2]

PUBIC HAIR	NON-HISPANIC WHITE	NON-HISPANIC BLACK	MEXICAN-AMERICAN
PH2	11.98 (11.69-12.29)	11.16 (10.89-11.43)	12.30 (12.06-12.56)
PH3	12.65 (12.37-12.95)	12.51 (12.26-12.77)	13.06 (12.79-13.36)
PH4	13.56 (13.27-13.86)	13.73 (13.49-13.99)	14.08 (13.83-14.32)
PH5	15.67 (15.30-16.05)	15.32 (14.99-15.67)	15.75 (15.46-16.03)
GENITALIA DEVELOPMENT			
G2	10.03 (9.61-10.40)	9.20 (8.62-9.64)	10.29 (9.94-10.60)
G3	12.32 (12.00-12.67)	11.78 (11.50-12.08)	12.53 (12.29-12.79)
G4	13.52 (13.22-13.83)	13.40 (13.15-13.66)	13.77 (13.51-14.03)
G5	16.01 (15.57-16.50)	15.00 (14.70-15.32)	15.76 (15.39-16.14)

Table 2. Median Ages at Entry into Each Maturity Stage and Fiducial Limits in Years for Pubic Hair and Genitalia Development in Boys by Race. Shumei S. Sun, *et al.*, *National Estimates of the Timing of Sexual Maturation and Racial Differences Among U.S. Children*, 110(5) PEDIATRICS 911-919 (2002).

[Table 3]

STUDY	FEMALES	MALES
	B2-B5 /PH2-PH5	G2-G5 /PH2-PH5
Roy (France) 1972	11.4-14.0 /11.3-13.2(PH4)	12.2-14.3(G4) /12.4-14.3(PH4)
Tarranger (Sweden) 1976	11.4-15.6 /11.5-15.2	12.2-15.1 /12.5-15.5
Largo & Prader (Switzerland) 1983	10.9-14.0 /10.4-14.0	11.2-14.7 /12.2-14.9
Villarreal (Mexico) 1989	10.9-15.1 /11.2-15.5	12.2-16.3 /12.8-16.1
Roede (Netherlands) 1990	10.5-14.2 /10.8-14.0	11.3-15.3 /11.7-14.9
Agarwal, Agarwal, Upadhyay, Mittal, Prakash, Rai (India) 1992	10.9-14.8 / NA	11.9-15.9 /NA
Dober & Kiralyfalvi (Hungary) 1993	10.0-16.4 /10.1-15.5	11.9-14.4 /11.8-14.6
Willers, Englehardt & Pelz (Germany) 1995/1996	10.8-15.7 /11.1-14.6	10.8-15.9 /11.4-15.6
Roche, Wellens, Attie & Siervogel (USA) 1995	11.2-12.4 (B4) /11.0-13.1	11.2-14.3 /11.2-14.3
Wacharasindhu, Pri-Ngam & Kongchonrak (Thailand) 2002	10.4-13.6 (B4) /11.9-13.5	11.3-13.2 /12.2-13.9

Table 3: Sexual maturation studies with median ages for females and males from various countries.

It is also critically important to note in regard to these studies (especially the recent Shumei study) that all stages below B5, PH5, and G5 are consistent with children well below the age of 18 years of almost all nationalities. For example, as shown in Tables 1 and 2 above, recent data from the United States illustrates that the median ages consistent with PH4 and G4 in non-Hispanic Black boys is 13.73 years and 13.40 years, respectively. Such demographic information may make it easier for a medical expert to opine as to whether an image is consistent with that of a child less than full adult maturation (*i.e.*, 18 years of age under federal law).

In sum, it is important to re-emphasize that Tanner staging is merely one of the various tools

that a medical expert will utilize in forming an opinion as to the age of a child depicted, and that the reliability of the expert's testimony should be based on other grounds as well. As the court stated in *Pollard*:

> It is manifest from Dr. Woodling's testimony that he did utilize the Tanner scale in helping to formulate his expert opinion, but that was only one of a number of factors he took into account when reaching his expert opinion. Dr. Woodling testified that he had treated thousands of young girls and young women, he is a qualified forensic examining physician, and he has worked and written extensively in the area of sexual abuse of children. The United States Supreme Court ruled in *Daubert* that in order for expert testimony to be admissible at trial, it must be both relevant and reliable. The "reliability" of the proposed expert testimony was addressed by the Supreme Court by requiring that the expert be properly qualified and possess valid scientific and/or technical knowledge. It is the opinion of the undersigned that the qualifications and the reliability of Dr. Woodling's testimony has been properly established, and his testimony is properly reliable to be introduced into evidence pursuant to Rule 702, Federal Rules of Evidence.

Pollard at 1123-24.

V. Proving that a child depicted is real

The Supreme Court's decision in *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002), made clear that the government must prove beyond a reasonable doubt that the image depicts a "real" child. There had been much discussion regarding the methods by which the government can meet this burden, particularly given the prospect that defendants could allege that an image might be of a "virtual" child, created out of whole cloth by digital imaging software and indistinguishable from a real child, despite the fact that no such image has ever been seen to date. The methods that prosecutors can use to prove that a child is real are discussed in a separate article in this issue. In conjunction with these methods, testimony from a pediatrician may be helpful.

Testimony from a medical expert can be potentially helpful in establishing that the images in question are of real children by eliminating defense-posited hypotheticals, such as the proposition that the images at issue might be composite images prepared with adult pornography. For example, in *United States v. Nolan,* 818 F.2d 1015 (1st Cir. 1987), the First Circuit held that the government was not required to present expert testimony from a photography expert to negate speculation by the defense that the charged images may have been "doctored" or prepared from composites. The court also noted that during the direct examination of the pediatrician, the following exchange took place, which would also help negate such speculation:

> Q[:] And why do you conclude that, Doctor? People can doctor photographs. People can alter photographs. Why do you conclude that these are not altered photographs or perhaps composites of adult genitalia, let's say, with children's torsos and arms and legs and heads?
>
> A[:] Well, I think that that kind of conglomeration of parts, body parts, would be very bizarre appearing, because of the differences in size, texture. The gestalt would be wrong; in other words, the total picture would not be of a normal human being, most likely.

Id. at 1019; *see also United States v. Bender*, 290 F.3d 1279, 1282 (11th Cir. 2002) (pediatrician testified that "photographs appeared to portray real children"); *United States v. Vig*, 167 F.3d 443, 449-50 (8th Cir. 1999) (jury could infer from images and pediatrician's testimony that children depicted were real). *Nolan* therefore suggests that pediatricians, if called to testify about the ages of children depicted, can help the government rebut *unsubstantiated* claims of computer-generated or composite images.

VI. Conclusion

In appropriate cases, the forensic medical expert can greatly enhance the investigation and prosecution of child pornography cases. The expert's knowledge of childhood growth and development can significantly augment the skill of those who analyze images to determine if they are consistent with children younger than a certain age. Furthermore, the forensic medical practitioner can provide important expert witness assistance with regard to whether real children are depicted in the images at issue in child pornography prosecutions.❖

ABOUT THE AUTHORS

❑**Dr. Sharon W. Cooper** is a Forensic and Developmental Pediatrician and an Associate Professor of Pediatrics at the University of North Carolina's School of Medicine in Chapel Hill, North Carolina. She has testified as an expert witness in more than 150 cases in federal, state,

and military courts, in matters involving child physical abuse, sexual abuse, and exploitation.

❑**Damon King** is a Trial Attorney in the Child Exploitation and Obscenity Section. Mr. King joined the Section in 2001 after serving for seven years as a prosecutor in the U.S. Army JAG Corps. For six of those years, he was a Special Assistant United States Attorney in the Eastern District of Virginia.✠

Request for Subscription Update

In an effort to provide the UNITED STATES ATTORNEYS' BULLETIN to all who wish to receive it, we are requesting that you e-mail Nancy Bowman (nancy.bowman@usdoj.gov) with the following information: Name, title, complete address, telephone number, number of copies desired, and e-mail address. If there is more than one person in your office receiving the BULLETIN, we ask that you have one receiving contact and make distribution within your organization. If you do not have access to e-mail, please call 803-576-7659. Your cooperation is appreciated.