Sexual Exploitation Crimes Against Children

In This Issue

September 2011
Volume 59
Number 5

United States
Department of Justice
Executive Office for
United States Attorneys
Washington, DC
20530

H. Marshall Jarrett
Director

Contributors' opinions and statements should not be considered an endorsement by EOUSA for any policy, program, or service.

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

The United States Attorneys' Bulletin is published bimonthly by the Executive Office for United States Attorneys, Office of Legal Education, 1620 Pendleton Street, Columbia, South Carolina 29201.

Managing Editor
Jim Donovan

Law Clerk
Carmel Matin

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

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

Introduction to the Sexual Exploitation Crimes Against Children Issue of the USA Bulletin 1
By Paul R. Almanza

Meeting the Government's Discovery Obligations in Child Exploitation Cases 3
By Jeffrey Zeeman

Getting Your Evidence into Evidence in a Digital World 14
By Damon King and Meredith Owen

Understanding Probable Cause and Overcoming Staleness Issues in Child Pornography Cases 27
By Chantel Febus, Jason Claude, and Kimberly Singer

SORNA: A Primer 42
By Bonnie Kane

Social Networking Sites: Breeding Grounds for "Sextortion" Prosecutions 54
By Darcy Katzin, Mi Yung Park, and Keith Becker

Emerging Issues in the Extraterritorial Sexual Exploitation of Children . 59
By Anitha S. Ibrahim, Ed McAndrew, and Wendy Waldron

Units of Prosecution in Child Pornography Cases and Rebutting the Argument that Possession of Child Pornography is a Lesser Included Offense of Receipt 68
By Andrew McCormack

Beyond the Child Pornography Sentencing Guidelines: Strategies for Success at Sentencing 76
By Alexandra R. Gelber

The Fallacy of Simple Possession: The Impact of Targeting, Charging, and Plea Bargaining at Sentencing 86
By Drew Oosterbaan

Introduction to the Sexual Exploitation Crimes Against Children Issue of the USABulletin

Paul R. Almanza
Deputy Chief
Child Exploitation and Obscenity Section

In the five years since the Child Exploitation and Obscenity Section (CEOS) last prepared an issue of the U.S. Attorney's Bulletin, there have been many changes in how offenders commit these crimes and in how the federal law enforcement community has responded. There have also been changes in the legal landscape, most notably the increasing extent to which judges are imposing sentences below the ranges established by the existing child pornography sentencing guidelines. This issue of the Bulletin reflects and responds to many of these changes and is intended as a guide and resource for federal child exploitation prosecutors in their continuing work to hold child sexual offenders accountable for their actions.

As the continuing evolution of the Internet has made it so much easier for legitimate users to exchange ideas and information with each other, so too has it greatly expanded opportunities for offenders to find and distribute child sexual abuse images and to share with each other their mutual interest in sexually exploiting children. These developments have led to a pandemic of child exploitation crimes, ranging from those committed by relatively unsophisticated offenders, such as those using only Peer-to-Peer technologies to receive and to distribute child pornography, to those committed by extremely sophisticated offenders, such as those who use complex technologies such as encryption and anonymizers to commit child exploitation offenses in concert with one another as part of international online groups dedicated to child exploitation.

Federal law enforcement has responded to these developments by increasing its coordination with state, local, tribal, and international law enforcement, and by developing investigative strategies that keep abreast of the increasing sophistication shown by offenders. Federal prosecutors have taken a lead role in coordinating these efforts through the Department's Project Safe Childhood (PSC), which began as an effort to address technology-facilitated child sexual exploitation crimes but was expanded this year to cover all federal child sexual exploitation crimes, including offenses such as the prostitution of children here in the United States. PSC has achieved a great deal since its launch in 2006, and we at CEOS look forward to working with all of our PSC partners to continue the fight against child sexual exploitation.

Despite the success of PSC, there has been growing criticism of the existing child pornography sentencing guidelines, which are deemed by some judges to be flawed and unhelpful in determining the appropriate sentences for child pornography defendants, especially those convicted of child pornography trafficking and possession offenses. Prosecutors need to adapt their sentencing strategy to better demonstrate in court the seriousness of these crimes and the risk these defendants pose to society, and to persuade skeptics, who may be judges or interested members of the public, that these offenses merit appropriate punishment. Two articles, discussed in more detail below, provide guidance to federal

prosecutors on exactly how to do that during the entire prosecution of a case, as well as during the presentation of the government's sentencing case.

Overall, the articles in this issue of the Bulletin cover three general topics:

- Four articles cover legal issues that federal prosecutors should be aware of as they handle individual cases. These articles discuss topics such as meeting the government's discovery obligations in child pornography cases, admitting electronic communications, probable cause and overcoming staleness arguments in child pornography cases, and information prosecutors should know concerning the Sex Offender Registration and Notification Act.
- Two articles deal with new developments. One covers offenders' increasing use of social networking sites to commit sextortion, while the other examines emerging issues in the extraterritorial sexual exploitation of children, otherwise known as child sex tourism, through three case studies.
- Three articles provide guidance on fundamental prosecutorial functions such as deciding what to charge and presenting the best case possible from the government's perspective. The first examines the proper units of prosecution in child pornography cases, which will assist federal prosecutors as they draft charging documents. The second, briefly mentioned above, provides prosecutors with a roadmap for an effective sentencing presentation that goes beyond the sentencing guidelines. The third, also briefly mentioned above, explodes the notion that there ever could be a true "simple possession" case, and asks prosecutors to base their decisions on how to handle a case upon evidence demonstrating the full extent of the offenders' conduct and to ensure that the court is aware at sentencing of the seriousness of the offense and the risk posed by the offender.

The recent expansion of Project Safe Childhood to cover all federal child exploitation offenses and the development of the National Strategy for Child Exploitation Prevention and Interdiction underscore the Department's continuing commitment to protecting our children from sexual offenders. This issue of the Bulletin, which I have had the privilege of editing, will help further that commitment by giving federal prosecutors additional information that will help them more effectively prosecute child exploitation cases.

Paul R. Almanza
Deputy Chief
Child Exploitation and Obscenity Section

Meeting the Government's Discovery Obligations in Child Exploitation Cases

Jeffrey Zeeman
Trial Attorney
Child Exploitation and Obscenity Section

I. Introduction

Prior to passage of the Adam Walsh Child Protection and Safety Act of 2006 (the Act), 42 U.S.C. §§ 16901–16991 (2006), Federal Rule of Criminal Procedure 16(a)(1)(E) governed, without statutory qualification, the production of evidence in child pornography cases. Although Rule 16 contains no provisions tailored to the discovery of child pornography, most courts, cognizant of the potential harm to victims from redistribution of pornographic materials, permitted the Government to provide the defense with access to such evidence in lieu of providing the defense with its own copy of the materials. The Act codified this principle in 18 U.S.C. § 3509(m) by explicitly prohibiting the Government from providing copies of evidence of child pornography so long as that evidence is made "reasonably available" to the defense.

The defense bar has repeatedly challenged the Act on constitutional grounds, but none of those challenges have proven successful. Two courts, however, did mandate Government production of evidence on the grounds that the Government had failed to make that evidence "reasonably available" as required by statute. This article discusses the courts' opinions in more detail by reviewing the factual and legal analysis of the two cases, *United States v. Knellinger*, 471 F. Supp. 2d 640 (E.D. Va. 2007) and *United States v. Winslow*, No. 3:07-CR-00072-TMB-DMS (D. Alaska Jan. 28, 2008), *available at* http://www.fd.org/pdf_lib/Discovery_AW_Winslow_Unconstitutional.pdf. *See infra* Part IV.A–B. Since the issuance of those decisions, the defense bar has consistently cited these cases as persuasive authority during subsequent attempts to obtain copies of child pornography evidence. Those attempts have generally proven to be unsuccessful because those isolated adverse holdings each concerned very narrow circumstances. *Knellinger* dealt with reliance by defense experts on specialized, highly technical analysis particular to the "virtual child" defense; and *Winslow* concerned unduly restrictive conditions imposed by the Government during on-site examination by the defense forensic expert. Prosecutors should be prepared to rebut a defense argument grounded in these decisions by emphasizing the narrowness of their holdings and the far broader array of decisions rejecting defense requests for production of copies of child pornography evidence.

Some defendants have requested that, in the alternative, prosecutors create and produce in discovery a mirror image copy, scrubbed of all contraband images, of all hard drives or other storage devices containing child pornography. Defendants have argued that such production would allow unfettered access to probative evidence without violating the Act. It is nearly impossible, however, for the Government to ever be completely certain that it has successfully eliminated all contraband child pornography from a hard drive. Moreover, the costs of even attempting to do so would be prohibitive, while the benefits to the defense of obtaining electronic information divorced from the context of the

charged child pornography images and videos would be minimal. Accordingly, prosecutors should instead insist that defendants view all electronic storage media containing contraband child pornography in a secure government facility.

II. Federal Rule of Criminal Procedure 16

> Rule 16(a)(1)(E) provides, in relevant part:
>
> [T]he government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any [one] of these items, if the item is within the government's possession, custody or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant.

FED. R. CRIM. P. 16(a)(1)(E).

Rule 16 does not, as some defense counsel contend, compel the Government to employ its resources to copy or otherwise supply criminal defendants with material in the Government's possession. *See United States v. Freedman*, 688 F.2d 1364, 1366 (11th Cir. 1982). Rule 16 merely requires the Government to "*disclose* to the defendant, and make *available* for inspection, copying, or photographing" the items listed in Rule 16(a)(1)(B). *See United States v. Tyree*, 236 F.R.D. 242, 244 (E.D. Pa. 2006) (emphasis added). In other words, Rule 16 provides a defendant access to documents and items so that he may inspect and copy them but does not require the Government to conduct the inspecting and copying for the defendant. *See, e.g.*, *United States v. Jordan*, 316 F.3d 1215, 1249 (11th Cir. 2003) (holding that even if there is a request by the defendant to make copies of discovery materials, the Government is not obligated to make copies of the items); *Freedman*, 688 F.2d at 1366-67 (holding that the district court abused its discretion by ordering the Government to copy and pay the costs of reproduction of discoverable documents); *United States v. Gleason*, 616 F.2d 2, 25 (2d Cir. 1979) ("With respect to such material, if any obligation to disclose existed under Rule 16(a), it was satisfied by making the underlying files available to the defendant prior to trial."); *Tyree*, 236 F.R.D. at 244 ("[A] fair examination of the four corners of [Rule 16] reveals no affirmative duty on the Government to *pay* for copying . . . its only duty is to make documents 'available for inspection, copying or photographing' or to allow the defense 'to inspect and to copy or photograph' documents and things.") (emphasis in original). Accordingly, unless the defendant is indigent or has been prohibited from inspecting the particular documents, defendants should not be permitted to transfer the cost of discovery requests to the Government. *See Freedman*, 688 F.2d at 1366-67; *United States v. Green*, 144 F.R.D. 631, 637-38 (W.D.N.Y. 1992).

III. Discovery in child pornography cases prior to enactment of the Act

Prior to the 2006 passage of the Act, no statute expressly addressed child pornography and discovery. Nevertheless, in child pornography cases, most courts denied defendants' motions to compel the Government to provide copies of child pornography images in discovery. *See, e.g.*, *United States v. Horn*, 187 F.3d 781, 792 (8th Cir. 1999) (upholding denial of discovery under Rule 16 because the tapes requested were prima facie contraband); *United States v. Kimbrough*, 69 F.3d 723, 731 (5th Cir. 1995) (where Government's offer to make the child pornography materials available for inspection but not to allow them to be copied was reasonable under Rule 16); *United States v. Husband*, 246 F. Supp. 2d 467, 468-69 (E.D. Va. 2003) (where Government's offer to make videotape available for inspection and its refusal to copy the videotape did not violate Rule 16); *United States v. Cox*, 190 F. Supp. 2d 330, 334 (N.D.N.Y. 2002) (denying defendant's motion where he provided no factual basis for asserting that, to

adequately prepare his defense, physical possession of the Government's evidence was necessary). In denying defendants' discovery motions filed prior to the Act's enactment, courts typically emphasized that computer files that were or contained child pornography: (1) are illegal contraband; (2) can easily be duplicated and transmitted by individuals who possess them; and (3) are "a permanent record of a child's abuse [whose] continued circulation itself would harm the child who had participated. Like a defamatory statement, each new publication . . . would cause new injury to the child's reputation and emotional well-being." *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 249 (2002).

A minority of courts, however, adopted a contrary view that the risk of loss or unlawful duplication and distribution of child pornography images produced in discovery may be mitigated by the court issuing a protective order. These courts asserted that such risks were outweighed by a defendant's claim that his counsel or expert needed to have actual possession of the materials outside of Government custody in order to adequately prepare for trial. *See, e.g.*, *United States v. Cadet*, 423 F. Supp. 2d 1, 4 (E.D.N.Y. 2006) ("There is a much greater likelihood that the Defendant would be harmed in his inability to prepare a defense by limited access to the materials than there is that the materials will be further distributed by the defense . . . ."); *United States v. Fabrizio*, 341 F. Supp. 2d 47, 51 (D. Mass. 2004) (where defendant was entitled to obtain copies of images seized from his computer to enable his counsel to investigate how images appeared and were accessed on his computer); *United States v. Hill*, 322 F. Supp. 2d 1081, 1091-92 (C.D. Cal. 2004).

IV. Discovery conflicts subsequent to the passage of the Act

To codify the procedure followed in the *Horn* and *Kimbrough* cases, Congress passed the Act that was signed into law on July 27, 2006. *See* Pub. L. No. 109-248, § 504, 120 Stat. 587, 629 (July 27, 2006). Section 3509(m) of the Act, "Prohibition on reproduction of child pornography," codified procedures with respect to the disclosure of child pornography materials and provides in relevant part:

> (1) in any criminal proceeding, any property or material that constitutes child pornography (as defined by section 2256 of this title) shall remain in the care, custody, and control of either the Government or the court.
>
> (2)(A) Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography (as defined by section 2256 of this title), so long as the Government makes the property or material reasonably available to the defendant.
>
> (B) For the purposes of subparagraph (A), property or material shall be deemed to be reasonably available to the defendant if the Government provides *ample opportunity for inspection, viewing, and examination at a Government facility of the property or material* by the defendant, his or her attorney, and any individual the defendant may seek to qualify to furnish expert testimony at trial.

Pub. L. No. 109-248, § 504 (emphasis added).

This provision was enacted to accomplish the congressional goal of "protecting children from repeat exploitation in child pornography." *Id.* § 501(2); *see also* § 501(1)(B). Prosecutors should be aware that if the expert is not an employee of the Government, § 3509(m) applies to prosecution expert witnesses as well. *United States v. Shrake*, 515 F.3d 743, 746 (7th Cir. 2008) (cautioning that provision by the Government of contraband images to a private consultant testifying on the Government's behalf violated the terms of the Act).

Since the enactment of the Act in 2006, many defendants have challenged the constitutionality of § 3509(m). Courts across the country addressing these challenges, however, have consistently held that the Act comports with due process and is constitutional in light of the Act's "safety valve" provision. This provision ensures that child pornography material be made "reasonably available" to the defendant by requiring the Government to "provide[] ample opportunity for inspection, viewing, and examination at a Government facility . . . ." 18 U.S.C. § 3509(m)(2)(B) (2010). *See United States v. Spivack*, 528 F. Supp. 2d 103, 106 (E.D.N.Y. 2007) (listing cases).

Notwithstanding the myriad of decisions rejecting facial constitutional challenges to the Act, some defendants have challenged the statute "as-applied" to their particular cases. In these cases, the defendant typically claims that the Government failed to provide an "ample opportunity" to inspect, view, and examine the material at a government facility as required by § 3509(m). Courts have likewise consistently rejected these as-applied challenges. *See, e.g.*, *United States v. Wright*, 625 F.3d 583, 616 (9th Cir. 2010) (Act does not require Government and defendant to have equal access to child pornography evidence so long as defendant has ample opportunity to examine the evidence); *United States v. Shrake*, 515 F.3d 743, 746 (7th Cir. 2008) (affirming district court's denial of defendant's request for production of hard drive mirror image); *United States v. Hornback*, 2010 WL 4628944, at *2 (E.D. Ky. Nov. 8, 2010) (lack of a simultaneous Internet connection while examining contraband does not amount to a denial of an "ample opportunity"); *United States v. Doane*, 501 F. Supp. 2d 897, 901-02 (E.D. Ky. 2007) (requiring defense expert to examine computer hard drive at government facility would provide defendant with ample opportunity for inspection); *United States v. Sturm*, 2007 WL 1453108, at *8 (D. Colo. May 17, 2007) (Act precluded defendant from receiving bit-by-bit copies of computer-generated media containing evidence that the Government intended to introduce at trial); *United States v. Renshaw*, 2007 WL 710239, at *1 (S.D. Ohio Mar. 6, 2007) (rejecting defendant's argument that § 3509(m) permits the Government to bypass its burden to authenticate evidence).

The only exceptions to this widespread rejection of defense challenges to the Act are two anomalous decisions. Both decisions ground their reasoning in purported violations by the Government of the statutory requirements rather than holding the Act itself unconstitutional. These two cases, *United States v. Knellinger*, 471 F. Supp. 2d 640 (E.D. Va. 2007) and *United States v. Winslow*, No. 3:07-CR-0072-TMB-DMS (D. Alaska Jan. 28, 2008) (order granting defense motion to compel), are prominently featured on www.fd.org, the Federal Office of Defender Services' training Web site, and have been and will continue to be frequently cited by defense counsel. Prosecutors may counter that *Knellinger* and *Winslow* are both outliers that differ from the vast majority of cases interpreting the Act and that, in all events, the facts of both are readily distinguishable from most discovery conflicts.

A. *United States v. Knellinger*

In *Knellinger*, the defendant requested production of a mirror image of his computer hard drive, claiming that he was constitutionally entitled to copies of the child pornography that would be presented as evidence against him. Defendant argued that his intended "virtual child" defense at trial required determination of whether the children depicted were real and that this analysis could not feasibly be performed at a government facility. In support of this assertion, defendant primarily relied on the testimony of two digital video experts who each testified that inspection at a government facility would be unduly expensive and would greatly hamper their ability to perform the required analysis to the point that they would not accept the job. Based on this testimony, the district court concluded that the practical effect of § 3509(m) was to prevent defendant from conducting the "real or virtual child" analysis required for his defense. *Knellinger*, 471 F. Supp. 2d at 649-50. Consequently, the court ordered that copies of the hard drive be produced to defense counsel subject to a protective order. *See id.*

Critically, the *Knellinger* court did not adopt defendant's arguments that the Act violated the Rules Enabling Act and rejected all of the defendant's various claims that the provision was unconstitutional on its face. *Id.* at 644-45. On the contrary, the court concluded that if "ample opportunity" for inspection is, as required by statute, provided to the defendant, his constitutional rights will, by definition, be protected. *Id.* at 646. The court therefore grounded its holding in its view that the Government failed to provide the defendant with the ample opportunity for inspection explicitly afforded by the Act rather than in any constitutional concern. *See id.*

During the evidentiary hearing in *Knellinger*, James Griffin, a defense expert in the field of audio and video forensics, claimed that he required on-site access to a computer with software, video cards, video playback decks, waveform monitors, a vectrascope, an audio spectrum analyzer, and high resolution computer and video monitors. Because of the significant costs incurred in the transportation of this specialized equipment, coupled with the interruption to his business during the travel period, Griffin asserted that he would decline Knellinger's request for forensic services if he had to perform his work at a government facility.

Once provided a mirror image copy of the hard drive, however, it appears that Griffin did not carry out the type of sophisticated analysis he claimed he needed to perform at his own facility. According to the expert report provided by Knellinger to the United States, Griffin spent a mere three days on the project and analyzed only nineteen of the thirty-two files located on the computer hard drive. JAMES A. GRIFFIN, REPORT ON COMPUTER VIDEO IMAGE FILES, *In the matter of United States v. Knellinger* (2007). Furthermore, according to his report, Griffin utilized only a computer with software programs, studio quality speakers, video playback decks, and high resolution video monitors to complete his analysis. Nothing in his expert report references any of the equipment or techniques he described at the prior hearing.

At the evidentiary hearing, the defendant presented a second expert witness, Tom Owen, who specialized in audio, video, and digital forensic analysis. Owen testified that his forensic services would quadruple in cost to $545,000 if he was forced to conduct his examination at a government facility. Defendant, however, never hired Owens to perform the purportedly required analysis, even though the court relied on his testimony in arriving at its decision.

In short, because Griffin's testimony before the District Court was ultimately inconsistent with the forensic analysis he later conducted and Owen was never hired by the defendant, the *Knellinger* court based its ruling on what became inaccurate or irrelevant facts. Because Knellinger pled guilty, the Government had no opportunity to revisit the issue and correct the record. *Knellinger*, therefore, is of limited value as persuasive authority and, in all events, is relevant only in extraordinarily narrow circumstances. In order for this case to provide authority, a defendant must: (1) be relying on the "virtual child" defense; (2) present credible evidence that the logistical problem of safely transporting equipment is prohibitively expensive and prevents experts from being able to perform work necessary to the defense; and (3) demonstrate that government-provided equipment is insufficient to satisfy the requirements of the forensic experts. Moreover, the *Knellinger* decision is actually very helpful to the Government in one respect: the court made its ruling only after conducting a full hearing involving the presentation of two purported defense experts. Therefore, a mere claim by a defendant that he was denied ample opportunity to examine the child pornography evidence, without substantial evidentiary support, is not a sufficient basis for a court order to provide the defense with its own copy of contraband materials.

Furthermore, the defense experts' about-face in *Knellinger* teaches that, to the extent any future court signals an interest in adopting the *Knellinger* court's logic, prosecutors should press the court to be certain that defense experts truly intend to perform the analysis they claim is necessary. For example,

prosecutors could request a proffer that defense experts in prior cases have actually used the sophisticated technology they claim is crucial to the task at hand and that forensic analysis would be impossible or prohibitively expensive to conduct on-site. Anything less than satisfying this request risks a replay of *Knellinger*'s troubling result, where the Act's goal of protecting victims from additional harm is undermined without any potential to assist the defense.

B. *United States v. Winslow*

In *United States v. Winslow*, No. 3:07-CR-0072-TMB-DMS (D. Alaska Jan. 28, 2008), the Government seized defendant's hard drive containing child pornography images and evidence of on-line chats and emails between Winslow and an undercover officer. Defendant requested that the Government produce, pursuant to a detailed protective order utilized prior to the Act, a mirror image of his hard drive. In support of this request, defendant relied on forensic investigator Marcus Lawson's testimony at an evidentiary hearing. He also relied on copies of affidavits, originally appended to the search warrant application, from government agents discussing the need for a substantial and thorough review of data on a hard drive in a controlled environment. Lawson listed the following concerns to support his need for a mirror image of the hard drive: (1) hour limitations in government buildings lead to inadequate preparation time; (2) limited privacy due to presence of government agents in the forensic lab; (3) no access to phone lines or the Internet; (4) transit-related damage to the expert's equipment; and (5) the inability during trial to access the computer images to run tests and check data. *Id.* at 6-7.

The magistrate employed a similar approach to the *Knellinger* court by rejecting both the facial and as-applied constitutional challenges advanced by defendant, while stressing that the "ample opportunity" language contained in the Act was sufficient to protect defendant's rights. *Id.* at 17. The magistrate emphasized that, in light of the court's responsibility to construe a statute to avoid a ruling of unconstitutionality, "the term 'ample opportunity' [] must be read to at least include the same opportunity for inspection, viewing, and examination that is required by the Fifth and Sixth Amendments of the Constitution." *Id.* at 18. The magistrate concluded that "[t]he Government's requirement that the discovery room remain under surveillance by closed circuit television, with the promise that the camera will not be trained on the computer monitor, [did] not provide 'ample opportunity' to conduct discovery as required by the Constitution" because such surveillance may "intrude upon the attorney work product privilege in meaningful ways." *Id.* at 21. The magistrate further held that the defense experts were impermissibly hampered by the Government's refusal to make phone lines and Internet access available. *Id.* at 22. *Compare id.* at 21-22, *with United States v. Harvey*, 3:07-CR-00103-RRB-DMS (D. Alaska Jan. 6, 2008), Docket No. 104 (private room with 24-hour access, including phone and Internet access, with a government agent posted outside the room, provided ample opportunity to examine discovery materials).

The magistrate voiced no objection to the general practice of requiring defendants to examine evidence at a government facility, nor did she opine that the Act was unconstitutional on its face or as-applied. Rather, the magistrate held only that the purportedly intrusive restrictions imposed by the Government effectively denied the defendant ample opportunity for discovery. Accordingly, defense counsel cannot credibly cite the *Winslow* opinion as persuasive authority for any proposition beyond its narrow holding that the Government should provide phone and Internet access to defense experts and should not closely monitor those experts via closed-circuit cameras during the course of their forensic analysis. Thus, *Winslow* is even more narrow in scope than *Knellinger*.

C. The reasonable availability standard after *Knellinger*

Courts have consistently rejected allegations by defendants, often relying on *Knellinger*, that general problems of higher costs and/or inconvenience to experts violate the reasonable availability requirement of § 3509(m)(2)(B). Indeed, in rejecting *Knellinger*'s holding, one court went so far as to comment that "*Knellinger* sets a template for indirect repeal of § 3509(m)" by allowing defense counsel to manipulate the statute "by merely positing [non case-specific] conceptual difficulties to be encountered at government facilities, or mere preferences to use their own." *United States v. Flinn*, 521 F. Supp. 2d 1097, 1102 (E.D. Cal. 2007).

Many other courts have refrained from direct critique of the holding in *Knellinger* and instead distinguish it on factual grounds. For example, in *United States v. Spivack*, 528 F. Supp. 2d 103, 104 (E.D.N.Y. 2007), a defendant charged with transporting child pornography by means of a computer and possession of child pornography sought production of a mirror image of the hard drive seized from his computer. The court refused to mandate the requested production because, unlike Knellinger, Spivack failed to raise the "virtual child" defense. He also failed to raise any factual issue regarding the Government's compliance with the reasonable availability requirement. The court rejected defendant's general argument that "the problems are those of time, equipment and unfettered access" because the record lacked specific factual support for those claims. *Id.* at 107.

Similarly, in *United States v. Battaglia*, 2007 WL 1831108, at *4-6 (N.D. Ohio June 25, 2007), the defendant relied on *Knellinger* and argued that his defense experts were not provided an "ample opportunity" to examine his computer hard drive. In support of this contention, defendant presented a letter from a prospective expert describing the costliness of on-site analysis and argued that "the process of reviewing the material at the government facility is cumbersome, requires multiple trips back and forth, permits viewing only during business hours, and is generally uncomfortable because it is done in the presence of counsel for the government." *Id.* at *6. The court rejected these arguments, holding that increased discovery costs were an obvious result of passage of the Act and that general inconvenience and extra costs for defense counsel did not deprive him of an "ample opportunity" to examine discovery materials. *Id.*

In *United States v. O'Rourke*, 470 F. Supp. 2d 1049, 1058 (D. Ariz. 2007), the defendant, charged with possession, receipt, and transportation of child pornography, argued that the conditions offered by the Government "made it virtually impossible for the Defendant's forensic experts to analyze the hard drive containing the images." *Id.* at 1057. Specifically, the defendant asserted that the forensic experts needed private access to the Internet that was not available at the Government's office and that the copy of the hard drive provided by the Government contained "malware" that prevented the experts from gathering necessary data from the hard drive. The court concluded that the two problems identified by the defendant did not amount to "a denial of due process or of an ample opportunity to inspect the hard drive" but rather an easily remedied "communication" problem. *Id.* at 1058.

Other courts have also rejected defense arguments grounded in *Knellinger*. *See United States v. Wright*, 625 F.3d 583, 615-16 (9th Cir. 2010) (*Knellinger* was "easily distinguishable" where defense expert had fourteen months to access forensic evidence); *United States v. Hornback*, 2010 WL 4628944, at *2 (E.D. Ky. Nov. 8, 2010) (unlike *Knellinger*, no evidence presented that costs of analysis at a government facility would be so high as to make analysis infeasible); *United States v. Patt*, 2008 WL 2915433, at *20 (W.D.N.Y. July 24, 2008) (*Knellinger* inapplicable where defense expert provided ample opportunity for inspection of hard drives allowing him to complete his analysis despite inefficiencies and inconveniences resulting from requirement to utilize government facility). *See also United States v. Donatos Sarras*, 2007 WL 3231797, at *4 (M.D. Fla. Oct. 30, 2007) (holding that the

purportedly unreasonable expense of private examinations at a government facility is insufficient to override the clear statutory prohibition of production of mirror image hard drives containing child pornography); *United States v. Tyson*, 2007 WL 2859746, at *3 (W.D.N.Y. Sept. 26, 2007) (defendant had not demonstrated that the Government failed to provide defense counsel with "ample opportunity" for the inspection of material at a government facility); *United States v. Doane*, 501 F. Supp. 2d 897, 901-02 (E.D. Ky. 2007) (rejecting defendant's argument that the time and expense required for expert travel to the government facility; the lack of privacy and confidentiality for the expert at that facility; the unavailability of the forensic computer equipment needed to conduct the proper examination; and concerns about interruptions during the analysis process prohibited defendant from having an ample opportunity for inspection of contraband materials); *United States v. Butts*, 2006 WL 3613364, at *2 (D. Ariz. Dec. 6, 2006) ("When determining whether material is reasonably available to a defendant, the applicable standard does not consider expense or location as relevant factors."); *United States v. Johnson*, 456 F. Supp. 2d 1016, 1020 (N.D. Iowa 2006) ("In enacting § 3509(m), Congress has presumably balanced the public interest in prohibiting the dissemination of child pornography used in criminal trials with the public interest in reducing the costs of expert services for the indigent . . . . It is not the province of this court to strike a different balance."); and *United States v. Burkhart*, 2006 WL 2432919, at *1 (W.D. Pa. Aug. 21, 2006) ("[T]he relevant standard does not consider expense or location of the expert as factors to consider when determining whether the material is reasonably available to a defendant.").

Practically speaking, prosecutors should keep in mind that although § 3509(m) furthers the Government's interest in protecting against dissemination of evidence of child pornography, it is not foolproof. Defense experts could, either intentionally or inadvertently, copy contraband onto equipment they bring into a government facility. Accordingly, even if forensic analysis is conducted wholly on-site, it is advisable for prosecutors to, at a minimum, request a protective order directed towards preventing any copying of contraband evidence by defense experts. As an additional (albeit imperfect) security measure, government agents can, prior to departure, scan defense experts' electronic equipment to ascertain whether any contraband materials have been copied onto such equipment. Some courts, however, view this type of precaution as an unreasonable restriction on the defendant's ability to prepare a defense. *See, e.g.*, *United States v. Bortnick*, 2010 WL 935842, at *3 (D. Kan. Mar. 11, 2010) (evidence is not "reasonably available" if defense expert is subject to search of his electronic materials when he leaves government facility; instead, defense expert should certify in writing that he has not taken any child pornography materials or caused them to be sent off-site).

V. Rebutting defense requests for scrubbed mirror image discovery

Defendants' inability to procure, following passage of the Act, mirror images of seized computer hard drives containing child pornography has inspired a new defense strategy: requesting the production of "sanitized" copies of seized hard drives. In other words, defendants request a mirror copy of all contents of the drive scrubbed of contraband materials. As explained in more detail below, production of such sanitized copies: (1) is not technically feasible and, at best, is unduly burdensome; (2) may easily result in inadvertent production of contraband images; and (3) fails to provide substantial forensic value to defense examiners.

Before they can delete all suspected images of child pornography from a seized hard drive, forensic examiners first need to locate all images on that hard drive. Unfortunately, no single extant tool can successfully identify all images stored on a computer. Instead, examiners must analyze each individual file on the hard drive—a time and resource-intensive undertaking that is subject to human error. Even searching all of the specific file formats that usually contain visual files, such as ".jpg" files, would not uncover all of the images stored on a computer because image file types are continuously

evolving and these file extensions may easily be changed by someone attempting to mask a file's true contents. Similarly, child pornographers can easily embed visual images within other files, such as a PDF, an Excel Spreadsheet, or a Microsoft Word document. Accordingly, to comply with the Act, even seemingly innocuous files must be examined to determine whether they contain child pornography. Moreover, although hitting the computer's delete key and emptying its recycle bin removes images from the user's sight, those images remain in the hard drive's unallocated space (also known as slack space) until they are overwritten. Searching for images in unallocated space is a particularly difficult and time consuming process. Furthermore, in some cases, forensic examiners may be unable to access encrypted child pornography files on a hard drive, whereas defendants may possess information that would unlock that encryption.

This onerous process of compiling images is only a first step. The forensic examiner would next be required to analyze each individual image to determine whether it is in fact child pornography rather than adult pornography or some other non-contraband image. As hard drives often contain tens or even hundreds of thousands of image files, this additional step would require even more substantial time and technological resources. Committing a single forensic examiner to such a project would place an enormous and undue burden on government resources. More importantly, despite its best efforts, the Government would be unable to guarantee the deletion of all contraband materials from a seized hard drive. Child pornography images and videos embedded within seemingly innocuous files or located in unallocated space may well remain on the computer notwithstanding a diligent search of these locations by an expert forensic examiner.

The substantial costs of attempting to create a sanitized hard drive for production far outweigh the minimal benefits to the defense from such a production. Indeed, removal of the contraband from the hard drive would effectively alter what is likely to be the evidence most material to the defense by divorcing the images from their context and preventing the expert from accessing file data, such as the file's origin or upload date, necessary to support commonly employed defenses (for example, where defendant asserts he did not knowingly receive the child pornography).

In the limited volume of cases addressing this issue, at least one court has treated with skepticism defense claims that the Government can easily and effectively produce sanitized hard drives. In recognizing the complexity inherent in attempting to create a sanitized hard drive, the court in *United States v. Flinn*, 521 F. Supp. 2d 1097, 1099 (E.D. Cal. 2007), noted that "[e]vidently, a computer's hard drive has more hidden nooks and crannies than the Winchester Mystery House. . . . [a]nd child pornography, once placed on a hard drive, can infiltrate those nooks and crannies even without the conscious knowledge of a computer operator." In *United States v. Kramer*, No. 5:07CR50027-001 (W.D. Ark. Jan. 15, 2008), a defense expert claimed that a software program called "Case Sanitizer" could remove all contraband images from a hard drive prior to its production. After the Government twice moved to prohibit the use of this software, the defense eventually relinquished its claim. The Government argued that the defense had not provided, nor could it locate, any reports or results regarding validation testing of the Case Sanitizer software, rendering it unlikely to withstand a Daubert test. *See id.*; Docket Nos. 36, 38. Moreover, the Government exposed the defense expert's faulty assumption that the Government could easily double-check the results of his sanitizing to ascertain whether all image files were successfully removed from the hard drive. The parties did, however, eventually reach an agreement allowing defense counsel to copy digital evidence stored at the government facility, but prohibiting defense counsel from copying any child pornography. Under this agreement, the defense was prohibited from utilizing the Case Sanitizer software to create a full mirror copy of the hard drive that was purportedly scrubbed of all image or video files. *Id.*; Docket No. 40.

On the other hand, in *United States v. Tummins*, 2011 WL 2078107, at *5 (M.D. Tenn. May 26, 2011), the court ordered the Government to produce, over its objection, a copy of a hard drive scrubbed of child pornography images. The court conducted an evidentiary hearing during which a defense expert testified that the forensic program EnCase could overwrite all child pornography files on the computer while leaving the remainder of the file information intact. That defense expert did, however, concede on cross-examination that some files containing images of children could possibly remain in unallocated space even after EnCase concluded its performance. The Government expert testified that the "only way to guarantee that no child pornography gets out is for the Government to maintain control of the hard drives" and that "there is no way to ensure that no child pornography images remain after a digital redaction." *Id.* at *5.

After considering this testimony, the court ruled that it could not precisely answer the question of "what is the realistic possibility that recognizable child pornography will remain on this forensic copy of the hard drive despite digital redaction of the contents of all files identified by the Government as containing child pornography." *Id.* at *6. The court nevertheless ruled in defendant's favor on the grounds that the restrictions placed on the defense by the Government precluded the ample opportunity for inspection of contraband materials required by the Act. Specifically, the defense expert could only access the government facility eight hours per day, Monday through Friday. *Id.* Because the 750 gigabytes of electronic data required 19 hours of continuous run time merely to index, the defense expert would be required to "leave his hardware and software running unattended and inaccessible in Government offices, except during normal business hours, for the duration of an analysis that could take at least two weeks." *Id.* The defense expert had, furthermore, testified that his employer was unwilling to allow its equipment to remain inaccessible and unattended in a government facility.

Although the court ultimately ruled in defendant's favor, it grounded its holding in case-specific facts related to the Act's "ample opportunity" requirement and reached no blanket conclusion concerning the Government's obligation to produce scrubbed hard drives to a defense expert upon request. *Id.* at *7. Moreover, the court took great pains to ensure that any inadvertently produced contraband materials would not be further disseminated by ordering: (1) the redacted hard drives to be maintained in a secure location in the custody of defendant's forensic computer expert; (2) access to the hard drives be limited to the defense attorney and computer expert; (3) the hard drives to be used only for purposes of the present case; (4) no copy of any image of child pornography to be made; (5) the hard drives to be returned to the Government upon completion of the defense examination; and (6) certification by the defense expert that all files (or fragments thereof) obtained from the hard drives were permanently removed and deleted from any defense computer equipment. *Id.*

VI. Conclusion

The passage of the Act has prevented court-ordered production of copies of child pornography evidence to defense counsel in all but extremely narrow circumstances. Defense counsel seeking production of such evidence are likely to rely upon *Knellinger* and *Winslow* in contending that, unless they receive a mirror image of the Government's forensic evidence, they will be deprived of "ample opportunity" to conduct forensic examinations central to their defense strategy. Prosecutors can rebut these arguments by pointing to the numerous cases casting doubt on or limiting the scope of *Knellinger* and *Winslow*. When faced with a particularly skeptical judge, prosecutors can also make reasonable accommodations to defense experts conducting on-site work that cure the concerns outlined by these two opinions.

Defendants may also request production of a sanitized forensic copy of all electronic storage media. This production is a highly burdensome process that commands a massive amount of government time and resources. Moreover, even utilizing the best technology and manual skills available, the Government cannot guarantee a truly sanitized result, leaving the door open for potential violations of the Act via inadvertent production of contraband materials. In all events, any fully sanitized hard drive would provide little forensic value to defense experts. For these reasons, prosecutors should strongly oppose any such production requests.❖

ABOUT THE AUTHOR

❑**Jeffrey Zeeman** has been a Trial Attorney for the Child Exploitation and Obscenity Section (CEOS) in the Criminal Division of the U.S. Department of Justice since 2008. Prior to joining the Department, Mr. Zeeman was a litigation associate at the Washington, D.C. office of Covington & Burling LLP and the Boston office of Bingham McCutchen LLP and an Assistant District Attorney in Middlesex County, Massachusetts.✠

Getting Your Evidence into Evidence in a Digital World

Damon King
Deputy Chief and Senior Litigation Counsel
Child Exploitation and Obscenity Section
Meredith Owen
Legal Intern
Child Exploitation and Obscenity Section

I. Introduction

Electronic communications and child pornography are frequently obtained as evidence in child exploitation cases. In order to overcome an objection by the defense that an evidentiary exhibit lacks authentication or is inadmissible hearsay, the prosecutor must understand the rules of evidence as they apply to the admission of such evidence and be prepared to respond to such objections with respect to each exhibit being offered.

II. Authentication

The first step in laying the foundation for the admission of an evidentiary exhibit, whether the evidence is in digital or hard copy (printout) form, is to authenticate the exhibit. In order to authenticate an exhibit, Federal Rule of Evidence 901(a) requires the proponent to introduce "evidence sufficient to support a finding that the matter in question is what its proponent claims."

A. Electronic communications

The following excerpt from the Rutgers Computer and Technology Law Journal provides a clear explanation of authentication in practice:

> The simplest way to authenticate any item of evidence is through testimony by a knowledgeable witness "that a matter is what it is claimed to be." Where a document embodies a communication, if a participant in, or recipient of, that communication was able to perceive who communicated what, then that person can authenticate the communication. Where a written communication such as an e-mail message is transmitted, only the author of the e-mail message or anyone who saw the author compose and transmit the message will truly "know" the message's authorship, and be able to authenticate it. . . . Accordingly, where the author is unavailable to testify or where the witness authored only some of the messages contained in a chain of e-mail messages, questions regarding the knowledge requirement may arise. In these instances, however, authentication will be facilitated by the liberal approach taken by courts to the "knowledge" requirement and by the circumstantial methods of authentication available through Rule 901(b) and otherwise.
>
> . . . .

> Where the author of a message is not available to testify or where the purported author disclaims authorship of the message, Rule 901(b)(4) allows the proponent of an item of evidence to authenticate that item based on its "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with other circumstances." For example, if the contents of a document "disclos[e] knowledge of facts known peculiarly to" one person, those contents may establish that this person authored the document. Another established mechanism for authenticating letters from their contents may be useful in the e-mail context—namely, that "a letter may be authenticated by content and circumstances indicating it was in reply to a duly authenticated one." Language patterns used by an individual may also be helpful in establishing that a message with such language patterns was composed by that individual. For instance, an e-mail message may reflect an individual's distinctive word choice or sentence structure. Other factors that courts frequently consider in authenticating writings and other items will similarly apply to e-mail messages. These factors include where a document was located (including whether a party produced the document in discovery), whether a witness has knowledge that can connect the document to a particular person, whether the document was in existence at the time of circumstances necessary for a particular person to have created or received that item, whether the person who purportedly created the document had a motive for doing so that is consistent with the nature of the document, whether a person's or business's habit, routine, practice, or modus operandi is consistent with the document, whether the item reflects a date, return address, signature stamp, other marking, or letterhead that helps to identify the item's origin, and whether the contents of a writing reflect linguistic, grammatical, and stylistic traits consistent with a particular person's writing style.

Mark D. Robins, *Evidence at the Electronic Frontier: Introducing E-mail at Trial in Commercial Litigation*, 29 RUTGERS COMPUTER & TECH. L.J. 219, 226-29 (2003) (footnotes omitted); *see generally* Orin S. Kerr, *Computer Records and the Federal Rules of Evidence*, UNITED STATES ATTORNEYS' BULLETIN, Mar. 2001, at 26-29 (discussing the authentication of evidence).

Within the non-exhaustive list of examples set forth in Rule 901 of how to authenticate evidence, it is noted that "evidence that a [telephone] call was made to the number assigned at the time by the phone company to a particular person or business," together with circumstances identifying the recipient of the call, would authenticate the telephone conversation. FED. R. EVID. 901(b)(6). By analogy, evidence that an electronic communication such as an email or chat was sent from an account or an IP address assigned at the time by a particular Internet Service Provider or systems administrator to a particular person or computer, together with circumstances identifying the sender of the electronic communication, should sufficiently authenticate the electronic communication.

With regard to emails, for example, in *United States v. Siddiqui*, 235 F.3d 1318 (11th Cir. 2000), the Eleventh Circuit found that certain emails were adequately authenticated through circumstantial evidence and that the trial court had properly admitted the emails:

> In this case, a number of factors support the authenticity of the e-mail. The e-mail sent to Yamada and von Gunten each bore Siddiqui's e-mail address "*msiddiquo@jajuar1.usouthal.edu*" at the University of South Alabama. This address was the same as the e-mail sent to Siddiqui from Yamada as introduced by Siddiqui's counsel in his deposition cross-examination of Yamada. Von Gunten testified that when he replied to the e-mail apparently sent by Siddiqui, the "reply-function" on Von Gunten's e-mail system automatically dialed Siddiqui's e-mail address as the sender.

> The context of the e-mail sent to Yamada and von Gunten shows the author of the e-mail to have been someone who would have known the very details of Siddiqui's conduct with respect to the Waterman Award and the NSF's subsequent investigation. In addition, in one e-mail sent to von Gunten, the author makes apologies for cutting short his visit to EAWAG, the Swiss Federal Institute for Environmental Science and Technology. In his deposition, Von Gunten testified that in 1994 Siddiqui had gone to Switzerland to begin a collaboration with EAWAG for three or four months, but had left after only three weeks to take a teaching job.
>
> Moreover, the e-mail sent to Yamada and von Gunten referred to the author as "Mo." Both Yamada and von Gunten recognized this as Siddiqui's nickname. Finally, both Yamada and von Gunten testified that they spoke by phone with Siddiqui soon after the receipt of the e-mail, and that Siddiqui made the same requests that had been made in the e-mail. Considering these circumstances, the district court did not abuse its discretion in ruling that the documents were adequately authenticated.

Id. at 1322-23. *See also Fenje v. Feld*, 301 F. Supp. 2d 781, 809 (N.D. Ill. 2003) ("E-mail communications may be authenticated as being from the purported author based on an affidavit of the recipient; the e-mail address from which it originated; comparison of the content to other evidence; and/or statements or other communications from the purported author acknowledging the e-mail communication that is being authenticated.") (internal citations omitted).

Similarly, in *United States v. Simpson*, 152 F.3d 1241 (10th Cir. 1998), the Tenth Circuit held that chat logs were sufficiently authenticated and properly admitted by the trial court in a prosecution for receiving child pornography, stating:

> Simpson next argues that the trial court erred in admitting Plaintiff's Exhibit 11, which is a computer printout of the alleged chat room discussion between Simpson and Detective Rehman, because the government could not identify that the statements attributed to Simpson were in his handwriting, his writing style, or his voice pursuant to FED. R. EVID. 901(b)(2)S(5). Therefore, argues Simpson, the evidence was not authenticated and should not have been admitted. The specific examples of authentication referred to by Simpson are merely illustrative, however, and are not intended as an exclusive enumeration of allowable methods of authentication. *See* FED. R. EVID. 901(b). Rather, all that is ultimately required is "evidence sufficient to support a finding that the matter in question is what its proponent claims." FED. R. EVID. 901(a).
>
> The evidence introduced at trial clearly satisfies this standard. In the printout of the chat room discussion, the individual using the identity "Stavron" gave Detective Rehman his name as B. Simpson and his correct street address. The discussion and subsequent e-mail exchanges indicated an e-mail address which belonged to Simpson. And the pages found near the computer in Simpson's home and introduced as evidence as Plaintiff's Exhibit 6 contain a notation of the name, street address, e-mail address, and telephone number that Detective Rehman gave to the individual in the chat room. Based on this evidence, the exhibit was properly authenticated and admitted as evidence.

Id. at 1249-50 (citations omitted).

In *United States v. Owens*, 2010 WL 988834 (N.D. Miss. Mar. 12, 2010), the court rejected the defendant's claim that instant messages had not been properly authenticated:

> [The witness] first verified that she received the instant messages reflected in the exhibit and that they were sent under Owens's user name. She then testified that she worked with Owens over the years; that they often communicated in this manner; that he was the only one in his office with detailed knowledge of the subject matter discussed in the messages (something confirmed by others); and that when others would use Owens's user name, they would identify themselves. Rule 901 requires authentication through "evidence sufficient to support a finding that the matter in question is what its proponent claims." The testimony was sufficient to authenticate the exhibit.

Id. at *5.

However, where a proponent fails to present sufficient evidence that the electronic communication is what it is claimed to be, a trial court may properly exclude it. In *United States v. Jackson*, 208 F.3d 633 (7th Cir. 2000), the defendant was charged with fraud and obstruction of justice for, among other things, falsely claiming that a delivery service had defaced her packages with racial slurs in an effort to extort money from the delivery service and sending hate mail to various prominent individuals in an attempt to frame another person. At trial, the defendant claimed that the packages had really been defaced and damaged by the delivery service and that the hate mail had been sent by white supremacist groups. The defendant appealed her conviction, claiming that the trial court improperly precluded her from introducing certain postings on the Web sites of several white supremacist groups. These postings, she asserted, gloat about the defendant's prosecution and take credit for having sent the mailings. The government, however, alleged that the defendant concocted and posted these statements on the Web sites herself in an attempt to cover up her crimes.

The Seventh Circuit held that the trial court properly excluded the postings for a number of reasons, including their lack of sufficient authentication. Specifically, the court held that the defendant failed to show that the Web postings, stating that the white supremacist groups took responsibility for the racist mailings, were actually posted by those groups as opposed to being slipped onto the groups' Web sites by the defendant herself, a skilled computer user. *Id.* at 638. *See also Boim v. Holy Land Found. for Relief and Dev.*, 549 F.3d 685, 703 (7th Cir. 2008) ("[I]nternet website postings would not be admissible into evidence for their truth absent proper authentication, and this would typically require some type of proof that the postings were actually made by the individual or organization to which they are being attributed . . . as opposed to others with access to the website."); *Victaulic Co. v. Tieman*, 499 F.3d 227, 236 (3d Cir. 2007) ("Anyone may purchase an internet address, and so, without proceeding to discovery or some other means of authentication, it is premature to assume that a webpage is owned by a company merely because its trade name appears in the uniform resource locator."); *Bell v. Rochester Gas & Elec. Corp.*, 540 F. Supp. 2d 421, 429 (W.D.N.Y. 2008) (printout of alleged email held unauthenticated and inadmissible where the printout's header had been deleted and only the text was saved, where all senders and recipients denied communication, and where no other support was offered to substantiate the email as sent and unadulterated). *See generally* Michael Weingarten & Adam Weingarten, *Email Tampering —This Time, The Good Guys Won*, BUSINESS COMMUNICATIONS REVIEW (Jan. 2002), http://www.signallake.com/publications/emailtampering. pdf (describing civil litigation where the defendant proved through expert analysis that plaintiff had fabricated and altered email evidence that plaintiff was attempting to introduce).

In some instances, a witness may convert an electronic communication from one format into another format. For example, someone may cut and paste an email into a word processing document without adversely affecting the ability of a proponent to authenticate it. The ease of authentication in this case is especially true where the proponent is able to offer testimony from a witness that the exhibit is the communication in its entirety. In *United States v. Gagliardi*, 506 F.3d 140 (2d Cir. 2007), the Second

Circuit held that the district court did not abuse its discretion in admitting reformatted copies of the emails and transcripts of instant-message chats between the defendant, an FBI agent, and an informant who were posing as 13-year-old girls in an Internet chat room. The court found that the copies were sufficiently authenticated to be admissible where both the informant and the agent testified that the exhibits were in fact accurate records of defendant's conversations with them:

> Gagliardi's final claim is that the e-mails and transcripts of instant-message chats offered by the government were not properly authenticated. He argues that because the documents were largely cut from his electronic communications and then pasted into word processing files, they were not originals and *could have been subject to editing* by the government. Gagliardi contends that the communications could even have been completely fabricated. Due to these "highly suspicious" circumstances . . . Gagliardi submits that the government failed to establish authenticity and the trial court therefore erred in admitting the evidence. We disagree.
>
> We review a district court's evidentiary rulings for abuse of discretion. *Reilly v. Natwest Mkts. Group Inc.*, 181 F.3d 253, 266 (2d Cir. 1999). The bar for authentication of evidence is not particularly high. *United States v. Dhinsa*, 243 F.3d 635, 658 (2d Cir. 2001). "The requirement of authentication . . . is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." FED. R. EVID. 901(a). Generally, a document is properly authenticated if a reasonable juror could find in favor of authenticity. *United States v. Tin Yat Chin*, 371 F.3d 31, 38 (2d Cir. 2004). The proponent need not "rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be." *United States v. Pluta*, 176 F.3d 43, 49 (2d Cir. 1999) (internal quotation marks and citation omitted).
>
> We have stated that the standard for authentication is one of "reasonable likelihood," *id*. (internal quotation marks and citation omitted), and is "minimal," *Tin Yat Chin*, 371 F.3d at 38. The testimony of a witness with knowledge that a matter is what it is claimed to be is sufficient to satisfy this standard. *See* FED. R. EVID. 901(b)(1). In this case, both the informant and Agent Berglas testified that the exhibits were in fact accurate records of Gagliardi's conversations with Lorie and Julie. Based on their testimony, a reasonable juror could have found that the exhibits did represent those conversations, notwithstanding that the e-mails and online chats were editable. The district court did not abuse its discretion in admitting the documents into evidence.

Id. at 151 (emphasis added). *See United States v. Lanzon*, 639 F.3d 1293, 1301 (11th Cir. 2011) (transcripts of instant messenger conversations between detective and defendant in the form of a word processing document created by the detective using a cut-and-paste method that preserved the conversations in their entirety were properly authenticated and admitted where detective testified to their authenticity); *Porter v. United States*, 2008 WL 5451011, at *4 (E.D.N.Y. Dec. 31, 2008) (same); *see also United States v. Bonallo*, 858 F.2d 1427, 1436 (9th Cir. 1988) ("The fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness. The mere possibility [of alteration] goes only to the weight of the evidence not its admissibility."); *United States v. Hock Chee Koo*, 2011 WL 777965, at *10 (D. Or. Mar. 1, 2011) (same); *United States v. Safavian*, 435 F. Supp. 2d 36, 41 (D.D.C. 2006) (same).

Even where the exhibit is not the entire communication because portions of the communication have been deleted or destroyed, it may still be possible to authenticate the portions of the communication that remain. For instance, in *United States v. Tank*, 200 F.3d 627 (9th Cir. 2000), the Ninth Circuit held

that a third party's chat logs were properly authenticated and admitted in a child pornography prosecution, even though the third party had deleted nonsexual portions of the chats and other extraneous material in order to free space on his hard drive. The court stated:

> The foundational "requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." FED. R. EVID. 901(a); *see also United States v. Harrington*, 923 F.2d 1371, 1374 (9th Cir. 1991). "The government need only make a prima facie showing of authenticity, as '[t]he rule requires only that the court admit evidence if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification.' " *United States v. Black*, 767 F.2d 1334, 1342 (9th Cir. 1985) (quoting 5 J. Weinstein & M. Berger, Weinstein's Evidence ¶ 901(a) [01], at 901-16 to -17 (1983)). The government must also establish a connection between the proffered evidence and the defendant. *See id.*
>
> The government made a prima facie showing of authenticity because it presented evidence sufficient to allow a reasonable juror to find that the chat room log printouts were authenticated. In testimony at the evidentiary hearing and at trial, Riva explained how he created the logs with his computer and stated that the printouts, which did not contain the deleted material, appeared to be an accurate representation of the chat room conversations among members of the Orchid Club. *See United States v. Catabran*, 836 F.2d 453, 458 (9th Cir. 1988) ("Any question as to the accuracy of the printouts . . . would have affected only the weight of the printouts, not their admissibility."). Furthermore, the parties vigorously argued the issue of completeness of the chat room log evidence to the jury. *See United States v. Soulard*, 730 F.2d 1292, 1298 (9th Cir. 1984) ("[O]nce adequate foundational showings of authenticity and relevancy have been made, the issue of completeness then bears on the Government's burden of proof and is an issue for the jury to resolve.").
>
> The government also established a connection between Tank and the chat room log printouts. There is no question that the chat room log printouts were relevant to prove the conspiracy charge in the indictment and Tank's participation in the conspiracy. Tank admitted that he used the screen name "Cessna" when he participated in one of the conversations recorded in the chat room log printouts. Additionally, several co-conspirators testified that Tank used the chat room screen name "Cessna" that appeared throughout the printouts. They further testified that when they arranged a meeting with the person who used the screen name "Cessna," it was Tank who showed up.
>
> On the record before us, it is clear that the government made an adequate foundational showing of the relevance and the authenticity of the chat room log printouts. Thus, we cannot say that the district court abused its discretion by admitting the printouts into evidence and allowing the jury to decide what weight to give that evidence.

Id. at 630-31 (footnotes omitted).

A proponent's unjustified failure to properly preserve the entirety of a communication, coupled with a proponent having altered the portions that do in fact remain, is likely to result in exclusion. In *United States v. Jackson*, 488 F. Supp. 2d 866, 872 (D. Neb. 2007), the district court excluded a "cut-and-paste document" offered by the government. The document was purportedly Internet chat logs between the defendant and the undercover officer posing as 14-year-old girl. The government did not

offer the logs in their entirety apparently because: (1) the officer had saved the original data but had destroyed the originals when reformatting his hard-drive; (2) the only remaining parts were portions of the original; (3) the portions included the officer's added text and notes; (4) the government had lost an audiotape of a phone conversation between the officer and the defendant; and (5) the government had lost the defendant's computer after seizing it. Thus, what the government was offering as an exhibit was an "editorialized version of the cut-and-paste document." *Id.* at 871. Based on the foregoing, the court found that this document was "not authentic as a matter of law." *Id.* The court alternatively found that the best evidence rule precluded admission because not only was the exhibit not the entire conversation, the agent had editorialized the document. *Id.*

B. Child pornography

The Rule 901 authentication requirement—that the proponent introduce evidence sufficient to support a finding that the matter in question is what its proponent claims—is met with respect to child pornography evidentiary exhibits in the same manner as with any other evidentiary exhibit: the proponent introduces testimony from a witness with personal knowledge of where and how the child pornography evidentiary exhibits were obtained. In *United States v. Berringer*, 601 F. Supp. 2d 976 (N.D. Ohio 2008), a district court rejected a pretrial defense argument that the government would not be able to authenticate images of child pornography found on the defendant's computer:

> [T]he authentication requirement of Rule 901 applies to this case in essentially the same way it does to any similar item of evidence in any type of case. The Government must introduce sufficient proof so that a reasonable juror could conclude that [sic] the evidence is what the Government says it is—here, digital images found on computers and/or other electronic storage media found at Berringer's home. To authenticate such evidence, the Government simply must offer testimony establishing that the images were found on computers taken from Berringer's residence. This, the Government can (and presumably will) do by offering the testimony of a witness who was present and observed the procedure by which the evidence was obtained from Berringer's computers.

Id. at 979-80 (citations omitted).

In some cases, the child pornography evidentiary exhibit that is authenticated and introduced may be in the form of an actual film negative, printed photograph, or videotape seized or obtained by the government and associated with the defendant. *See United States v. Secrest*, 2000 WL 1763326, at *1 (7th Cir. Nov. 21, 2000). More commonly, however, the child pornography evidentiary exhibit will be in the form of a digital file that has been copied from a computer or digital device associated with the defendant or will be a printout of the copied digital file. For example, in *United States v. McNealy*, 625 F.3d 858 (5th Cir. 2010), federal agents seized the defendant's computer and used a computer forensic imaging process to produce exact copies of the three hard drives that were in the computer. These copies were placed on DVDs and the child pornography evidentiary exhibits introduced by the government were printed from the DVDs. The Fifth Circuit affirmed the district court's finding that the exhibits were properly authenticated and admitted under Rule 901. *Id.* at 867.

It is also not uncommon for a child pornography evidentiary exhibit to be a copy of a digital file from an Internet Service Provider (ISP) and an account associated with the defendant. The method and requirement for authenticating such an exhibit is similar to a child pornography exhibit derived from a physical device that is associated with the defendant. The following excerpt from *United States v. Cameron*, 762 F. Supp. 2d 152 (D. Me. 2011) illustrates this point:

> On March 15, 2007, Yahoo!, an ISP, received customer complaints about the existence of images of child pornography associated with the screen name "lilhottyohh." Yahoo! searched its servers for sites associated with that screen name and reported these images to the National Center for Missing and Exploited Children (NCMEC). In August 2007, after viewing the images, NCMEC referred the matter to the Maine State Police Computer Crimes Unit (MSPCCU), directing MSPCCU to images associated with the "lilhottyohh" screen name as well as to those associated with a second screen name, "lilhottee00000." Later, NCMEC made a second referral concerning child pornography that Yahoo! had discovered in the photographs section of an account under the screen name "harddude0000." Yahoo! records confirmed that these three screen names were traceable to an Internet Protocol (IP) address, which had been assigned to Mr. Cameron's wife at a residence they shared in Hallowell, Maine.
>
> On December 17, 2007, the Maine State Police executed a search warrant at Mr. Cameron's residence and seized four computers. An analysis of the four computers revealed, among other things, that an eMachines computer at Mr. Cameron's home had been used to access seventeen Yahoo! profiles, including variations of "lilhottee," "harddude," and other screen names. Based on this and other information, the Government served process on Yahoo!. In compliance with the subpoena, Yahoo! produced images and discs associated with the identified screen names that contained child pornography. At trial, the Government sought to introduce these images of child pornography with evidence tying the Defendant to the screen names.

Id. at 155-56 (footnotes omitted).

The government presented testimony from a Yahoo! records custodian in the company's legal compliance unit. The custodian testified that the evidence being offered by the government was the same as that from Yahoo!'s servers. The district court found that the government had satisfied the Rule 901 authenticity requirements and admitted the exhibits into evidence. *Id.* at 158-59; *cf. United States v. Baker*, 538 F.3d 324 (5th Cir. 2008) (reversing conviction where defendant was identified through Yahoo! report to NCMEC because exhibits were not properly authenticated).

As a general matter, objections to the authenticity of an exhibit that are premised on challenging the "chain of custody" of the exhibit or the item that the exhibit was produced from, such as an image copy of a hard drive, go to the weight of the evidence rather than its admissibility. *See, e.g.*, *United States v. Knowles*, 623 F.3d 381, 386-87 (6th Cir. 2010); *United States v. Gavegnano*, 305 F. App'x 954, 957-58 (4th Cir. 2009); *United States v. Black*, 239 F. App'x 210, 214 (6th Cir. 2007).

Lastly, courts have uniformly rejected defense claims that a child pornography evidentiary exhibit cannot be authenticated unless the government first establishes that the person(s) depicted in the image are "actual minors" (as opposed to computer generated images of minors, altered or modified photographic images, or adults who look like minors) and that a testifying witness authenticating the exhibit must have met the minor or even been present when the original photo or video of the minor was taken. Courts have rejected these claims because they conflate the issue of authentication of exhibits with the issue of weight and sufficiency of the evidence proving the elements of the offense charged. *United States v. McNealy*, 625 F.3d 858, 864-67 (5th Cir. 2010); *United States v. Secrest*, 2000 WL 1763326, at *2, *3 (7th Cir. Nov. 21, 2000); *United States v. Nolan*, 818 F.2d 1015, 1017 (1st Cir.1987); *United States v. Berringer*, 601 F. Supp. 2d 976, 979-80 (N.D. Ohio 2008).

C. The best evidence rule

The "best evidence" rule provides that "[t]o prove the content of a writing, recording, or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." FED. R. EVID. 1002.

Accurate printouts of computer data are "originals." Federal Rule of Evidence 1001(3) states, "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an 'original.' " Additionally, Rule 1003 provides, "A duplicate is admissible to the same extent as an original unless (1) a genuine question is raised as to the authenticity of the original or (2) in the circumstances it would be unfair to admit the duplicate in lieu of the original." *See United States v. McNealy*, 625 F.3d 858 (5th Cir. 2010), mentioned previously in section II.B.

Rule 1004 sets forth additional circumstances where the best evidence rule is satisfied:

> The original is not required, and other evidence of the contents of a writing, recording, or photograph is admissible if—
>
> (1) Originals lost or destroyed. All originals are lost or have been destroyed, unless the proponent lost or destroyed them in bad faith; or
>
> (2) Original not obtainable. No original can be obtained by any available judicial process or procedure; or
>
> (3) Original in possession of opponent. At a time when an original was under the control of the party against whom offered, that party was put on notice, by the pleadings or otherwise, that the contents would be a subject of proof at the hearing, and that party does not produce the original at the hearing; or
>
> (4) Collateral matters. The writing, recording, or photograph is not closely related to a controlling issue.

See United States v. Lanzon, 639 F.3d 1293, 1301(11th Cir. 2011) (transcripts of instant message conversations between detective and defendant in the form of a word processing document created by the detective using a cut-and-paste method were properly admitted under Rule 1004); *United States v. Nelson*, 38 F. App'x 386 (9th Cir. 2002) (testimony of two officers who described the contents of child pornography photographs the defendant possessed two years earlier, offered under Federal Rule of Evidence 404(b), was properly admitted where the government claimed the originals had been "lost in the shuffle"); *see also McNealy*, 625 F.3d at 868-70 (government's negligent destruction of defendant's computer was not in bad faith).

III. Responding to a hearsay objection

Other than a claim that an evidentiary exhibit is insufficiently authenticated, the most frequently lodged objection to the introduction of the exhibit is that the exhibit is hearsay. In many instances, the government will be able to overcome a hearsay objection either because it is not hearsay as defined by the Federal Rules of Evidence or because the communication is admissible under an exception to the general rule precluding introduction of hearsay. *See generally* Orin S. Kerr, *Computer Records and the Federal Rules of Evidence*, UNITED STATES ATTORNEYS' BULLETIN, Mar. 2001, at 29-31 (discussing theories of admissibility and cases involving computer records).

A. Non-hearsay

Often an electronic communication being offered by the prosecution will qualify as an admission of a party opponent under Federal Rule of Evidence 801(d)(2)(A). *United States v. Burt*, 495 F.3d 733, 738 (7th Cir. 2007) (portions of internet chat written by defendant concerning distribution of child pornography constitute admissions and portions written by person with whom the defendant was conversing admitted, not for the truth of the matter asserted, but rather as necessary context of defendant's admissions); *United States v. Siddiqui*, 235 F.3d 1318, 1323 (11th Cir. 2000) (defendant's emails pertaining to fraud scheme that were sent to two individuals were admissible as admissions of a party opponent); *United States v. Moran*, 493 F.3d 1002, 1011 (9th Cir. 2007) (per curiam) (Quickbooks financial data recovered from coconspirator's computer held admissible because coconspirator statements were made during the course and in furtherance of the conspiracy and because "alleged evidence of inaccuracies in the computer records does not affect their admissibility, but merely goes to their weight"); *Van Westrienen v. Americontinental Collection Corp.*, 94 F. Supp. 2d 1087, 1109 (D. Or. 2000) (representations made by defendants on their Web site were admissible as admissions of a party opponent); *cf. United States v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000) (Web site postings allegedly made by third parties were hearsay that no exception applied to and were also unauthenticated, unfairly prejudicial, and irrelevant to fraud charges).

In other instances, the electronic communication (or a portion of a communication) will qualify as non-hearsay because it is not a "statement" of a person. One example is email header information such as the date, time, or IP address, because such information is machine-generated much like the header information on a fax transmission. *See United States v. Washington*, 498 F.3d 225, 231 (4th Cir. 2007) (holding that raw data generated by machines are not hearsay statements because statements must be declared by persons); *accord United States v. Hamilton*, 413 F.3d 1138, 1142-43 (10th Cir. 2005) (holding that computer-generated header information including uploader's IP address that is automatically attached to images of child pornography posted on newsgroup is not hearsay because computer generations without the input or assistance of persons are not statements); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) (where defendant sought to admit a fax transmission's header information bearing the transmission date in prosecution for bank fraud, the header information was not hearsay because under Federal Rule of Evidence 801(a) nothing said by a machine is hearsay).

Additionally, an electronic communication is not hearsay if it is being offered, not for the truth of the matters asserted in the communication, but for another purpose such as to show the relationship between the defendant and another person, the defendant's method of communicating, or the relationship between the defendant and a piece of physical or documentary evidence (such as a computer or a particular image). *United States v. Koch*, 625 F.3d 470, 479-80 (8th Cir. 2010) (documents authored by defendant Jonathan Koch for college courses and other subjects, digital photographs of defendant, and the user names "Jo" and "Jonathon" on computer and flash drive were not offered for the truth of the matter asserted and were properly admitted as circumstantial evidence associating the defendant with the computer and flash drive containing child pornography); *Siddiqui*, 235 F.3d at 1323 (emails that defendant sent to another person that were unrelated to the fraud scheme were nonetheless admissible as non-hearsay because they were offered to show the relationship between the defendant and the other person and their custom of communicating by email); *Khorozian*, 333 F.3d at 506 (holding that the trial court erred when it excluded a fax on hearsay grounds where the defendant moved to admit the fax not to prove the truth of the matters asserted in the text but rather for the fact that the fax contained a certain name); *see also United States v. Cameron*, 762 F. Supp. 2d 152, 157-58 (D. Me. 2011) (child pornography images are not hearsay).

B. Hearsay exceptions

In some circumstances, an electronic communication that is hearsay may qualify for admission into evidence under a hearsay exception. For example, in a prosecution for fraud, bribery, and extortion, the government sought to admit into evidence an email written by the defendant's superior that recounted a conversation between the superior and the defendant. The defendant made incriminating statements in this email. The trial court found that the email did not qualify for admission pursuant to the business record exception of Federal Rule of Evidence 803(6) because the defendant's superior was under no business duty to make and maintain email messages such as the one being offered by the prosecution. Additionally, the company that employed him did not follow a routine of making and maintaining such records. The trial court also rejected the government's claim that the email qualified as an excited utterance pursuant to Federal Rule of Evidence 803(2). However, the court found that the email qualified for admission into evidence under Rule 803(1) as a present sense impression of the defendant's superior and thus admitted it into evidence over the defendant's objection. *United States v. Ferber*, 966 F. Supp. 90, 98-99 (D. Mass. 1997).

Prosecutors should note that contents of electronic communications, such as email text, that are obtained from an ISP will likely not qualify for admission into evidence as business records under Rule 803(6). Such contents will not likely be admitted in this way primarily because ISPs do not take any steps to ensure the accuracy of the statements contained in the emails sent or received by their account holders. As one court stated, "Internet service providers . . . are merely conduits. . . . The fact that the Internet service providers may be able to retrieve information that its customers posted or email that its customers sent does not turn that material into a business record of the Internet service provider." *United States v. Jackson*, 208 F.3d 633, 637 (7th Cir. 2000) (where Web site postings obtained from ISP were hearsay and did not qualify as business records under Rule 803(6)); *cf. Cameron*, 762 F. Supp. 2d at 157-58 (expressing that child pornography images on Yahoo!'s servers are best viewed as non-hearsay because they are substantive evidence but, in the alternative, are potentially admissible under Rule 803(6) because Yahoo!'s receipt and storage of postings and images by its customers on Yahoo!'s servers were made in the "course of regularly conducted business activity").

It is important to note, however, that although the contents of such communications may not qualify as business records, other information and records in the possession of the ISP, including some of the subscriber information described in 18 U.S.C. § 2703(c)(2), may in fact qualify for admission as a business record. *See United States v. Salgado*, 250 F.3d 438, 453 (6th Cir. 2001) (telephone company's toll records that included "subscriber line information, [such as] the subscriber's name, the location where the telephone was installed, the date and duration of local and long distance telephone calls, the numbers from which calls were placed and at which they were received, and billing amounts" were admissible as business records where telephone company security manager testified that it was a regular practice of the telephone company to make these reports and keep these types of records because the records are relied on by the telephone company to ensure accuracy of billing).

C. Summaries and demonstrative exhibits

Electronic communications may also be admitted into evidence either as a summary of evidence already introduced into evidence at trial or under Federal Rule of Evidence 1006 as a summary of voluminous records. In *United States v. Burt*, 495 F.3d 733 (7th Cir. 2007), the Seventh Circuit upheld admission of excerpts of chat logs concerning distribution of child pornography where the government had substituted the screen-names of defendant and informant. In this particular instance, the "raw chat logs" had already been introduced into evidence, so the excerpts were being introduced as a summary of

evidence already introduced at trial. Accordingly, the Seventh Circuit held that the alterations were not hearsay and not overly and unduly prejudicial:

> We come to this conclusion by considering the altered chat logs in the context for which they were offered, and by analogizing to other more commonly accepted demonstrative exhibits. When the government introduced the excerpts, the prosecutor asked Brelsford to authenticate the excerpts. He replied that it was "a summary, a synopsis, of the chats reflected in the previous Government exhibit." Tr. at 406. After Brelsford clarified that the excerpts were "direct quote excerpts of the overall chats," the government asked, "have you reviewed [the excerpts] and determined that that exhibit accurately transcribes what is portrayed in Government Exhibit Starved Rock Chat?" *Id.* at 407. Brelsford agreed that, with the exception of two typographic errors which were corrected, "the actual context of the communication is verbatim." *Id.*
>
> The court admonished the jury that they were to independently evaluate whether the evidence convinced them that the screen names were actually used by Martin and Burt. The court noted that there was evidence that the screen names corresponded to those individuals, and warned the jury that "even though [the] exhibit says Martin and Burt . . . if I advise you that in fact it was Starved Rock and BsomeSmoke . . . that is what it said." *Id.* at 412-13. Finally, the court clarified to the jury that "whether or not [Martin and Burt] really authored these statements is something that you will have to conclude." *Id.* at 413. At that point the government led agent Brelsford through an analysis of the chat logs to clarify what Martin and Burt had written to each other.
>
> . . . .
>
> We see no reason not to extend the logic of allowing models, maps, sketches, and diagrams to incorporate these particular chat excerpts as well. In this case, the excerpted chat logs were used to aid two witnesses in interpreting and explaining the raw computer chat logs, which forensic examiners had recovered from Martin's computer. Just as a sketch or model of a crime scene can be used to help a witness to recount aspects of testimony and to make that testimony more accessible and understandable for the jury, so might affixing the names of real people in place of their aliases put the computer chat comments into a more useful context for the witnesses and the jury.
>
> . . . .
>
> As for being prejudicial, Rule 403 speaks of "unfair prejudice, confusion of the issues, or misleading the jury." There is a difference between evidence that brings unfair prejudice and evidence that is damning. If this chat log were being offered in a prosecution for an unrelated crime, we might be more sympathetic to a claim that it could unfairly prejudice a jury. Being associated with the sexual exploitation of children tends to do that. But the point is that in this case Burt was being prosecuted for exactly what this chat log depicts: creating, trading, and distributing photos of children for the sexual satisfaction of himself and his online partners. The chat may well have been damning, but we do not see how it created unfair prejudice. We caution that allowing the government to insert the real names in place of the screen names is a path that a district court should be careful to tread. But the court very clearly instructed the jury about the limited extent to which that substitution of names could be considered by the jury, and we emphasize that in this particular trial nobody seriously contended that this internet chat was conducted by

> anybody other than Martin and Burt. We find no error in the admission of the raw chat logs or the excerpted chats.

Id. at 739-41.

If, however, the electronic communications or portions thereof are not being offered as summaries of evidence already introduced at trial, but rather as a summary of voluminous records under Rule 1006, the underlying material need not already have been introduced into evidence so long as the underlying materials are in fact admissible. *United States v. Pelullo*, 964 F.2d 193, 204 (3d Cir. 1992). The rule requires that the underlying material, but not the summary itself, be made available to the adverse party before trial. *Coates v. Johnson & Johnson*, 756 F.2d 524, 549-50 (7th Cir. 1985); *but see Air Safety, Inc. v. Roman Catholic Archbishop of Boston*, 94 F.3d 1, 8 (1st Cir. 1996) ("[In order] to satisfy the 'made available' requirement, a party seeking to use a summary under Rule 1006 must identify its exhibit as such, provide a list or description of the documents supporting the exhibit, and state when and where they may be reviewed."). Whether the underlying material must be produced in court is a matter of the court's discretion under the rule. *United States v. Bakker*, 925 F.2d 728, 736 (4th Cir. 1991) (original broadcast tapes need not have been produced in court and introduced into evidence in order for eleven composite tapes summarizing the 200 hours of broadcasts occurring over three year period to be properly admitted).

IV. Conclusion

In order to avoid admissibility problems at trial, it is important for the prosecutor to understand the rules of evidence as they apply to the admission of electronic evidence and to be able to articulate a theory of admissibility with respect to each exhibit that the prosecutor intends to offer into evidence. Advance thought, preparation, and planning in this regard will greatly improve the prosecutor's chances of successfully admitting the exhibits into evidence.❖

ABOUT THE AUTHORS

❑**Damon King** is a Deputy Chief and Senior Litigation Counsel in the Child Exploitation and Obscenity Section (CEOS) of the Criminal Division of the U.S. Department of Justice. Mr. King served at the U.S. Attorney's Office in the Eastern District of Virginia from 1996 through 2001 and as a Special Assistant United States Attorney while also serving on active duty as a prosecutor in the U.S. Army Judge Advocate General's Corps. After joining CEOS in 2001 as a Trial Attorney, he became a Deputy Chief in 2005 and a Senior Litigation Counsel in 2008.✠

❑**Meredith Owen** served with the Child Exploitation and Obscenity Section in the Criminal Division of the U.S. Department of Justice as a law clerk in the spring of 2011. Ms. Owen plans to pursue a career in international criminal justice. She received a Distinguished Fellowship with the World Organization for Human Rights USA and beginning September 2011 will represent survivors of human trafficking in civil actions and immigration proceedings.✠

Understanding Probable Cause and Overcoming Staleness Issues in Child Pornography Cases

Chantel Febus
Trial Attorney
Child Exploitation and Obscenity Section

I. Introduction

"Probable cause exists where 'the facts and circumstances within [an officer's] knowledge and of which [he] ha[s] reasonably trustworthy information are sufficient in themselves to warrant a man of reasonable caution in the belief that' an offense has been or is being committed." *Brinegar v. United States*, 338 U.S. 160, 175-76 (1949) (citing *Carroll v. United States*, 267 U.S. 132, 162 (1925)). Probable cause to search a particular place rests upon the "commonsense, practical question whether there is 'probable cause' to believe that contraband or evidence is located in a particular place." *Illinois v. Gates*, 462 U.S. 213, 230 (1983).

The issue of staleness arises when the passage of time between the act(s) underlying the basis for probable cause and the search warrant application suggest that the sought-after evidence will no longer be located at the place to be searched. Staleness allegations often surface in child pornography cases because the nature of these investigations often means that weeks, months, or even years may pass between the initial development of probable cause facts and the presentation of a search warrant application to a magistrate judge. This passage of time, however, need not be fatal.

The age of the information presented in a search warrant is an important consideration. *See Sgro v. United States*, 287 U.S. 206 (1932). However, contrary to common defense arguments, no rigid, technical, or temporal litmus test for probable cause exists. *Gates*, 462 U.S. at 231-32. Indeed, in most instances, the mere passage of time is unlikely to render information in a child pornography warrant stale because, as courts have recognized, child pornography evidence has a long preservation period, is not transient or easily degraded by the passage of time, and is forensically recoverable even in the case of file corruption, deletion, or steganography. Moreover, if properly presented with corroborating and contemporary investigative information, an affidavit in support of a child pornography search warrant should set forth the progression of the investigation in a manner that is more than sufficient to overcome staleness concerns.

II. The Fourth Amendment probable cause requirement and the fair probability standard

The Fourth Amendment protects citizens from unreasonable searches and seizures. *See* U.S. CONST. amend. IV. As interpreted, the Fourth Amendment requires that a search warrant be issued based on probable cause. *Gates*, 462 U.S. at 238. Probable cause for a search warrant exists where, based on the facts and circumstances, it is reasonable to believe that a crime has been committed and that evidence of a crime will be located in the place to be searched. *Id.* at 230.

The standard for probable cause is "fair probability" in light of the totality of the circumstances. *Id.* at 233, 238. As the Supreme Court has explained, when an application for a search warrant is presented:

> [t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the "veracity" and "basis of knowledge" of persons supplying hearsay information, there is a *fair probability* that contraband or evidence of a crime will be found in a particular place.

Id. at 238 (emphasis added).

The probable cause standard "is a 'practical, nontechnical conception.' " *Id.* at 231 (quoting *Brinegar v. United States*, 338 U.S. 160, 176 (1949)). It "does not require the fine resolution of conflicting evidence that a reasonable-doubt or even a preponderance standard demands . . . ." *Gerstein v. Pugh*, 420 U.S. 103, 121 (1975). Nor is it amenable to hard-and-fast rules. *See Gates*, 462 U.S. at 232. Indeed, the Supreme Court made clear in *Gates* that:

> [i]n dealing with probable cause . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act . . . . *The process does not deal with hard certainties, but with probabilities.*

Id. at 231 (borrowing from the particularized suspicion standard set forth in *United States v. Cortez*, 449 U.S. 411, 418 (1981)) (emphasis added). Notwithstanding the persistent appeal for a more exacting standard, courts have squarely rejected attempts by defendants "to sidestep the 'fair probability' standard and elevate probable cause to a test of near certainty." *United States v. Gourde*, 440 F.3d 1065, 1072 (9th Cir. 2006) (en banc). For instance, in *Gourde*, the defendant argued that the court should disregard "profile" information contained in the search warrant application and apply a near-certainty standard to the probable cause determination. Rejecting that position, the court explained that:

> *Gates . . . does not compel the government to provide more facts than necessary to show a "fair probability" that Gourde had committed a crime.* Gourde's approach imposes a standard explicitly rejected by *Gates*. He confuses the relaxed standard of "fair probability" with the higher standards imposed at trial.

Id. at 1073 (citing *Gates*, 462 U.S. at 235) (emphasis added); *see also id.* (citing *Gates* for the proposition that "[f]inely-tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the magistrate's decision."). An enhanced standard would be inconsistent with *Gates* because "[p]robable cause requires only a probability or substantial chance of criminal activity, not an actual showing of such activity." *United States v. Lapsins*, 570 F.3d 758, 764 (6th Cir. 2009) (quoting *Gates*, 462 U.S. at 243).

In addition to the facts presented in support of probable cause, it is well-established that the training and experience of law enforcement agents bears significantly in probable cause determinations. *Gates*, 462 U.S. at 232. Accordingly, probable cause may rest on reasonable inferences drawn by law enforcement agents based on the facts known to them, the totality of the circumstances surrounding the conduct at issue, and their training and experience. *Id.* Specialized law enforcement training amplifies the significance of this factor because "officers assigned to 'specialized areas of enforcement, become familiar with the methods of those engaged in particular types of criminal activity,' giving them an ability to detect unlawful activity where laymen might not." *United States v. Funches*, 327 F.3d 582, 586 (7th Cir. 2003) (quoting WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH

AMENDMENT, § 3.2(c), at 38 (3d ed. 1996)). Moreover, courts have recognized the deference to be accorded to probable cause determinations made by informed and specially trained law enforcement agents. *See United States v. Arvizu*, 534 U.S. 266, 273 (2002) (reviewing courts must "allow[] officers to draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that 'might well elude an untrained person' ").

Specialized law enforcement training plays a significant role in probable cause determinations in child pornography warrants. The vast majority of child pornography investigations are computer and Internet based. As generally set forth in child pornography warrants, agents working in this field often receive specialized training regarding the computer technologies, networks, and software applications used in the commission of child pornography crimes; namely, how these technologies are used by offenders to produce, trade, store, and maintain child pornography and exploitation evidence, as well as how these technologies may be forensically examined to recover evidence of crime. Agents' training and experience also qualify these agents to make statements about characteristics that are common to individuals who possess and traffic in child pornography. One specific characteristic is that these individuals tend to collect and keep their child pornography materials for extended periods. This type of "profile" information supports the basis for a reasonable belief that evidence of child pornography is likely to be found at the place to be searched. Although the use of "profile" language has met some resistance, its use is appropriate when the warrant also includes "sufficient information from which it can be concluded that the target falls within these categories." *United States v. Lamb*, 945 F. Supp. 441, 460 (N.D.N.Y. 1996). This wealth of specialized training is critical to an agent's ability to detect specific instances or patterns of child pornography and exploitation activity that an untrained agent may not recognize, investigate, or develop. This training is also critical in preserving evidence and determining the type and length of investigation needed to develop legally sufficient probable cause facts.

III. Staleness analysis in child pornography cases

Staleness tests whether facts presented in support of probable cause "relat[e] to presently existing condition[s]." LAFAVE, SEARCH AND SEIZURE, § 3.7 at 338, 339. Accordingly, when the issue of staleness arises in the context of a probable cause determination for a search warrant, the question is whether, *at the time of the application for the warrant*, a fair probability existed that a crime had been committed and that the items to be seized will be in the place to be searched. *United States v. Spikes*, 158 F.3d 913, 923 (6th Cir. 1998) (citing *Sgro*, 287 U.S. 206 and LAFAVE, *supra*). With respect to child pornography warrants the answer usually is "yes."

Similar to general probable cause analysis, staleness is not amenable to technical, "bright-line" rules. *See United States v. Koelling*, 992 F.2d 817, 822 (8th Cir. 1993). Nor is it intended "to create an arbitrary time limitation within which discovered facts must be presented to a magistrate." *Spikes*, 158 F.3d at 923 (quoting *United States v. Henson*, 848 F.2d 1374, 1382 (6th Cir. 1988)). Rather, staleness is a flexible concept that turns, in significant part, on the nature of the crime at issue. *See United States v. Tehfe*, 722 F.2d 1114, 1119 (3d Cir. 1983). Although staleness analysis differs by jurisdiction, most courts focus on a set of considerations that includes the character of the crime, the nature of the item to be seized, the criminal suspect, and the place to be searched. *See United States v. Frechette*, 583 F.3d 374, 378 (6th Cir. 2009); *United States v. Morales-Aldahondo*, 524 F.3d 115, 119-20 (1st Cir. 2008); *United States v. Perrine*, 518 F.3d 1196, 1205-06 (10th Cir. 2008); *United States v. Rugh*, 968 F.2d 750, 754 (8th Cir. 1992).

A. Character of the crime

Courts have recognized that child pornography offenses are "[non]-fleeting" crimes. *Frechette*, 583 F.3d at 378 (upholding search warrant based on thirteen-month-old information about the suspect's subscription to a child pornography Web site). In *Frechette*, the court reasoned that "because the crime [of child pornography] is generally carried out in the secrecy of the home and over a long period, the same time limitations that have been applied to more fleeting crimes do not control the staleness inquiry for child pornography." *Id.* (quoting *United States v. Paull*, 551 F.3d 516, 522 (6th Cir. 2009)). Other courts have described the non-fleeting nature of child pornography crimes in terms of the "hoarding" and "collecting" that are often associated with these offenses. For example, in *Perrine*, a search warrant alleged that the defendant, who had a prior offense, transmitted several child pornography videos using a Yahoo! chat room. The warrant was based on facts that were nearly four months old at the time of warrant application. Concluding that the information set forth in the warrant application was not stale, the court stated that:

> The observation that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes is supported by common sense and the cases. Since the materials are illegal to distribute and possess, initial collection is difficult. Having succeeded in obtaining images, collectors are unlikely to destroy them. Because of their illegality and the imprimatur of severe social stigma such images carry, collectors will want to secret them in secure places, like a private residence. This proposition is not novel in either state or federal court: pedophiles, preferential child molesters, and child pornography collectors maintain their materials for significant periods of time.

Perrine, 518 F.3d at 1206; *see also United States v. Potts*, 586 F.3d 823, 830 (10th Cir. 2009) (observing that individuals who possess child pornography "are likely to hoard their materials and maintain them for significant periods of time"); *United States v. Lacy*, 119 F.3d 742, 745-46 (9th Cir. 1997) (same).

The "hoarder" rationale is similar in kind to the "collector" profile often associated with persons who receive, distribute, and possess child pornography. In *United States v. Pappas*, 592 F.3d 799 (7th Cir. 2010), the Seventh Circuit recently observed that:

> [T]he moniker "collector" merely recognizes that experts in the field have found that because child pornography is difficult to come by, those receiving the material often keep the images for years. There is nothing especially unique about individuals who are "collectors" of child pornography; rather, it is the nature of child pornography, i.e., its illegality and the difficulty procuring it, that causes recipients to become "collectors."

Id. at 804; *see also United States v. Lemon*, 590 F.3d 612 (8th Cir. 2010) (rejecting a staleness claim where the nature of the defendant's behavior and crime supported the law enforcement officer's categorization of the defendant as a "preferential collector of child pornography").

With respect to the character of the crime, courts have also observed that staleness is less of a concern where the criminal activity is continuous in nature. *See United States v. Albert*, 195 F. Supp. 2d 267, 277 (D. Mass. 2002) (quoting *United States v. Jewell*, 60 F.3d 20, 23 (1st Cir. 1995)); *see also United States v. Watzman*, 486 F.3d 1004, 1008 (7th Cir. 2007). For instance, in *Albert*, the defendant had given a compact disk to an informant whom law enforcement agents had deemed reliable. The disk contained 1,500 images of child pornography. The informant corresponded with defendant several times and viewed images of child pornography on defendant's home computer. Four months lapsed between the time the informant gave the disk to law enforcement agents and the date that an agent applied for a

search warrant. The court held that four-month-old information indicating that the defendant possessed and traded child pornography was not stale because "[t]he affidavit supports a finding of probable cause that Albert maintained a 'deep and continuing interest' in his collection of child pornography and that he 'traded regularly.' " *Id.* at 277 (quoting *United States v. Horn*, 187 F.3d 781, 787 (8th Cir. 1999)).

In *United States v. Harvey*, 2 F.3d 1318, 1321-22 (3d Cir. 1993), the search warrant application set forth facts that the defendant maintained a post office box where organizations that distributed child pornography sent information to him. The mailing activity dates ranged from two months to fifteen months before agents presented the search warrant application to a magistrate judge. The court rejected the defendant's staleness challenge, holding that the age of information is not the sole determinant of whether the information is stale. *Id*. at 1322. Rather, the nature of the crime being investigated and the type of evidence sought are also to be considered when determining whether information is fresh enough to establish probable cause. *Id.* (citing *United States v. Williams*, 897 F.2d 1034, 1039 (10th Cir. 1990); *United States v. McCall*, 740 F.2d 1331, 1135-36 (4th Cir. 1984); *United States v. Tehfe*, 722 F.2d 1114, 1119 (3d Cir. 1983); *United States v. Forsythe*, 560 F.2d 1127, 1132 (3d Cir. 1977)). The court concluded that a fair probability existed that child pornography evidence would be found at the defendant's apartment, notwithstanding the passage of time, because he maintained a post office box to receive child pornography over the course of several months and because persons who collect child pornography tend to keep this material, suggesting that the criminal activity would be of a continuous nature. *Harvey*, 2 F.3d at 1323.

In *United States v. Wiser-Amos*, 2007 WL 2669377, at *1 (W.D. Ky. Sept. 7, 2007), seven months passed between the time the law enforcement intercepted a child pornography video transported by the defendant using Peer-2-Peer software and the time when the search warrant was issued and executed. Rejecting the defendant's staleness challenge, the court reasoned that "[c]ourts which have considered the character of child pornography crimes . . . reject the characterization of such sexual offenses as being isolated or sporadic in nature . . . [because] . . . the widely accepted view [is] that 'individuals who possess and trade in child pornography tend to maintain visual depictions they have downloaded for long periods of time.' " *Id.* at *6-7. The court further observed that the defendant had invested time in installing Peer-2-Peer software that is "specifically designed to permit peer-to-peer sharing of electronic image files such as the [] child pornography video." *Id.* at *7. The court found that "[t]his conduct would cause a reasonably objective law enforcement officer or a magistrate judge to conclude that [the defendant] had a longstanding, serious interest in obtaining and distributing images of child pornography." *Id.*

B. Nature of the item to be seized

When considering the nature of the thing to be seized, courts have found the passage of time to be less significant for purposes of establishing probable cause in computer-based cases because trained forensic examiners have the ability to recover files from a computer, even when the files have been corrupted, hidden, or intentionally or inadvertently deleted. *See United States v. Hay*, 231 F.3d 630, 636 (9th Cir. 2000). This forensic capability undermines the argument that the passage of time suggests that a reasonable basis no longer exists to believe that the items to be seized are in the place to be searched. *See United States v. Toups*, 2007 WL 433562, at *4 (M.D. Ala. Feb. 6, 2007) (unpub.) ("Further bolstering the conclusion that the staleness calculation is unique when it comes to cases of internet child pornography is the images and videos stored on a computer are not easily eliminated from a computer's hard drive."); *United States v. Lamb*, 945 F. Supp. 441, 461 (N.D.N.Y. 1996).

In assessing the nature of the crime and things to be seized, courts often draw comparisons between the types of evidence at issue in child pornography cases and the types of evidence at issue in drug, gun, and business record cases. *See Lamb*, 945 F. Supp. at 460 (contrasting evidence in child pornography cases to drug cases and stating that "[s]ome contraband, like narcotic drugs, are consumable. Other evidence, like an illegal firearm, is more apt to remain in one place for extended periods"). For example, in cases involving drugs, because drugs are sold, moved, and consumed rapidly, probable cause to believe that the items to be seized are in the place to be searched becomes stale relatively quickly. *See United States v. Kennedy*, 427 F.3d 1136, 1142 (8th Cir. 2005) (holding that information about a narcotics crime can quickly go stale without information indicating an ongoing narcotics operation). Contrast that scenario with certain types of firearm cases: because firearms are collected and are likely to remain in the same place for years, probable cause exists for longer periods of time. *See United States v. Maxim*, 55 F.3d 394, 397-98 (8th Cir. 1995). Likewise, because business records are created for the very purpose of preservation, the passage of time means little and probable cause exists for extended periods of time as well. *See United States v. Williams*, 124 F.3d 411, 421 (3d Cir. 1997).

Federal courts have consistently recognized that child pornography evidence is more like business record and firearm evidence than drug evidence because child pornography is more likely to be collected and preserved for longer periods of time and is thus more likely to be recovered from the place subject to search. *Frechette*, 583 F.3d at 379. ("Unlike cases involving narcotics that are bought, sold, or used, digital images of child pornography can be easily duplicated and kept indefinitely even if they are sold or traded."). The court in *Frechette* explained that "images of child pornography can have an infinite life span." *Id.*; *see also Lamb*, 945 F. Supp. at 460 ("[T]he hare and the tortoise do not disappear at the same rate of speed.") (quoting *Andresen v. Maryland*, 24 Md. App. 128, 172 (1975), *aff'd*, 427 U.S. 463 (1976)).

C. The criminal suspect and the place to be searched

In evaluating staleness, courts sometimes credit the length of time that the criminal suspect has been associated with the place to be searched. Interestingly, courts have rejected staleness challenges in cases where defendants have occupied residences for extended periods and in cases where defendants have been more transient. For instance, in *Wiser-Amos*, the court observed that "[o]bviously, if a criminal defendant moves frequently with the hope of avoiding detection or capture, the probability that evidence of his or her criminal conduct will be found in a given location diminishes rapidly with the passage of time." 2007 WL 2669377, at *7 (finding that the defendant was not "nomadic" given that he had high-speed Internet access at his home and the same IP address during the seven-month period in question). In *Wiser-Amos* and like cases, however, this factor turns less on the length of residential occupancy and more on whether the criminal suspect lived in or maintained control over the place to be searched during the period in question. *See Frechette*, 583 F.3d at 378; *see also United States v. Hanson*, 2007 WL 4287716, at *6 (D. Me. Dec. 5, 2007) (finding that although the defendant moved frequently in the hopes of avoiding detection or capture, the fact that the defendant was expected to return several months later demonstrated that the subject premises was the defendant's primary residence for purposes of establishing probable cause to search that location).

Thus, with respect to premises search warrants, because child pornography crimes are "generally carried out in the secrecy of the home and over a long period," the caution to relate facts to the presently existing condition may be satisfied in cases where there is a lapse of time between information supporting probable cause and the date of search warrant application. *Frechette*, 583 F.3d at 378 (quoting

United States v. Paull, 551 F.3d 516, 522 (6th Cir. 2009) (referring to the defendant's home as a "secure operational base" from which he committed the crimes)).

IV. Examining adverse staleness dispositions in child pornography cases

In light of the fair probability standard and the staleness analysis, the great weight of authority suggests that in most circumstances a child pornography search warrant affidavit can be written to overcome staleness issues. In cases where courts have found a lack of probable cause on staleness grounds, the dispositions usually rest on the failure to develop corroborating facts, incorporate available supporting information, or otherwise update the initial probable cause facts.

For instance, in *United States v. Doan*, 245 F. App'x 550, 556 (7th Cir. 2007), the court held that information regarding the defendant's two seventeen-month-old subscriptions to child pornography Web sites was stale because the warrant affidavit failed to set forth information about the Web site or the defendant's activity, such as the duration of the defendant's subscriptions, the last date the defendant accessed the Web sites, whether the subscriptions allowed the defendant to download images, whether the defendant downloaded any images from the Web sites, or whether the defendant had a computer or Internet access at his home. *Id.* at 554. Rejecting probable cause for lack of an adequate factual basis, the court observed that "the older the information is regarding child pornography, the more necessary it is to include more detail concerning that information and concerning the person who is the subject of the investigation." *Id.* The court explained that "when aged information is minimal and when there is no additional information about the individual beyond the seventeen-month-old information, even taking the affidavit as a whole, there is no probable cause." *Id.*

In *United States v. Prideaux-Wentz*, 543 F.3d 954 (7th Cir. 2008), the court deemed stale four-year-old information regarding sixty-nine images of child pornography and erotica the defendant uploaded to eight Yahoo! e-groups and boilerplate profile information about child pornography collectors. *Id.* at 955. The court's ruling turned on its finding that although information that is four years old is not stale as a matter of law, the government failed to "freshen" the stale information with new evidence. *Id.* at 958. Specifically, the court pointed to the government's failure to obtain and include information about when the defendant uploaded the images even though this information was available from Yahoo!. *Id.* at 959. Therefore, the court found that "[t]he four year gap, without more recent evidence, undermine[d] the finding that there was probable cause that the images would be found during the search." *Id.*

V. Additional investigative steps for avoiding and rebutting staleness challenges

When dealing with a potentially problematic gap in time between the initial development of probable cause facts and the application for a search warrant, the case law provides several steps for prosecutors and law enforcement agents to take in order to bolster probable cause and obviate staleness concerns. The key is to present the historical facts that establish probable cause as well as updated information that demonstrates a continuing basis for probable cause at the time of the application for a search warrant.

A. Refresh information

In addition to the time it takes to develop probable cause facts, there is often additional time between the transfer of a search warrant from agency headquarters to a field office, the submission of a warrant application by a law enforcement agent to a United States Attorney's office, and the presentation

of the warrant application to a magistrate judge. One way to address this type of process-oriented delay is to use supplemental investigative or legal process to develop additional facts and incorporate those facts into the warrant application.

For example, in *United States v. Rabe*, 848 F.2d 994, 998 (9th Cir. 1988), the court rejected a staleness challenge because, in addition to two-year-old correspondence between the agent and the defendant, the search warrant application also included information regarding the agent's continued and more recent communications with the defendant. Likewise, in *United States v. Lemon*, 590 F.3d 612, 614 (8th Cir. 2010), probable cause rested largely on information regarding the defendant's December 2006 child pornography exchange. The search warrant was obtained in June 2008. The court rejected the defendant's staleness challenge because the investigating agent obtained evidence that the defendant's Internet Protocol Address and screen name were used in April 2008. The court found that this additional, contemporary information supported a fair probability that the defendant was still trading child pornography and would likely be maintaining the collection he was amassing. *Id.*

The *Doan* case, mentioned previously in section IV., provides another cautionary tale. In that case, the court deemed the warrant stale because it failed to include any facts that would "freshen" the defendant's two seventeen-month-old paid Web sites subscription information. Some of the facts that the court found lacking likely could have been obtained and included in the affidavit by serving an administrative subpoena on the defendant's Internet Service Provider(s) for information set forth in 18 U.S.C. § 2703(c)(2). Such information includes the name, address, local and long distance telephone connection records or records of session times and durations, length of service (including start date) and types of service utilized, subscriber number or identity, temporarily assigned network address, and means and source of payment for the service (including any credit card or bank account number).

B. Describe everything

The search warrant application must provide a factual basis for the determination that the defendant possessed, distributed, or received child pornography images and that evidence concerning that offense is likely to be found in the suspect's home and on the suspect's computer. If the investigation involves a commercial or other type of subscription or membership to a child pornography Web site, it is important to describe how membership or access is gained, to quote the web pages that explain the purpose of the Web site, to explain the membership or registration process and the evidence that indicates that the defendant engaged in that process, and to include evidence of subscription or membership such as credit card information or a confirmation page. It may also be critical to explain what the Web site offers (for example, fee-based downloads or free "sample" downloads) and the images that were available to be downloaded. Last but not least, a search warrant should describe the child pornography images likely to be found on the target's computer based on his suspected activity. Moreover, because determining whether an image qualifies as child pornography is a matter of law to be decided by the magistrate to whom the warrant is presented, the affidavit must set forth facts in sufficient detail to permit the magistrate to draw his own conclusion that the person depicted is a minor and that an image is child pornography.

With respect to minor status, when an affiant describes a child as pre-pubescent or assigns a minority age or range to a child depicted in an image (for example, "young female (8-10 YOA)"), that conclusion is generally sufficient for probable cause purposes. *See United States v. Battershell*, 457 F.3d 1048, 1054 (9th Cir. 2006) ("While a medical confirmation of the subject's age may be sufficient to establish probable cause absent an attached photograph, it is not necessary . . . we have accepted, for purposes of an affidavit in support of a search warrant, the conclusory age estimates made by civilians

and other untrained lay witnesses without demanding a detailed explanation of how the witnesses reached that conclusion."). However, the older a depicted child appears, the more likely it is that additional explanation may be required. *See United States v. Gatherum*, 338 F. App'x 271, 275 (4th Cir. 2009) ("While some 16- or 17-year-old models might be difficult to distinguish from 18-year-olds, the physical differences between a 12-year-old model and an 18-year-old model generally would be significant and readily apparent."). Even in those closer cases, "it [is] entirely reasonable for the magistrate to accept the officers' estimation of the child's age when determining whether probable cause existed." *Id*. at 275.

With respect to whether an image qualifies as child pornography, 18 U.S.C. § 2256(2)(A) provides five categories of "sexually explicit conduct," including actual or simulated: (1) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (2) bestiality; (3) masturbation; (4) sadistic or masochistic abuse; and (5) lascivious exhibition of the genitals or pubic area of any person. One court aptly described the first four categories of conduct as "easy to identify and describe" and "easily identifiable nouns that are not qualified by amorphous adjectives." *Battershell*, 457 F.3d at 1051, 1053; *see also United States v. Smith*, 795 F.2d 841, 848 (9th Cir. 1986) ("Although more specific descriptions of the photographs would have been desirable, we note that the affidavit specifically refers to violation of section 2251[, that the statute's] definitions are quite specific, and [that] the magistrate reasonably considered the statement of an experienced postal inspector that the photos depicted 'sexually explicit conduct' within the statute."). Accordingly, for the first four categories, simple reference to the statutory language is sufficient to allow a magistrate to determine whether an image is child pornography. *See Battershell*, 457 F.3d at 1053 ("Elaborate and detailed descriptions are unnecessary because '[a]ny rational adult person can recognize sexually explicit conduct engaged in by children under the age of 16 when he sees it.' ") (quoting *United States v. Hurt*, 808 F.2d 707, 708 (9th Cir. 1987)); *see also United States v. Mutschelknaus*, 592 F.3d 826, 828-29 (8th Cir. 2010) ("As a general matter, an issuing court does not need to look at the images described in an affidavit in order to determine whether there is probable cause that they constitute child pornography [because a] detailed verbal description is sufficient.") (internal quotations omitted).

In contrast, it is likely insufficient to simply reference the statutory language of the fifth category of conduct, "lascivious exhibition of the genitals or pubic area," without providing a detailed description of the image. For instance, in *United States v. Brunette*, 256 F.3d 14, 15 (1st Cir. 2001), the court found that affiant's affidavit description stating that an image "appeared to be within the statutory definition of child pornography, specifically, 'photographs of a pre-pubescent boy lasciviously displaying his genitals,' " was inadequate. The court in *Battershell* reached a similar conclusion. *Battershell*, 457 F.3d at 1051. In that case, an officer described a bathtub photograph simply as a "lascivious exhibition of the genitals or pubic area." The officer did not attach the image or provide more detailed description. Finding the description of that image insufficient to establish probable cause, the court explained that lasciviousness involves an "inherently subjective analysis" that requires supply of enough information for a magistrate to determine whether the image involves an exhibition of a minor's genital area. *Id.* The failure to provide an adequate description beyond the statutory language was fatal.

C. Support the scope of the warrant

Explaining the likelihood of collection and retention and the capabilities of forensic recovery will help establish probable cause that the evidence sought by the search warrant is likely to be in the places to be searched, even if significant time has passed between the acts giving rise to probable cause and the application for the search warrant. In this regard, the search warrant should include explanations regarding: (1) the affiant's specialized training in the area of child pornography and his knowledge,

based on his training and experience, that persons who receive, possess, or trade in child pornography tend to keep that material for extended periods; and (2) the capability of retrieving and recovering images and files from allocated and unallocated space even if those images have been corrupted, hidden, or inadvertently or intentionally deleted. The warrant should also explain how forensically recovered evidence that can be stored virtually anywhere on electronic media may help establish ownership, user identity, computer usage, and intent. If the investigation revealed consciousness of guilt evidence (for example, forum chats where the suspect advises others how to delete child pornography images from their computers or otherwise take steps to evade detection by law enforcement), those facts should be included in the warrant application as well.

D. Keep the information relevant

Suspect-specific information can obviate any concerns about using "boilerplate" language. All statements in the warrant should be applicable to the suspect. Incorporating information about characteristics that are common to the category of persons suspected of child pornography crimes in the warrant affidavit is not problematic so long as the affiant also explains in the affidavit why that "profile" applies to the suspect at issue. The more details about the investigation, the suspect, and the suspect's alleged criminal activity, the more reason there is to believe the suspect engaged in a child pornography offense and that evidence of that crime will be found at the place subject to the search.

E. Highlight and contextualize

Draw a full and complete picture of the suspect and the alleged criminal activity by emphasizing the relevant background facts and the range of conduct uncovered during the investigation. When dealing with aged information, fight the urge to over-edit. For example, if an investigation involves chat conversations between the suspect and the victim or other individuals, especially over an extended period, include samples of the most explicit chats, as well as chats that occurred over a wide range of dates to demonstrate the continuous nature of the criminal activity. Similarly, include emails, chats, or text messages where the suspect discusses his sexual interest in children or brags about committing contact offenses. *See United States v. Hay*, 231 F.3d 630, 634 (9th Cir. 2000) (affirming issuance of a search warrant where probable cause was predicated, in part, on the defendant's maintenance of a personal homepage where he discussed having access to children through volunteering with child-focused organizations and teaching and mentoring young children). This type of information, properly presented, belies staleness.

F. Assess and disclose the suspect's criminal history and dangerousness

Research the suspect's federal and state records and check with state and federal agencies to determine whether the suspect has prior criminal violations involving child sexual abuse, child pornography, and other sexual exploitation crimes, or has been a suspect in another similar federal or state investigation. Background investigation sources should include information maintained by the National Center for Missing and Exploited Children (NCMEC). In *United States v. Lapsins*, 570 F.3d 758 (6th Cir. 2009), the court held that information that was more than one year old was not stale because the affidavit was also supported by information from the NCMEC that the defendant had downloaded more than 100 images one month before the warrant was executed. *See id.* at 767 ("[NCMEC] information was reliable enough to contribute to a finding of probable cause, it remedied any potential staleness defect.").

State database checks should include the suspect's current state of residency as well as all other states in which the suspect has resided. If the state and federal checks reveal relevant prior offenses or involvement in other, similar investigations, this information should be included in the affidavit for the purpose of establishing a pattern of similar criminal activity that supports probable cause for the instant search warrant. In *Perrine*, the court rejected the defendant's challenge to the search warrant, in part, because it contained additional information regarding the defendant's previous state conviction in Kansas for exploitation of a child, his current probation for that offense, and because the prior offense involved the same activity under federal investigation. *Perrine*, 518 F.3d at 1205.

G. Associate the defendant's Internet activity to the subject premises

Use legal processes to associate the suspect's Internet activity to a computer and Internet capability at the premises subject to search. Although these steps usually occur during the investigation and well in advance of the presentation of the warrant to a magistrate, if there is a lapse in time, additional corroborative steps should be taken to establish probable cause that a computer was used in the commission of the child pornography offense, that the computer used to commit the crime is located at the suspect's residence, and that the residence has Internet service.

VI. Conclusion

Staleness challenges are a frequent feature of motions to suppress in child pornography cases and thus are a constant concern for federal prosecutors who must present and defend search warrants in these cases. Case law, however, shows that this often-asserted challenge need not be a serious obstacle in child pornography cases when investigative facts are presented fully, corroborated adequately, and updated appropriately at the time of search warrant application.

VII. Appendix: Circuit-by-circuit cases on staleness

A. First Circuit

Courts have approved search warrants based on information as old as three years. *See, e.g.*, *United States v. Wilder*, 526 F.3d 1 (1st Cir. 2008) (upholding a search warrant based on ten-month-old information and finding that the defendant's one-month subscription to a child pornography Web site, his four-year-old prior conviction for possession of child pornography, and his admission of collecting child pornography provided probable cause that the defendant had downloaded and preserved child pornography images on his computer from the Web site); *United States v. Morales-Aldahondo*, 524 F.3d 115 (1st Cir. 2008) (rejecting a staleness challenge to three-year-old information that the defendant subscribed to a commercial child pornography Web site because consumers of child pornography Web sites do not quickly dispose of their images); *United States v. Hanson*, 2007 WL 4287716, at *6 (D. Me. Dec. 5, 2007) (holding that sixth-month-old information that the defendant used Peer-to-Peer software to transmit a child pornography video was not stale because the defendant's activity indicated a continuing interest in child pornography that suggested that evidence of the crime would be found on his computer months after the offense was initially discovered).

B. Second Circuit

Courts in this jurisdiction have sanctioned search warrants based on information up to three years old. *See, e.g.*, *United States v. Irving*, 452 F.3d 110 (2d Cir. 2006) (twenty-three-month-old information not stale where sufficient information, evidence, and a prior conviction showed defendant to be a

pedophile who the court determined would be likely to hoard child pornographic images in his home for a long time); *United States v. Patt*, 2008 WL 2915433, at *12-13 (W.D.N.Y. July 24, 2008) (eight-month-old information not stale because the nature of downloading and collecting child pornography images and videos online, the relative short length of time between the computer activity and the warrant, and the capability of forensic experts to locate material on a computer that a user has "deleted" provided probable cause that the information would still be in defendant's possession); *United States v. Diaz*, 303 F. Supp. 2d 84 (D. Conn. 2004) (sixteen-month-old information not stale where the defendant sexually assaulted a minor and videotaped these incidents for two to three years, reasoning that individuals who engage in sexual activity with minors by using pornographic materials and other sexual aids retain these items for an extended time); *United States v. Cox*, 190 F. Supp. 2d 330 (N.D.N.Y. 2002) (three-year-old information suggesting that defendant collected child pornography was not stale because defendant was likely to retain the images of child pornography that he collected over a three-year period of time through his AOL account and where these images could be retrieved by a forensic computer analysis).

C. Third Circuit

In this jurisdiction, courts have approved search warrants based on information up to five years old. *See, e.g., United States v. Eberle*, 266 F. App'x 200 (3d Cir. 2008) (rejecting a staleness challenge to four-year-old information that suggested that the defendant sexually assaulted and videotaped a minor, even where the warrant application did not include evidence of child pornography on the defendant's computer, because individuals protect and retain child pornography for long periods of time and routinely save the files on other devices when they change computers); *United States v. Dennington*, 2009 WL 2591763 (W.D. Pa. Aug. 21, 2009) (five-year-old information that the defendant possessed a child pornography video of a nine-year-old boy was not stale where the age of the video was less significant because the defendant had continually manifested his sexual interest in molesting a minor boy and operated a fee-based Web site to offer images of himself a couple months prior to the search); *United States v. Worman*, 2008 WL 4093717, at *5 (E.D. Pa. Sept. 4, 2008) (three-year-old information that the defendant had sexually abused, photographed, and videotaped a minor girl and statements by the defendant that he would keep the password to his computer hidden and then pass it on to the minor victim upon his death were not stale where minor recently discovered nude photographs of her brother on the family computer).

D. Fourth Circuit

Courts in the Fourth Circuit have approved search warrants based on information up to six years old. *See, e.g., United States v. Ramsburg*, 114 Fed. App'x 78 (4th Cir. 2004) (six-year-old information that the defendant transmitted an image of child pornography not stale where the warrant application included facts about defendant's membership in two child pornography Internet groups that evidenced an interest in the material that was likely to still be on his computer); *United States v. Sassani*, 1998 WL 89875, at *5 (4th Cir. Mar. 4, 1998) (sixth-month-old information revealing that the defendant transmitted several images of child pornography provided sufficient grounds for probable cause); *United States v. Richardson*, 2008 WL 818863, at *6-7 (W.D.N.C. Mar. 21, 2008) (two to seventeen-month-old information not stale because the warrant included information that the defendant transmitted child pornography using his AOL email in June 2004 and September 2005, and had a criminal history of sex offenses involving children); *United States v. Sherr*, 400 F. Supp. 2d 843 (D. Md. 2005) (eight-month-old information indicating that the defendant received child pornography through his AOL account and that he expressed interest in trading nude pictures of preteens to an undercover agent online was not stale).

E. Fifth Circuit

Courts have approved search warrants based on information that was up to sixteen months old. *See, e.g., United States v. Silva*, 2009 WL 1606453, at *5-6 (W.D. Tex. June 8, 2009) (sixteen-month-old information that the defendant purchased and accessed child pornography Web sites not stale because those facts indicated that defendant had a sexual interest in children and would retain child pornography images for many years); *United States v. Young*, 2009 WL 440557, at *2-3 (E.D. Tex. Feb. 23, 2009) (five-month-old information that the defendant used his PayPal account to subscribe to fifteen child pornography Web sites not stale); *United States v. Winkler*, 2008 WL 859197, at *5-6 (W.D. Tex. Mar. 28, 2008) (ten-month-old information that defendant subscribed to a child pornography Web site not stale where warrant was corroborated by ISP information, including the date, time, and subscription addresses); *United States v. Rowell*, 2007 WL 106024, at *3 (N.D. Tex. Jan. 16, 2007) (rejecting a staleness challenge to five-month-old warrant information that the defendant successfully purchased membership to a child pornography Web site where court observed that collectors of child pornography ordinarily retain images for long periods and view images repeatedly rather than only on a single occasion).

F. Sixth Circuit

In this jurisdiction, courts have approved search warrants based on information up to three years old. *See, e.g., United States v. Noda*, 137 F. App'x 856, 862 (6th Cir. 2005) (informant information ranging from one week to three years old not stale where the affidavit set forth facts that defendant regularly sexually molested minors and viewed child pornography on his computer and there was evidence suggesting an ongoing pattern of criminal activity); *United States v. Shackleford*, 2007 WL 403627, at *6-7 (E.D. Ky. Feb. 1, 2007) (eight-month-old information that a screen name registered to defendant's roommate transmitted a sexually explicit image of a minor not stale because evidence of child pornography involving a computer significantly diminishes staleness concerns).

G. Seventh Circuit

Courts here have approved search warrants based on information up to four and a half years old. *See, e.g., United States v. Newsom*, 402 F.3d 780, 783 (7th Cir. 2005) (one-year-old information that defendant produced, possessed, and received child pornography not stale where facts suggested that defendant still had the year-old images or something similar on his computer and where informant recently discovered the clips of her daughter); *United States v. Costello*, 596 F. Supp. 2d 1060, 1065-66 (E.D. Mich. 2009) (thirteen-month-old information that defendant possessed child pornography not stale where defendant subscribed to a child pornography Web sites and had logged into the email account used to register with these Web sites three months prior to the execution of the search warrant); *United States v. Blum*, 2007 WL 5515298, at *2-4 (W.D. Wis. June 27, 2007) (four-and-a-half-year-old information that defendant produced child pornography not stale where defendant purchased a one-month membership to a child pornography Web site, where agents found evidence that linked defendant to another set of child pornography Web sites two years after this purchase though it was not completely clear that defendant visited these sites, and where agents found twelve cyber tips that defendant was listed as the registrant or owner of two child pornography Web sites).

H. Eighth Circuit

Courts have approved search warrants based on information up to two and a half years old. *See, e.g., United States v. Lemon*, 590 F.3d 612, 614-15 (8th Cir. 2010) (information supporting probable

cause for search warrant not stale even though eighteen months passed between exchange of pornography and search warrant application because the nature of defendant's crime, including his previous exchange of child pornography and statements during online chat room conversations expressing his interest in the same, supported categorization of defendant as a "preferential collector of child pornography"); *United State v. Johnson*, 2008 WL 465258, at *2 (D. Minn. Feb. 15, 2008) (eleven-month-old information that defendant subscribed to a child pornography Web site and downloaded nineteen images not stale where the investigation was ongoing during the eleven-month period because offenses involving the possession of child pornography are continuing in nature and minimizes the significance of when the information was obtained); *United States v. Fossum*, 2007 WL 2159502, at *7 (D. Minn. July 25, 2007) (two-year-old information that defendant possessed child pornography not stale where the more recent incidents of sexual abuse "freshened" the older observations by defendant's sons of child pornography on their father's computer).

I. Ninth Circuit

Courts within this circuit have approved search warrants based on information up to three years old. *See, e.g., United States v. Lacy*, 119 F.3d 742 (9th Cir. 1997) (ten-month-old information that defendant possessed child pornography not stale where defendant received child pornography from a foreign computer bulletin board system and downloaded at least two picture files containing child pornography and where court concluded that the nature of the crime suggested that the computerized visual depictions would be present in defendant's apartment ten months later); *United States v. Chase*, 2006 WL 2347726, at *4 (D. Nev. 2006) (three-year-old informant information that defendant gave him child pornography disks not stale where that defendant was paranoid about keeping child pornography on his home computer, kept images at work, and had a "wiping program," illustrating the ongoing nature of this criminal activity).

J. Tenth Circuit

Courts have approved search warrants based on information up to five years old. *See, e.g.*,

United States v. Riccardi, 405 F.3d 852 (10th Cir. 2005) (five-year-old information not stale where defendant had made several harassing phone calls of a sexual nature to teenage boys and possessed approximately 300 photographs of young men, including 50 to 80 images of child pornography, notes of telephone calls to young men, and a five-year old Kinko's receipt for converting print material into digital media).

K. Eleventh Circuit

In this jurisdiction, courts have upheld search warrants based on information up to two years old. *See, e.g., United States v. Toups*, 2007 WL 433562, at *1 (M.D. Ala. 2007) (two-year-old information that defendant transmitted approximately thirty electronic messages with attached child pornography images from his AOL account not stale in light of the unique nature of child pornography); *United States v. Miller*, 450 F. Supp. 2d 1321 (M.D. Fla. 2006) (four-month-old information that defendant downloaded and traded child pornography through Peer-2-Peer file sharing software not stale because individuals who possess and trade in child pornography tend to save the material they have downloaded for long periods of time).

L. District of Columbia Circuit

To date neither the District Court for the District of Columbia or the D.C. Circuit has issued a published or unpublished decision regarding staleness in a child pornography case.❖

ABOUT THE AUTHOR

❑**Chantel Febus** is Trial Attorney in the Child Exploitation and Obscenity Section of the Criminal Division of the U.S. Department of Justice. In this role, she assists in the enforcement and prosecution of violations of federal criminal statutes involving all aspects of child sexual exploitation, such as child pornography offenses, enticement or traveler offenses, sex tourism offenses, and child prostitution. She also advises on the development of prosecution and enforcement policies, legislation, and federal agency regulations in the areas of child sexual exploitation. Ms. Febus has also presented numerous lectures on topics relating to child exploitation and has authored three articles for the Criminal Division, Child Exploitation and Obscenity Section Newsletter.✠

The author would like to acknowledge the assistance of Jason Claude and Kimberly Singer, Legal Interns, in the preparation of this article.

SORNA: A Primer

Bonnie Kane
Trial Attorney
Child Exploitation and Obscenity Section

I. Introduction

On July 27, 2006, the Sex Offender Registration and Notification Act (SORNA) was enacted as Title I of the Adam Walsh Child Protection and Safety Act of 2006, Pub. L. 109–248, 120 Stat. 587, 42 U.S.C. §§ 16901 - 62 (2006). SORNA established "a comprehensive national system for the registration of [sex] offenders" to harmonize the existing patchwork of registration laws that existed under both federal and state laws across the country. *Id*. § 16901. Under existing registration schemes, many sex offenders were "lost" based on the transient nature of sex offenders and the inability of states to track offenders after they crossed state lines. *See* H.R. Rep. No. 109-218, pt. 1 (2005).

The purpose of SORNA is twofold: (1) it created direct registration requirements for all sex offenders that are federally enforceable under certain circumstances; and (2) it created grant-related incentives for "jurisdictions" to adopt and "substantially implement" minimum national standards under their laws for sex offender registration and notification. 42 U.S.C. §§ 16912(a), 16913(a), 16925(a) (2010); 18 U.S.C. § 2250 (2010). Under SORNA, jurisdictions consist of the fifty states, the District of Columbia, and certain U.S. territories and Indian tribes. 42 U.S.C. § 16911(10) (2010).

This article addresses SORNA's direct registration requirements for sex offenders and the federal criminal enforcement of these requirements by 18 U.S.C. § 2250. Prosecutors should understand SORNA, because effective enforcement of its obligations assists law enforcement in the investigation of new sex offenses by recidivist sex offenders and may deter the commission of new offenses by such offenders. Further, a § 2250 violation may be the basis for an initial and prompt charge at the outset of an investigation where a sex offender is alleged to have committed another sex offense.

II. What guidance exists regarding SORNA's requirements?

The Attorney General issued The National Guidelines for Sex Offender Registration and Notification (Guidelines), 73 Fed. Reg. 38030 (Jul. 2, 2008), and the Supplemental Guidelines for Sex Offender Registration and Notification (Supplemental Guidelines), 76 Fed. Reg. 1630 (Jan. 11, 2011). The Guidelines and Supplemental Guidelines provide detailed guidance on, and interpretations of, SORNA's requirements in order to advise jurisdictions of what they must do to "substantially implement" those requirements in their sex offender registration and notification programs. 42 U.S.C. § 16925(a) (2010). Although the Guidelines and Supplemental Guidelines are expressly addressed to the jurisdictions, the guidance and interpretations contained therein are highly relevant to the United States' position regarding those statutory provisions of SORNA that are directed to individual sex offenders.

III. Who is subject to SORNA's registration requirements?

SORNA requires sex offenders to register and defines "sex offender" as an individual who was convicted of a "sex offense," including certain federal, state, local, tribal, foreign, and military offenses, and attempts or conspiracies to commit such offenses as well. 42 U.S.C. §§ 16911(1), (5)(A)(v), (6) (2010). In its definition of "sex offense," SORNA provides an enumerated but non-exclusive list of

qualifying federal offenses, such as those under chapters 109A and 117 of Title 18 of the United States Code. *Id.* § 16911(5)(A)(iii). *See United States v. Dodge*, 597 F.3d 1347, 1352-53 (11th Cir. 2010) (SORNA's definition of "sex offense" includes the non-enumerated federal offense of 18 U.S.C. § 1470, which prohibits the transfer of obscene material to a minor). SORNA's definition of sex offense also includes certain military offenses, criminal offenses that have "an element involving a sexual act or sexual contact with another," and any criminal offense that is a "specified offense against a minor." *Id.* § 16911 (5)(A)(i), (ii), (iv). SORNA further defines "specified offense against a minor" to include offenses against a minor that involve particular conduct, such as engaging in or soliciting sexual conduct involving minors and child pornography offenses. *Id.* § 16911(7). The phrase also includes those offenses that fall within the catchall provision of "any conduct that by its nature is a sex offense against a minor." *Id.*

With respect to juvenile offenders, SORNA requires individuals who have been "adjudicated delinquent" for certain serious sex offenses to comply with registration requirements if they were fourteen years of age or older at the time of the offense. *Id.* § 16911(8). SORNA requires the juvenile's registration if his sex offense is comparable to or more severe than a federal aggravated sexual abuse offense as set forth in 18 U.S.C. § 2241, or is an attempt or conspiracy to commit such an offense. *Id.*

For offenses involving consensual sexual conduct, SORNA does not require registration if the victim was at least thirteen years old and the offender was not more than four years older than the victim. *Id.* § 16911(5)(C). For example, if the consenting victim was fifteen years old and the offender was eighteen years old, SORNA would not require the offender's registration. However, if the consenting victim was exactly fourteen years old and the offender was eighteen-and-a-half years old, SORNA would require the offender's registration because the offender was more than four years older than the victim. SORNA also does not require registration for consensual sexual conduct offenses involving adult victims, unless the victim was under the offender's custodial authority. Thus, for example, most adult prostitution offenses involving consensual sexual conduct do not require registration under SORNA.

A limited number of courts have addressed what information may be considered in determining whether an offense of conviction is a "sex offense" that requires registration. With respect to criminal offenses that have "an element involving a sexual act or sexual contact with another," SORNA on its face restricts the analysis to consideration of the elements of the crime, that is, a categorical approach. *Id.* § 16911(5)(A)(i). However, within the "specified offense against a minor" definition of "sex offense," SORNA makes no reference to the elements of the offense. *See id.* § 16911(5)(A)(ii). In *United States v. Byun*, 539 F.3d 982, 992 (9th Cir. 2008), with respect to a "specified offense against a minor," the court adopted a non-categorical approach regarding the limited issue of the victim's age where the offense of conviction did not include the victim's age as an element. After considering the offense's underlying facts in the plea agreement, the court held that the defendant's offense of importation of an alien for purposes of prostitution was a "specified offense against a minor" based on the victim's age and thus constituted a "sex offense" requiring registration. *Id.* at 993-94.

In *United States v. Dodge*, 597 F.3d 1347 (11th Cir. 2010), the Eleventh Circuit adopted a non-categorical approach that permits examination of the "underlying facts of a defendant's offense, to determine whether a defendant has committed a 'specified offense against a minor.' " *Id.* at 1356. Through review of the defendant's plea colloquy, the court found that the circumstances of the defendant's violation of 18 U.S.C. § 1470 fell within the catchall category of "conduct that by its nature is a sex offense against a minor," regarding which the court concluded that Congress had "left courts with broad discretion." *Id.* at 1355-56.

IV. When did SORNA's requirements become effective?

SORNA's general rule is that sex offenders are required to register before completing their sentences of imprisonment for the qualifying offense or, if the sex offender was not sentenced to a term of imprisonment, he must register no later than three business days after being sentenced for the qualifying offense. 42 U.S.C. § 16913(b) (2010). This general rule, however, does not in itself resolve questions that have arisen in practice as to when sex offenders with past convictions (and often previous registrations) must now register or face criminal liability under 18 U.S.C. § 2250 for failing to comply with SORNA's requirements. The effective date of SORNA's requirements for this purpose has been the subject of extensive litigation and divergent judicial decisions. In general, for offenders whose qualifying sex offense convictions were obtained before SORNA's enactment, courts have held that the effective date of registration obligations was either July 27, 2006 (the date of SORNA's enactment), February 28, 2007 (the date that the Attorney General issued the interim rule Applicability of the Sex Offender Registration and Notification Act, 72 Fed. Reg. 8894 (2007)), or August 1, 2008 (the date that the Guidelines to the jurisdictions became effective).

On January 24, 2011, the U.S. Supreme Court granted certiorari in *Reynolds v. United States*, 131 S. Ct. 1043 (2011). This case appears likely to resolve the existing circuit split regarding SORNA's effective date. Until the Supreme Court's decision in *Reynolds* is published, prosecutors are encouraged to review the case law in their circuits in order to determine the applicable effective date of SORNA in their circuits. *See United States v. Johnson*, 632 F.3d 912, 922 (5th Cir. 2011); *United States v. Valverde*, 628 F.3d 1159, 1162-65 (9th Cir. 2010); *United States v. Fuller*, 627 F.3d 499, 501 (2d Cir. 2010); *United States v. DiTomasso*, 621 F.3d 17, 22-25 (1st Cir. 2010); *United States v. Dean*, 604 F.3d 1275, 1278-82 (11th Cir. 2010); *United States v. Utesch*, 596 F.3d 302, 306-09 (6th Cir. 2010); *United States v. Shenandoah*, 595 F.3d 151, 157 (3d Cir. 2010); *United States v. Cain*, 583 F.3d 408, 419-24 (6th Cir. 2009); *United States v. Young*, 585 F.3d 199, 201 (5th Cir. 2009); *United States v. Gould*, 568 F.3d 459, 469-70 (4th Cir. 2009); *United States v. Hatcher*, 560 F.3d 222, 226-29 (4th Cir. 2009); *United States v. Dixon*, 551 F.3d 578, 582 (7th Cir. 2008), *rev'd on other grounds, sub nom. Carr v. United States*, 130 S. Ct. 2229 (2010); *United States v. Hinckley*, 550 F.3d 926, 929-35 (10th Cir. 2008); *United States v. May*, 535 F.3d 912, 918-19 (8th Cir. 2008).

V. How long are sex offenders required to be registered under SORNA?

Sex offenders are required to keep their registrations current for their "full registration period," the length of which is determined by their "tier" status. 42 U.S.C. § 16915(a) (2010). SORNA divides sex offenders into three tiers and assigns a different registration period to each tier. *Id.* Tier III sex offenders are required to register for life. *Id.* § 16915(a)(3). Tier III sex offenders include certain recidivist sex offenders and individuals who have been convicted of the most serious sex offenses, such as felony offenses involving aggravated sexual abuse, sexual abuse, sexual contact with victims below the age of thirteen, or kidnapping of minors. *Id.* § 16911(4). Tier II sex offenders are required to register for twenty-five years. *Id.* § 16915(a)(2). Tier II sex offenders are certain recidivist sex offenders and individuals who have been convicted of most felony sex offenses against minors, including production or distribution of child pornography. *Id.* § 16911(3). Tier I sex offenders are required to register for fifteen years. *Id.* § 16915(a)(1). Tier I sex offenders include all other sex offenders whose qualifying sex offenses do not meet the criteria for Tier II or Tier III. *Id.* § 16911(2). Such sex offenses include the receipt and possession of child pornography and misdemeanor sex offenses. Guidelines, 73 Fed. Reg. 38030, 38053. SORNA also contains a "clean record" provision that allows, in specified circumstances, for the reduction of the registration periods for Tier I sex offenders and Tier III sex offenders if their sex offenses were based on juvenile delinquency adjudications. *Id.* § 16915(b).

The Guidelines provide that in determining the applicable tier for a sex offense, "jurisdictions generally may premise the determination on the elements of the offense, and are not required to look to underlying conduct that is not reflected in the offense of conviction," excepting the age of the victim. Guidelines, 73 Fed. Reg. 38030, 38053. However, for purposes of determining a sex offender's tier under federal law, the analysis may differ if the courts, as in *United States v. Dodge*, 597 F.3d 1347, 1356 (11th Cir. 2010) (permitting examination of the underlying facts of a defendant's offense), rely on a non-categorical approach to determine whether an offense of conviction is a "sex offense" that requires registration.

VI. Where is registration required?

If a sex offender is required to register under SORNA, he must "register . . . in each jurisdiction where the offender resides, where the offender is an employee, and where the offender is a student." 42 U.S.C. § 16913(a) (2010). Following their sex offense convictions, sex offenders who are sentenced to probation or due to be released from prison also must initially register in the jurisdictions that they are convicted in, even if they have no intention of staying in these jurisdictions. *Id.* § 16913(a). This requirement to register in the jurisdiction of conviction is not applicable to sex offenders who were sentenced to probation or released from prison prior to SORNA's enactment.

SORNA defines the term "resides" as "the location of the individual's home or other place where the individual habitually lives." *Id.* § 16911(13). The Guidelines state that the phrase " 'habitually lives' . . . is not self-explanatory and requires further definition," and provides:

> "Habitually lives" accordingly should be understood to include places in which the sex offender lives with some regularity, and with reference to where the sex offender actually lives, not just in terms of what he would choose to characterize as his home address or place of residence for self-interested reasons. The specific interpretation of this element of "residence" these Guidelines adopt is that a sex offender habitually lives in the relevant sense in any place in which the sex offender lives for at least 30 days. Hence, a sex offender resides in a jurisdiction for purposes of SORNA if the sex offender has a home in the jurisdiction, or if the sex offender lives in the jurisdiction for at least 30 days. Jurisdictions may specify in the manner of their choosing the application of the 30-day standard to sex offenders whose presence in the jurisdiction is intermittent but who live in the jurisdiction for 30 days in the aggregate over some longer period of time.

73 Fed. Reg. 38030, 38061-38062.

The issue of whether a sex offender "habitually lives" in a jurisdiction arises frequently in the context of itinerant or homeless offenders. In *United States v. Voice*, 622 F.3d 870, 874 (8th Cir. 2010), the defendant sex offender asserted that he had not changed his registered residence and that he was on a trip visiting friends and family for approximately two months. The evidence at trial showed that the defendant had violated his supervised release conditions by leaving a halfway house and then staying at various locations on an Indian reservation for short periods of time, including a stint on a cement slab outside of a building. While the defendant had registered the address of the halfway house, he did not register any of his Indian reservation addresses or locations. The court found that sufficient evidence was available for the jury to conclude that the defendant was "habitually" living at the reservation and rejected "the suggestion that a savvy sex offender can move to a different city and avoid having to update his SORNA registration by sleeping in a different shelter or other location every night." *Id.* at 874-75.

If a sex offender is an employee and/or a student in a different jurisdiction than the one he resides in, SORNA requires sex offenders to register in each of those jurisdictions as well. SORNA defines "employee" to include an "individual who is self-employed or works for any other entity, whether compensated or not" and "student" as an "individual who enrolls in or attends an educational institution, including (whether public or private) a secondary school, trade or professional school, and institution of higher education." 42 U.S.C. §§ 16911(11), (12) (2010). Thus, if a sex offender resides in one jurisdiction but is employed in a different jurisdiction and also attends school in yet another jurisdiction, he is required to register in all three jurisdictions.

At the time of SORNA's enactment, every state had a sex offender registration system in place. SORNA depends on these existing state, tribal, and territorial registries as the physical locations where sex offenders register and update their registrations. *Id.* § 16911(9); *Carr v. United States*, 130 S. Ct. 2229, 2238 (2010) ("[F]ederal sex-offender registration laws have, from their inception, expressly relied on state-level enforcement."). Despite SORNA's use of jurisdictions' existing registration mechanisms, "the registration requirements for sex offenders are neither conditioned on nor harnessed to state implementation of SORNA's state-directed mandate." *United States v. DiTomasso*, 621 F.3d 17, 27 (1st Cir. 2010).

Should a jurisdiction fail to "substantially implement" SORNA's minimum standards within the requisite period, the jurisdiction faces the recurring loss of ten percent of the funds that would otherwise be allocated to the jurisdiction each fiscal year under the Edward Byrne Memorial Justice Assistance Grant Program, 42 U.S.C. § 3750 - 3758 , until compliance is achieved. 42 U.S.C. § 16925(a) (2010). However, any non-compliance by a jurisdiction does not excuse the failure of sex offenders within its boundaries to abide by their SORNA obligations. As stated in *DiTomasso*, 621 F.3d at 27, "as long as a state maintains a registration mechanism for sex offenders, what the state does or does not do with respect to implementing its state-specific obligations under SORNA is not relevant to a sex offender's obligation to register." *See also United States v. Guzman*, 591 F.3d 83, 93 (2d Cir. 2010) ("SORNA creates a federal duty to register with the relevant existing state registries regardless of state implementation of the specific additional requirements of SORNA."). Even though SORNA may require a sex offender to register in a jurisdiction, the existing laws of that jurisdiction may not require his registration. In such circumstances, the jurisdiction could refuse to accept the offender's registration.

VII. What information does SORNA require sex offenders to provide in their registrations?

In order to comply with SORNA's registration requirement, sex offenders must provide all of the following information to the sex offender registry in all jurisdictions that he is required to register in:

- The name of the sex offender (including any alias used by the individual).
- The Social Security number of the sex offender.
- The address of each residence that the sex offender resides in or will reside in.
- The name and address of any place where the sex offender is an employee or will be an employee.
- The name and address of any place where the sex offender is a student or will be a student.
- The license plate number and a description of any vehicle owned or operated by the sex offender.

- Any other information required by the Attorney General.

42 U.S.C. § 16914(a) (2010).

Further, in the Guidelines and Supplemental Guidelines, the Attorney General has exercised his authority under 18 U.S.C. § 16914(a)(7) to require jurisdictions to implement several additional requirements for sex offenders. These additional requirements include, among other things, reporting information related to temporary lodging, intended international travel, and intended commencement of residence, employment, or school attendance outside the United States. *See* Guidelines, 73 Fed. Reg. 38030, 38056, 38066-38067; Supplemental Guidelines, 76 Fed. Reg. 1630, 1637-1638. However, the formulation of the Guidelines and Supplemental Guidelines as directions to jurisdictions that may or may not implement them creates difficulties in attempting to enforce these additional requirements against sex offenders through prosecution under 18 U.S.C. § 2250.

SORNA also requires sex offenders to keep their registration information "current." 42 U.S.C. § 16913(a) (2010). Thus, after "each change of name, residence, employment, or student status," SORNA requires sex offenders to "appear in person in at least 1 jurisdiction involved" and "inform that jurisdiction of all changes in the information required for that offender in the sex offender registry." *Id.* § 16913(c). Section 16913(c) allows up to three business days for a sex offender to provide this information. After a sex offender registers or updates registration in one jurisdiction, that jurisdiction is then required to provide the sex offender's information to "[e]ach jurisdiction where the sex offender resides, is an employee, or is a student, and each jurisdiction from or to which a change of residence, employment, or student status occurs." *Id.* § 16921(b)(3).

Under SORNA, a sex offender may move out-of-state without informing the sex offender registry in the jurisdiction that he is departing. However, the Guidelines and most jurisdictions require notification before the offender's departure. Such a sex offender has up to three business days to register at the sex offender registry in his new jurisdiction. The registry in the new jurisdiction is then responsible for informing the registry in the sex offender's former jurisdiction of the sex offender's departure. *Id.* § 16921(b)(3). However, if a sex offender terminates his residence in a jurisdiction with no intention of returning and no plans to establish a new residence elsewhere, that is, he is not going to register in a new jurisdiction within the requisite period, the offender must "appear" and notify the sex offender registry in the jurisdiction that he is departing from and inform that jurisdiction of his "change" in residence within three business days. *Id.* § 16913(c); *see also United States v. Van Buren*, 599 F.3d 170, 174-75 (2d Cir. 2010) ("[I]t is clear that a registrant must update his registration information if he alters his residence such that it no longer conforms to the information that he earlier provided to the registry.").

SORNA further requires sex offenders to periodically appear in person at their registries and "verify" their registration information even if the information has not changed. 18 U.S.C. § 16916 (2010). At such time, sex offenders also must permit their jurisdictions to take current photographs of them. *Id.* The frequency of these in-person appearance requirements depends on the tier of the sex offender: each year for Tier I sex offenders; every six months for Tier II sex offenders; and every three months for Tier III sex offenders. *Id.*

VIII. How are SORNA's registration requirements enforced?

Sex offenders who knowingly fail to comply with SORNA's requirements are subject to federal prosecution under 18 U.S.C. § 2250(a). Section 2250(a) provides:

> Whoever—
>
> (1) is required to register under the Sex Offender Registration and Notification Act;
>
> (2)(A) is a sex offender as defined for the purposes of the Sex Offender Registration and Notification Act by reason of a conviction under Federal law (including the Uniform Code of Military Justice), the law of the District of Columbia, Indian tribal law, or the law of any territory or possession of the United States; or
>
> (B) travels in interstate or foreign commerce, or enters or leaves, or resides in, Indian country; and
>
> (3) knowingly fails to register or update a registration as required by the Sex Offender Registration and Notification Act;
>
> shall be fined under this title or imprisoned not more than 10 years, or both.

18 U.S.C. § 2250(a) (2010).

Sex offenders who violate § 2250(a) face a maximum sentence of ten years in prison. *Id.* If the sex offender also commits a federal crime of violence during his failure to register status, he may be additionally charged with violating § 2250(c) and face an additional five to thirty years of imprisonment that would run consecutive to his § 2250(a) sentence. *Id.* at § 2250(c).

IX. In what order must the three elements of § 2250(a) occur?

Pursuant to § 2250(a), SORNA's requirements are enforced against two classes of sex offenders: (i) individuals who are sex offenders based on a conviction under federal, District of Columbia, Indian tribal, or U.S. territorial law, *see* § 2250(a)(2)(A); and (ii) individuals who are sex offenders based on convictions under state or foreign law, that is, "non-federal sex offenders." For sex offenders in the latter class, federal jurisdiction to prosecute their SORNA violations usually depends on the travel requirement appearing in § 2250(a)(2)(B). With regard to prosecuting these non-federal sex offenders, the Supreme Court in *Carr v. United States*, 130 S. Ct. 2229 (2010), held that § 2250(a) is not violated if the offender's travel occurred before SORNA became effective. *Id.* at 2236, 2242. Because of that decision, it is now understood that when prosecuting non-federal sex offenders, § 2250(a)'s three elements must occur in sequence. Specifically, the court stated that "[o]nce a person becomes subject to SORNA's registration requirements, which can occur *only after* the statute's effective date, that person can be convicted under § 2250 if he *thereafter* travels and *then* fails to register." *Id.* at 2236 (emphasis added).

Thus, a non-federal sex offender, whose qualifying sex offense conviction occurred prior to SORNA's enactment, can violate § 2250(a) only if he is, first, "required to register under the Sex Offender Registration and Notification Act," which depends on SORNA's effective date, an issue that has produced a split in court opinions. *See supra* Part IV. 18 U.S.C. § 2250(a)(1) (2010). Second, the non-federal sex offender must then "travel[] in interstate or foreign commerce, or enter[] or leave[], or reside[] in, Indian country." *Id.* § 2250(a)(2)(B). Third, he must subsequently "knowingly fail[] to register or update a registration." *Id.* § 2250(a)(3).

X. What is the mens rea requirement in § 2250(a)'s third element?

In § 2250(a) prosecutions the United States must prove that the defendant knowingly failed to register or update his registration; that is, the defendant knew he was required to register or update his registration and failed to do so. However, the United States does not need to prove that the defendant

knew his registration obligations were mandated by federal law. *United States v. Vasquez*, 611 F.3d 325, 328-29 (7th Cir. 2010). In *Vasquez*, the Seventh Circuit joined several other courts in holding that "a defendant can be convicted under SORNA if the government can prove that he knew he was required to register as a sex offender" under state law and that proof of the defendant's "knowledge of the federal obligation under SORNA is not required." *Id. See also United States v. Griffey*, 589 F.3d 1363, 1367 (11th Cir. 2009); *United States v. Whaley*, 577 F.3d 254, 262 (5th Cir. 2009); *United States v. Gould*, 568 F.3d 459, 468 (4th Cir. 2009); *United States v. Baccam*, 562 F.3d 1197, 1199-1200 (8th Cir. 2009).

Furthermore, although SORNA requires that sex offenders be notified of their federal registration obligations under § 16917, the United States does not need to prove that a defendant received such notice. *See, e.g., United States v. Fuller*, 627 F.3d 499, 507-08 (2d Cir. 2010); *Baccam*, 562 F.3d at 1199-1200. Prosecutors may thus rely on evidence of defendant's awareness of his registration obligations under state or local law, such as signed registration or notification forms acknowledging that he was required to register under state or local law. *Baccam*, 562 F.3d at 1199-1200 ("There is no reason to believe that the SORNA notice provision in § 16917 was intended to dilute the effect of state notice requirements, given the stated congressional intent to protect the public by establishing a comprehensive national system for registration of sex offenders.").

In *Vasquez*, the Seventh Circuit identified a possible mens rea issue in cases where a difference exists between the registration requirements imposed on a defendant under federal and state laws. *See Vasquez*, 611 F.3d at 329. The court noted that a situation may arise where a defendant complied with his state law registration obligations but not his different federal registration obligations and where he had not been made aware of the additional obligations under the federal statute. The court declined to address what evidence would be needed to satisfy the mens rea requirement in such cases. *Id.* Accordingly, the status of a jurisdiction's implementation of SORNA and the differences between a jurisdiction's registration laws and SORNA may be relevant to determining and proving the defendant's knowledge of his registration obligations.

XI. How does a sex offender fail to register or update a registration as required by SORNA?

A clear statutory symmetry and correlation exists between SORNA's civil requirements to "register, and keep the registration current" under § 16913(a) and § 2250(a)'s penalization of a failure to "register or update a registration." *See United States v. Gould*, 568 F.3d 459, 463 (4th Cir. 2009) ("The requirement [in § 2250(a)] to 'register or update a registration' is imposed by SORNA [42 U.S.C. § 16913(a)], which provides: 'A sex offender shall register, and keep the registration current, in each jurisdiction where the offender resides, where the offender is an employee, and where the offender is a student.' "). Thus, in general, a sex offender "fails to register" if he does not "register" the information required to be provided by § 16914(a) in "each jurisdiction where the offender resides, where the offender is an employee, and where the offender is a student." 42 U.S.C. § 16913(a) (2010).

Although § 2250(a) uses the phrase "update a registration" instead of SORNA's phrase "keep the registration current" in § 16913, it is plain that their meanings are synonymous in the context of the interrelated statutory schemes. Courts addressing these related civil and criminal provisions have assumed the phrases' meanings to be one and the same. *See, e.g., United States v. Heth*, 596 F.3d 255, 258 (5th Cir. 2010) ("To maintain the currentness of registration, sex offenders must update their registration within three business days of a 'change of name, residence, employment, or student status.' ") (citing 42 U.S.C. § 16913(c)); *United States v. Hester*, 589 F.3d 86, 90 (2d Cir. 2009) ("[I]ndividuals who have been convicted of a sex offense . . . must keep his or her registration current by updating the

relevant jurisdiction after each change of name, residence, employment, or student status.") (citing 42 U.S.C. § 16913); *United States v. Brown*, 586 F.3d 1342, 1348 (11th Cir. 2009) ("In order to keep one's registration 'current,' a sex offender must update his registry information in at least one jurisdiction involved in [42 U.S.C. § 16913(a)] . . . ").

Thus, in order to avoid prosecution under § 2250(a), a registered sex offender must "keep the registration current" by ensuring that the existing required information is accurate and complete and, if otherwise, to "update" accordingly. 42 U.S.C. § 16913(a) (2010); 18 U.S.C. § 2250(a)(3) (2010). Regardless of whether a sex offender's registration information has changed, his failure to comply with SORNA's periodic in-person appearance requirement is logically regarded as a failure to "update a registration as required by [SORNA]." 18 U.S.C. § 2250(a)(3) (2010). This is because periodically verifying the current accuracy of the registration information and allowing a photograph of the sex offender to be taken for documentation of their current appearance are part of SORNA's requirements for keeping a registration up to date. *See* 42 U.S.C. § 16916 (2010).

Importantly, a sex offender's failure to comply with his jurisdiction's registration laws (for example, state or tribal registration laws) alone does not subject the offender to federal prosecution under § 2250(a). Section 2250(a)'s third element requires the sex offender's violation of SORNA's requirements, which may differ from a jurisdiction's laws even following the jurisdiction's "substantial implementation" of SORNA. SORNA only created minimum registration standards for jurisdictions and, accordingly, jurisdictions are free to create additional requirements such as registration by a broader class of offenders or longer periods of registration. In circumstances where a sex offender has complied with SORNA but violated an additional and more stringent state registration requirement, his violation of that state requirement may only be prosecuted by the state.

XII. When does a sex offender's § 2250(a) offense end?

A sex offender's failure to register or update a registration as required by SORNA is a continuing offense. *United States v. George*, 625 F.3d 1124, 1131 (9th Cir. 2010) (finding defendant to be under a continuing obligation to register and interpreting the violation of the sex offender registration requirement as a "continuing offense"); *United States v. Hinckley*, 550 F.3d 926, 936 (10th Cir. 2008) ("An interpretation of the sex offender registration requirement that defines it in any way other than as a continuing offense would result in absurdity."); *but see United States v. Stinson*, 507 F. Supp. 2d 560, 569-70 (S.D. W.Va. 2007) (finding that a violation of § 2250(a) is not a continuing offense because nothing in the express language of § 16913(b) or (c) imposes a continuing duty to register or update a registration if the offender fails to do so within three business days). That is, a sex offender continues to violate § 2250(a) until he is arrested or complies with SORNA's registration requirements. *United States v. Pietrantonio*, 637 F.3d 865, 869-70 (8th Cir. 2011) (defendant's failure to register offense stopped when he untimely registered in his new jurisdiction).

XIII. Where is a § 2250(a) offense properly venued?

Venue for § 2250(a) offenses is often appropriate in more than one district. The most common scenario for § 2250(a) offenses involves a sex offender's change of residence from one state to another. In such circumstances, the offender is required to update his registration in "at least 1 jurisdiction involved." 42 U.S.C. § 16913(c) (2010). If he fails to register in the new jurisdiction and fails to update his existing registration in the departed jurisdiction, the offender's registration in the departed jurisdiction is no longer current or accurate and the new jurisdiction that he is residing in has no registration information at all.

When determining the appropriate venue for such an offense, courts have relied on 18 U.S.C. § 3237(a), providing that any offense "begun in one district and completed in another, or committed in more than one district may . . . be prosecuted in any district in which such offense was begun, continued, or completed." *See, e.g.*, *United States. v. Leach*, 639 F.3d 769, 771-72 (7th Cir. 2011) (stating that venue was proper in the Northern District of Indiana even though the offender was arrested in South Carolina because the defendant did not update his Indiana registration after leaving the state). The Supreme Court stated that the offender's travel in such cases is "the very conduct at which Congress took aim," *Carr v. United States*, 130 S. Ct. 2229, 2240 (2010), and thus the offense begins in the jurisdiction from which the offender departed.

Accordingly, venue is proper in either the former district of residence or the district to which the sex offender travels. *Leach*, 639 F.3d at 772 ("Venue was proper in Indiana, as it would have been in South Carolina if the government had opted to prosecute there."); *United States v. Howell*, 552 F.3d 709, 717-18 (8th Cir. 2009) ("A [non-federal] sex offender violates SORNA only when he or she moves between states [and, t]hus, a SORNA violation involves two different jurisdictions."); *United States v. Thompson*, 595 F. Supp. 2d 143, 148-49 (D. Me. 2009) (holding that venue was proper in either Maine or New Mexico because "when Mr. Thompson traveled in interstate commerce, he failed to update his registration in Maine, the state he left, and failed to register in New Mexico, the state he traveled to").

Section 3237(a) further provides in relevant part that "[a]ny offense involving . . . transportation in interstate or foreign commerce . . . is a continuing offense and, except as otherwise expressly provided by enactment of Congress, may be inquired of and prosecuted in any district from, through, or into which such . . . person moves." In *United States v. Young*, 582 F. Supp. 2d 846, 849 (W.D. Tex. 2008), the court found that "the federal rules and the general venue statute in conjunction with § 2250 establish a continuing offense so that venue is proper in any district in which a defendant has moved."

Thus, a sex offender who travels in interstate commerce and fails to register and/or update his registration as required within the requisite period has committed a § 2250(a) offense. As previously discussed, this § 2250(a) offense then "continues" until the offender is either arrested or registered in an appropriate jurisdiction. *United States v. Pietrantonio*, 637 F.3d 865, 869-70 (8th Cir. 2011). Therefore, pursuant to § 3237(a), the offender may arguably be prosecuted for his continuing § 2250(a) offense in any district that he travels through or into while in this unregistered status, regardless of whether he intends to or has commenced residence therein.

XIV. What defenses to § 2250(a) are available to sex offenders?

Section 2250(b) expressly provides that "[i]n a prosecution for a violation under [§ 2250(a)]" the following is an affirmative defense:

> (1) uncontrollable circumstances prevented the individual from complying;
>
> (2) the individual did not contribute to the creation of such circumstances in reckless disregard of the requirement to comply; and
>
> (3) the individual complied as soon as such circumstances ceased to exist.

Id.

This affirmative defense may be encountered in circumstances where SORNA requires a sex offender to register but where the jurisdiction has not yet implemented SORNA and under its existing registration laws the sex offender may not be required to register. In these instances, as previously

discussed, the sex offender is still required to register and/or attempt to register, but if the jurisdiction refuses to accept his registration, the offender would have a viable defense under § 2250(b).

XV. Conclusion

SORNA created direct registration requirements for both federal and non-federal sex offenders. These requirements are federally enforceable through criminal prosecution pursuant to § 2250 if the basis for registration is a federal sex offense conviction, if a non-federal sex offender travels in interstate or foreign commerce, or if a non-federal sex offender enters, leaves, or resides in Indian country. SORNA and § 2250 can be effective tools in the investigation and prosecution of recidivist sex offenders. By enforcing SORNA's obligations, prosecutors may help address the risks posed to the public by unregistered sex offenders.❖

ABOUT THE AUTHOR

❑**Bonnie Kane** joined the Child Exploitation and Obscenity Section (CEOS) in the Criminal Division of the U.S. Department of Justice as a Trial Attorney in 2006. Prior to joining the Department, Ms. Kane was an associate at K&L Gates LLP in Boston and Arent Fox LLP in Washington, D.C.✠

Social Networking Sites: Breeding Grounds for "Sextortion" Prosecutions

Darcy Katzin
Trial Attorney
Child Exploitation and Obscenity Section

Mi Yung Park
Trial Attorney
Child Exploitation and Obscenity Section

Keith Becker
Trial Attorney
Child Exploitation and Obscenity Section

I. Introduction

Social networking via the Internet takes place in many forms and has exploded in popularity in recent years. Numerous social networking sites exist, such as Facebook, perhaps the most recognizable. In general, social networking sites and tools allow computer users to establish online communities where individuals may communicate and access information about other users. While these sites are typically used for legitimate purposes, such as keeping in touch with friends and family, dating, and professional networking, they are increasingly used to extort sexually explicit images from minor victims, sometimes referred to as "sextortion." This article will explain how child exploitation offenders use social networking sites as a tool to extort sexually explicit images from minor victims and will discuss how to investigate, charge, and prosecute cases involving this conduct.

II. How child exploitation offenders use social networking sites to extort child pornography

While the crime of extortion has long been in existence, the onset of social networking sites provides child exploitation offenders with a tool to obtain newly created images of minors engaged in sexually explicit conduct. In sextortion cases, child exploitation offenders use social networking sites to target minors and demand that they provide sexually explicit material under the threat of disseminating embarrassing or humiliating pictures of the minor to his or her entire online social networking community, school, or parents. Notably, the way social networking sites are organized and used by minors makes it easy for online predators to identify and target victims—no specialized computer expertise is required.

Although all "sextortion" cases involve the use of threats to coerce a child into providing sexually explicit images, the manner of the threat can take different forms. For example, in one unreported Northern District of California sextortion case, a minor girl voluntarily sent a sexual image of herself to her then-boyfriend who was also a teenager. After they broke up, he posted the picture on an Internet site for a short time. The photograph was posted long enough for several online predators to find it. More than one of these predators were able to locate the teenage girl's Facebook page and contact her directly. One of the offenders threatened to send the sexual picture he obtained online to all of the victim's Facebook friends as well as her school principal if the victim did not send him additional

sexually explicit images of herself. The victim complied at first but when she stopped sending him new material, the offender carried out his threat and emailed a sexually explicit picture of the victim to one of her friends.

In another case, the defendant identified his victims on My Space. After he made contact with them, he used instant messaging programs to communicate with them. The defendant tricked the victims into installing a virus on their computers, giving the defendant remote access to and control of the victims' computers. The defendant used information found on the computers to threaten the victims. For example, he told some of the victims that if they did not send him sexually explicit photos, he would use the information he obtained from their banking and financial files on their computers to ruin their parents' credit. *See* FEDS: ONLINE "SEXTORTION" OF TEENS ON THE RISE, *available at* http://www.msnbc.msn.com/id/38714259/ns/technology_and_science-security/t/feds-online-sextortion-teens-rise/from/toolbar.

Because social networking sites operate online, child exploitation offenders often believe they can remain anonymous and avoid detection by law enforcement. This perceived anonymity and the ease of identifying minor targets and obtaining information about them make social networking sites a breeding ground for cases of sextortion.

III. Investigating and prosecuting extortion cases committed on social networking Web sites

A. Prosecuting "sextortion" cases under the production of child pornography statute

An attempt to convince a minor to create images depicting the minor engaging in sexually explicit conduct may be prosecuted as attempted production of child pornography pursuant to 18 U.S.C. § 2251(a) and (e), regardless of whether the attempt was accompanied by extortion. Section 2251(a) supports the prosecution of any person who "employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in . . . any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct . . . ." Section 2251(e) establishes penalties for "[a]ny individual who violates, or attempts or conspires to violate" that section, ranging from a mandatory minimum of fifteen years in prison to a maximum of thirty years in prison for a first offense. As with all attempt prosecutions, a § 2251(a) and (e) prosecution under an attempt theory requires proof that the suspect intended to commit the crime and took a substantial step to do so. Efforts to convince a minor to take sexually explicit pictures or video of himself may provide such proof depending on the individual facts of the case. Some evidence that courts have found persuasive in determining whether a defendant who is charged with attempted production of child pornography intended to commit the crime and took a substantial step in furtherance of the crime include: (1) requesting images or videos from the minor; (2) specifically describing what sexually explicit conduct the minor should engage in; (3) sending a sexually explicit image of himself to the minor; and (4) taking steps to meet the minor in person.

In order to successfully prosecute such a charge, it is important to develop evidence that the conduct the suspect wished the minor to engage in was sexually explicit as defined under 18 U.S.C. § 2256(2). Such evidence may include emails, social networking messages, instant messages, testimony by the victim regarding what the defendant requested or demanded that he do on camera or video, or images of the victim already in the defendant's possession if the defendant requested or demanded that the minor produce similar images.

B. Prosecuting sextortion cases as extortion under other federal laws

The factor that differentiates sextortion cases from attempted production of child pornography cases is, of course, the suspect's threats of retribution if such images are not created. Moreover, while a vast majority of the "sextortion" fact scenarios would likely encompass production or attempted production charges, some cases may fall short of the production requirements. For example, where a perpetrator asks a victim for sexually explicit images of the victim that already exist (for example, the perpetrator does not persuade, induce, entice, or coerce the child to produce the image), the perpetrator is exploiting the existence of such photographs but he is not persuading or coercing that minor to engage in sexually explicit conduct. Similarly, a perpetrator may ask the minor to "send more" photos of himself. However, if it is unclear as to whether the perpetrator means "take more pictures of yourself" or simply "send more already existing pictures of yourself," an attempted production case may be difficult to prove. Prosecutors have more than one charging option for extortion under federal law.

Extortion under 18 U.S.C. § 875: One option is 18 U.S.C. § 875, which proscribes four types of extortion or threats, three of which may be useful in a "sextortion" prosecution, depending on the facts of the case. Section 875(d), for example, will be chargeable in nearly all "sextortion" cases and carries a maximum penalty of two years' imprisonment. It prohibits the transmission in interstate or foreign commerce of "any communication containing any threat to injure the property or reputation of the addressee or of another" that is undertaken with the "intent to extort from any person . . . any money or other thing of value." In an online sexual extortion case, the "thing of value" generally consists of images of sexually explicit conduct that the suspect implores the victim to produce. The threat would be to injure the victim's reputation by publishing other images of or information about the child on the Internet or to send such images or information to friends or family. Courts have supported the premise that the disclosure of matters similar to sexually explicit images may be viewed as a wrongful threat to reputation. *See United States v. Jackson*, 180 F.3d 55, 70-71 (2d Cir. 1999) ("[T]hreatened disclosures of such matters as sexual indiscretions that have no nexus with any plausible claim of right. . . . [are] inherently wrongful and . . . prohibited by § 875(d)); *United States v. Pascucci*, 943 F.2d 1032, 1036-37 (9th Cir. 1991) (evidence was sufficient to support a § 875(d) conviction where defendant threatened to reveal audio tapes of victim's adulterous sexual acts if not paid by victim).

Where threats of violence or physical harm to the victim are made in conjunction with the attempt to extort, § 875(b) or (c) may apply. Section 875(b) proscribes the transmission in interstate or foreign commerce of "any communication containing any threat to kidnap . . . or . . . injure the person of another" with the intent to extort money or another thing of value. This section carries a maximum penalty of twenty years' imprisonment. Section 875(c) prohibits the transmission in interstate or foreign commerce of "any communication containing any threat to kidnap . . . or . . . injure the person of another" without the requirement of any intent to extort the person. This section carries a maximum penalty of five years' imprisonment.

Travel Act extortion: In addition to possibly charging extortion under 18 U.S.C. § 875(d), a prosecutor may wish to consider charging extortion under the Travel Act, 18 U.S.C. § 1952, which provides for a higher maximum sentence.

The Travel Act states, in relevant part, that anyone who "travels in interstate or foreign commerce or uses the mail or any facility in interstate or foreign commerce, with intent to . . . promote, manage, establish, carry on, or facilitate the promotion, management, establishment, or carrying on, of any unlawful activity and thereafter performs or attempts to perform [said act] shall be fined under this title, imprisoned not more than 5 years, or both . . . ." 18 U.S.C. § 1952(a)(3) (2010). One of the types of unlawful activity referenced in the Travel Act is "extortion . . . in violation of the laws of the State in

which committed or of the United States . . . ." *Id.* § 1952(b). Although the Travel Act does not define "extortion," the Supreme Court, in *United States v. Nardello*, 393 U.S. 286 (1969), found extortion committed under the Travel Act where "money was to be obtained from the victim by virtue of fear and threats of exposure." *Id.* at 296.

Because "sextortion" in the child pornography context is a fairly new concept, no reported cases charged under the Travel Act are available involving the extortion of minors for sexually explicit images of themselves. The extortion charge under the Travel Act, however, has been used against individuals attempting to obtain money through threats of exposure of the victim's past sexual indiscretion. *See id.* at 295-96 (finding the existence of extortion where the defendants attempted to obtain money from their victims by threatening to expose the victims' alleged homosexual conduct); *United States v. Hughes*, 411 F.3d 461 (2d Cir. 1969) (extortion under Travel Act exists where defendants attempted to obtain money by threatening the victim with possible arrest for sodomy charges and exposure of the victim's sexual orientation); *cf. United States v. Schwartz*, 398 F.2d 464 (7th Cir. 1968) (violation of § 1952 based on extortion exists where defendants use fear of arrest and loss of reputation to coerce payment from victim). These cases thus provide support for charging a violation of § 1952 in a sextortion case.

The same type of extortion is at issue under 18 U.S.C. § 875(d) and the Travel Act: Because the same type of extortionate activity is prohibited under § 875(d) and the Travel Act, a prosecution under either of these extortion statutes should be viable where a minor is being extorted to provide sexually explicit pictures of himself. Moreover, the Supreme Court has noted generally that several federal statutes, including the Travel Act and the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. §§ 1961–1968, use a broad concept of extortion. Under such an expansive view, the modern concept of extortion in most states now includes, inter alia, exposing a secret of the victim that would subject him to public disgrace. *James v. United States*, 550 U.S. 192, 221-22 (2007) (citations omitted). Even the Model Penal Code's definition of "Theft by Extortion" adopts the modern broad view of extortion to include "[the] expose[ure of] any secret tending to subject any person to hatred, contempt or ridicule, or to impair his credit or business repute . . . ." *Id.* at 221 (citing MODEL PENAL CODE § 223.4); *see also Nardello*, 393 U.S. at 295-96 (where the Supreme Court found that the generic definition of extortion applied to the victim's fear or threat of exposure of the victim's sexual conduct).

Case law addressing extortion based on fear of exposure of past sexual conduct supports charges under §§ 1952 and 875(d) in sextortion cases. Prosecutors should thus consider charging violations of these statutes when appropriate, in addition to charging sexual exploitation violations such as attempted production of child pornography, production or distribution of child pornography, or enticement of a minor to engage in prohibited sexual conduct.

IV. Conclusion

Social networking sites serve numerous legitimate purposes and are advancements in the Internet's ability to connect people and to make information more readily accessible. Nevertheless, these sites also provide child predators with additional tools to exploit and commit crimes against children. Fortunately, investigators and prosecutors are equipped with numerous statutes that may be used to hold child exploitation offenders responsible for their actions. As discussed above, offenders who use social networking sites to identify minors and extort new sexually explicit images from them may be charged with production or attempted production of child pornography, enticement of a minor, as well as extortion offenses. Therefore, while social networking sites have become a breeding ground for child exploitation offenses, prosecutors are well equipped to bring charges against any child exploitation offender who uses such sites to exploit children.❖

ABOUT THE AUTHORS

❑**Darcy Katzin** has been a Trial Attorney with the Child Exploitation and Obscenity Section since 2005. Prior to joining the Section, Ms. Katzin served as an Assistant District Attorney for the New York County District Attorney's Office, where she prosecuted child abuse and other criminal cases.✠

❑**Mi Yung Park** is a Trial Attorney in the Child Exploitation and Obscenity Section in the Criminal Division of the U.S. Department of Justice. Prior to joining the Section, Ms. Park worked as an Assistant United States Attorney at the U.S. Attorney's Office for the Southern District of California.✠

❑**Keith Becker** joined the Child Exploitation and Obscenity Section as a Trial Attorney in 2010. He was previously an Assistant United States Attorney at the U.S. Attorney's Office for the District of Columbia, where he prosecuted federal and local cases involving violent crime, narcotics, and child pornography. Prior to joining the Department, Mr. Becker clerked for the Honorable Chief Judge Jon P. McCalla in the Western District of Tennessee.✠

Emerging Issues in the Extraterritorial Sexual Exploitation of Children

Anitha S. Ibrahim
Trial Attorney
Child Exploitation and Obscenity Section

Ed McAndrew
Assistant United States Attorney
District of Delaware

Wendy Waldron
Trial Attorney
Child Exploitation and Obscenity Section

I. Introduction

The extraterritorial sexual exploitation of children, commonly referred to as "child sex tourism," generally involves Americans traveling to foreign countries, often in economically depressed regions, where they sexually exploit minors. This article will focus on three emerging factual and legal issues in cases involving the extraterritorial sexual exploitation of children.

First, the phenomenon of individuals in the United States using webcams to view minor victims thousands of miles away engage in sexual acts in real time is becoming increasingly prevalent. A study of *United States v. Pavulak*, 672 F. Supp. 2d 622 (D. Del. 2009), will demonstrate how this technology is being abused by offenders and how to charge and prove these types of cases. *Pavulak* involved a convicted sex offender in Delaware who met a woman from the Philippines online, began grooming her two-year old daughter to engage in sexual acts, and tried to persuade the mother to engage in sexual acts with the child in front of a webcam.

Second, *United States v. Frank*, 486 F. Supp. 2d 1353 (S.D. Fla. 2007), will demonstrate how a statute carrying a mandatory minimum sentence of 30 years imprisonment can successfully be employed to prosecute the buying, selling, or otherwise obtaining custody or control of a child for the purpose of producing child pornography. The case involved a U.S. citizen who traveled to Cambodia and photographed his commercial sexual exploitation of minors.

The final issue presented will be the proper role and implementation of restitution in cases involving the extraterritorial sexual exploitation of children, as restitution in these cases is critically important to provide justice for victims who have often been targeted because of their depressed economic conditions. A case study of *United States v. Mathias*, Case No. 09-cr-60292 (S.D. Fla. Mar. 2, 2010), will present this restitution issue. The case involved a U.S. citizen who formed a long-term relationship with a woman in the Philippines. The woman had two minor girls who Mathias groomed for years through email, letters, and telephone calls and who he sexually abused during two trips to the Philippines. In *Mathias*, prosecutors were able to obtain a large restitution award through a negotiated plea agreement and worked to establish a restitution trust fund with a U.S. based trustee to ensure that the restitution money would be properly used.

II. Webcams

The use of webcams for the performance of sexually explicit acts by minors from foreign locations is becoming increasingly popular. United States law enforcement overseas, particularly in the Philippines, has received reports of adults who recruit minors or use their own children to pose nude and engage in sexual acts in front of a webcam. The webcam session is then broadcast to an individual located overseas who sends money to view such conduct. The money is sent through online payment Web sites with pickup places located overseas. The individuals paying to watch the conduct are mainly individuals located abroad in developed countries.

The two primary federal statutes proscribing such conduct are 18 U.S.C. § 2422(b) (coercion and enticement of a minor) and 18 U.S.C. § 2251(a), (e) (production and attempted production of child pornography). Both of these statutes were employed successfully in the prosecution of Paul Edward Pavulak.

Pavulak, a recidivist child sex offender, was previously convicted in 1998 and 2005 of second degree unlawful sexual contact with minors in Delaware. In each of those cases, Pavulak used personal advertisements in the local newspaper to meet women who had daughters. In each instance, Pavulak became romantically involved with the women and then sexually molested the daughters. He was released from custody in July 2008 and almost immediately began using the Internet to identify foreign women who might knowingly permit him to sexually exploit their daughters for money. Pavulak began by creating a profile on a Web site used to solicit Philippine prostitutes. Pavulak would identify females of interest, contact them, and then use Internet money transfer services to pay them to engage in sexually explicit webcam sessions and instant message chats with him.

In August 2008, Pavulak contacted a woman in the Philippines whose profile he had viewed on a Web site. The woman had a two-year-old daughter. Pavulak emailed the woman and told her that he planned to travel to the Philippines in December 2008 and was seeking a "wife" and was looking to find "a woman with a child." Pavulak continued to develop the relationship online with the woman over several months, sending her money through online payment Web sites and establishing plans to meet her and her daughter in the Philippines.

In December 2008, Pavulak traveled to the Philippines and met the woman and her daughter. He gave the woman a laptop computer equipped with a webcam. Pavulak produced a movie of himself and the woman engaging in sexually explicit conduct. He described the movie as the two-year-old girl's "training video." In another video produced using the laptop's webcam, Pavulak was recorded standing naked in a hotel room with the child and her mother. He did not touch the child in the video and there was no evidence that he sexually abused the child during this trip. As he left the Philippines on January 13, 2009, however, Pavulak engaged in a text message conversation with the woman and discussed his plan to sexually abuse her daughter on his next trip to the Philippines and his desire to watch, via webcam, the daughter using sex toys he had given to the mother. He also encouraged the mother to sexually molest the child to groom her for his planned sexual abuse of her upon his return to the Philippines.

On January 18, 2009, after returning to his office in Delaware, Pavulak engaged in another webcam and instant message chat session with the mother and again instructed her to groom the child for future sexual molestation by him. Pavulak then instructed the mother to display the child's genitals on the webcam. The mother displayed the child's pubic area covered by a diaper and told Pavulak that she would expose the child's genitals in their next webcam session.

The next morning, law enforcement agents executed a search warrant on his office obtained as a result of fellow employees having reported that Pavulak was viewing child pornography on his office computer. The agents arrested Pavulak, wholly unaware at the time of his webcam activities or of his relationship with the two-year-old child and her mother, conduct that was only discovered later during a comprehensive computer forensic examination.

No evidence was available to show that Pavulak had engaged in sexual contact with the two-year-old child during his trip to the Philippines and no video recording of the January 18th webcam session was available to demonstrate that Pavulak instructed the mother through an instant message chat to display the child's genitals via webcam. Nonetheless, the United States charged Pavulak with attempted coercion and enticement of a minor in violation of 18 U.S.C. § 2422(b) and attempted production of child pornography, in violation of 18 U.S.C. § 2251(a). Significantly, the production of child pornography statute was amended on October 13, 2008 to clarify that the statute applies to cases involving the live transmission of images of child sexual abuse, such as the use of a webcam. Pub. L. 110-401, §§ 301, 303 122 Stat. 4242 (2008).

The offense of coercion and enticement of a minor requires the Government to prove that the defendant "knowingly persuade[d], induce[d], entice[d], or coerce[d]" a minor to engage "in prostitution or any sexual activity for which any person can be charged with a criminal offense . . . ." 18 U.S.C. § 2422(b) (2010). The terms "persuade, induce, entice, or coerce" include everyday meanings, such as to " 'convince[], influence[], or ma[ke] the possibility more appealing' and 'to stimulate the occurrence of.' " *United States v. Kaye*, 451 F. Supp. 2d 775, 782-83 (E.D. Va. 2006) (citing *United States v. Rashkovski*, 301 F.3d 1133, 1137 (9th Cir. 2002) and *United States v. Murrell*, 368 F.3d 1283, 1287 (11th Cir. 2004)). To "coerce" means:

> To compel by force, intimidation or authority, esp. without regard for individual desire or volition . . . to bring about through the use of force or other forms of compulsion; exact . . . to dominate or control, esp. by exploiting fear, anxiety, etc.

WEBSTER'S ENCYCLOPEDIC UNABRIDGED DICTIONARY OF THE ENGLISH LANGUAGE 398 (Random House 1996). Convictions under § 2422(b) have been upheld in cases where the enticement of the child takes place through an intermediary, such as the two-year-old child's mother in *Pavulak*. *See, e.g.*, *United States v. Lanzon*, 639 F.3d 1293, 1299 (11th Cir. 2011); *United States v. Douglas*, 626 F.3d 161, 165 (2d Cir. 2010).

A defendant violates the attempt portion of § 2422(b) where he uses a facility of interstate or foreign commerce with the intent to "persuade[], induce[], entice[], or coerce[]" a minor to engage in "any sexual activity for which any person can be charged with a criminal offense." Whether the defendant intended to or actually did engage in the unlawful sex act is immaterial. *See, e.g., Douglas*, 626 F.3d at 164; *United States v. Brand*, 467 F.3d 179, 201-02 (2d Cir. 2006); *Murrell*, 368 F.3d at 1286 ("[I]f a person persuaded a minor to engage in sexual conduct (e.g. with himself or a third party), without then actually committing any sex act himself, he would nevertheless violate § 2422(b)").

In *Pavulak*, the jury was instructed to consider attempted production of child pornography in violation of § 2251 as the prohibited sexual activity. This related directly to Pavulak's January 18, 2009 webcam activities. In addition, because Pavulak traveled to the Philippines, and at the very least attempted to engage in sexual contact with the two-year-old, the jury was also instructed on two provisions of Philippine law: (1) rape, in violation of Revised Penal Code of Philippines, Article 266-A; and (2) corruption of minors, in violation of Revised Penal Code of Philippines, Article 340.

The Government's theory at trial was that Pavulak acted with the specific intent to commit the crimes of production of child pornography and coercion and enticement of a minor and that he took substantial steps toward doing so. The Government emphasized that Pavulak created a profile on a social networking Web site that featured Filipino females available for sex with tourists. He then identified a woman with a young child and spent months online and hundreds of dollars to establish a relationship with her in advance of his trip. He met the woman and child in the Philippines, where he was filmed nude in a room with them. Upon leaving the Philippines, he encouraged the woman to groom the child for sexual abuse by him for his next trip to the Philippines. He provided the woman with a webcam-enabled laptop so that he could continue his online relationship with the woman and her daughter upon his return to the United States and engaged in a webcam and instant message session where he specifically requested that the woman show him the child's genitalia. Pavulak also provided the woman with sex toys to be used to groom the child and planned to watch the grooming via webcam.

The evidence that the Government introduced during trial was similar to evidence introduced in other cases where convictions for attempted production of child pornography and attempted coercion and enticement of a minor have been upheld. Such evidence includes chat logs, phone calls, promises or transfers of gifts or money, plans to meet, travel by the defendant or victim, and efforts to photograph or record sexual images of a victim or to transmit such images between defendant and victim. *See, e.g.*, *United States v. Lee*, 603 F.3d 904, 918-19 (11th Cir. 2010); *United States v. Creary*, 382 F. App'x 850, 852-53 (11th Cir. 2010); *United States v. Nestor*, 574 F.3d 159, 161-62 (3d Cir. 2009); *United States v. Pierson*, 544 F.3d 933, 938 (8th Cir. 2008); *United States v. Tykarsky*, 446 F.3d 458, 469 (3d Cir. 2006); *United States v. Munro*, 394 F.3d 865, 869 (10th Cir. 2005); *Murrell*, 368 F.3d at 1288; *United States v. Kaye*, 451 F. Supp. 2d 775, 787 (E.D. Va. 2006).

In many instances, the evidence used to establish the intent and substantial step elements of the crimes of attempted enticement and attempted production of child pornography overlap. In *Pierson*, for instance, the defendant chatted online, through text message, and through cell phone calls for several months with an undercover agent posing as a 14-year-old girl. *Pierson*, 544 F.3d at 935-36. In online chats, the defendant asked "the girl" to pose nude in front of a webcam for the defendant's viewing pleasure. The defendant offered to send "the girl" money to purchase a webcam and offered to pay "the girl" to procure other young girls to pose nude on webcam. The Eighth Circuit found this evidence sufficient to support convictions for both attempted production of child pornography and attempted enticement of a minor. *Id.* at 938-39; *see also Creary*, 382 F. App'x at 852-53 (affirming attempted enticement conviction based on defendant's online chats where he encouraged minors to use webcams to transmit sexually explicit images of themselves to him).

In *Lee*, the Eleventh Circuit affirmed attempted enticement and attempted production of child pornography convictions where the defendant chatted online for several months with an undercover agent posing as the mother of two minor daughters available for sex. *Lee*, 603 F.3d at 908-11. The court looked to the chat logs where the defendant repeatedly asked "the mother" to produce and email sexually explicit photographs of the "daughters" to him and instructed "the mother" as to how many pictures to take and how to pose "the daughters." The court found that this evidence sufficiently supported his conviction for attempted production of child pornography. *Id.*

The *Lee* court relied on the same and some additional evidence to affirm the attempted enticement conviction, including the facts that the defendant also: (1) initiated the chat sessions; (2) expressed interest in engaging in sex acts with "the daughters;" (3) transmitted webcam images of himself masturbating; (4) sent "the mother" digital photographs of his penis to show to "the daughters;" and (5) promised gifts in exchange for sex with "the daughters" or for sexual images of them. *Id.* at 915-17; *see also United States v. Young*, 613 F.3d 735, 743-44 (8th Cir. 2010) (affirming attempted

enticement conviction where defendant developed online relationship with fictitious minor, planned to meet for sex, reserved motel room, and traveled to motel room).

The prosecution team in *Pavulak* successfully used multiple statutes to target the use of technology by the defendant in committing his extraterritorial sexual exploitation of a minor. The *Pavulak* case demonstrates that even in the absence of an actual video recording of the sexually explicit acts or evidence of actual sexual conduct between a child sex tourist and a minor victim, a conviction for at least attempted production of child pornography and/or enticement and coercion of a minor can be sustained.

III. Buying, selling, and obtaining custody or control of children

The prosecution of Kent Frank in the Southern District of Florida involved the use of a relatively untested statute—18 U.S.C. § 2251A (2008)—to address conduct that occurs in many cases where children are sexually abused abroad. The Eleventh Circuit's decision in *United States v. Frank*, 599 F.3d 1221 (11th Cir. 2010), supports a broader range of options when making charging decisions in child sex tourism prosecutions. Frank was charged in connection with two trips to Cambodia during which he paid several teenage girls to take sexually explicit images and to engage in sexually explicit conduct. In addition to child sex tourism charges under 18 U.S.C. §§ 2423(b) and 2423(c), Frank was charged with and convicted of purchasing a minor for the purpose of producing images of sexually explicit conduct under § 2251A(b) (buying and selling of children), a provision that carries a mandatory minimum sentence of 30 years' imprisonment. He was ultimately sentenced to 40 years' imprisonment for his crimes.

Frank met his four teenage victims in Phnom Penh. He did not use an intermediary but instead paid the victims directly to come back to his hotel room for sexual acts and to take sexually explicit photographs. The girls often would spend the night and were exploited by Frank multiple times over a three-month period. There was no evidence of physical coercion. At trial, the victims testified for the defense that they were eighteen-years-old when they met the defendant, that they were free to leave at any time, and that posing for photographs was their idea. It is also important to note defendant's wealth and that the Government suspected and suggested that the victims had been bribed by Frank to change their stories. The girls also testified, however, that they would not have posed for sexually explicit pictures if they had not been paid by Frank.

Because there was no proof that the images ever entered or were intended to enter the United States, Frank could not be charged with production of child pornography under 18 U.S.C. §§ 2251(c) or 2260. This limitation caused the government to consider using § 2251A to address the seriousness of Frank's conduct in producing child pornography. The relevant portion of § 2251A(b) punishes "[w]hoever purchases or otherwise obtains custody or control of a minor . . . with intent to promote . . . the engaging in of sexually explicit conduct by such minor for the purpose of producing any visual depiction of such conduct." Before the Eleventh Circuit's decision upholding Frank's conviction, no appellate decision was available that explored the meaning of "purchase" in the context of § 2251A, and some risk existed that a court would require more than paying money to obtain the compliance of the minor victim. Frank's conviction on the § 2251A charges was based entirely on the jury's finding that he "purchased" the victims for the purpose of producing child pornography. The jury declined to find, by special verdict form, that he "obtained control" over the minors.

Another anticipated appellate issue was whether § 2251A confers extraterritorial jurisdiction. The statute applies when "in the course of the conduct described . . . the minor or the actor traveled in or was transported in interstate or foreign commerce." At the time that the *Frank* case was charged, the only

decision on that issue, *United States v. Bredimus*, 234 F. Supp. 2d 639 (N.D. Tex. 2002), was at the district court level. The *Bredimus* case was resolved by a plea to 18 U.S.C. § 2423(b) after the district court decided that § 2251A reached the conduct of the defendant who had traveled to Thailand and used an intermediary to find minors to pay to take sexually explicit photographs and to engage in sexual acts.

Frank's appeal centered on his convictions under § 2251A. The Eleventh Circuit affirmed Frank's convictions and decided two issues of first impression. The court first determined that § 2251A reaches wholly extraterritorial conduct. *Frank*, 599 F.3d at 1229-30. This ruling was based on the statute's jurisdictional language, the type of offense covered, and the comprehensive nature of Congress' attempts to combat child pornography. *Id.* at 1230-31.

The court also rejected the defendant's attempt to limit the meaning of the word "purchase" to situations where money is paid to a third party or where a defendant exerts some sort of coercion or control akin to temporary enslavement of the minor. *Id.* at 1233-37. In recognizing that the term "purchase" encompasses situations where a defendant, without more, pays money to obtain the compliance of the victim, the court noted Supreme Court case law "holding that the most common definition of a word does not preclude other accepted alternatives." *Id.* at 1235 (citations omitted). In affirming Frank's conviction, the court also reasoned that his restrictive reading of the term "purchase" would undercut the efficacy of § 2251A and Congress' "intent to cast a wide net in preventing the sexual exploitation of children." *Id.* at 1236. The broad interpretation of the word "purchase" in the *Frank* decision thus supports the use of § 2251A in a range of child sex tourism cases where money is paid to obtain the compliance of the victim in creating sexually explicit images, even where no evidence is available to indicate that the images are intended to be imported into the United States.

In addition to the legal challenges to § 2251A, the defendant in *Frank* challenged the admissibility of his statements that he provided in an interrogation by Cambodian law enforcement. The Eleventh Circuit held that the district court properly denied Frank's motion to suppress his statements because it found that Miranda warnings were not needed and Frank's confession was voluntary. The Miranda warnings were found to be unnecessary because the United States and Cambodian law enforcement were not engaged in a joint venture at the time of the statements, because Cambodian law enforcement was not acting as an agent of the United States, and because Cambodian law enforcement actions did not shock the judicial conscience. *Id.* at 1229.

IV. Restitution trust funds for foreign children

Restitution in cases involving the extraterritorial sexual exploitation of children can be extremely complicated because of the difficulty in calculating, obtaining, and implementing restitution. However, restitution in these cases is also one of the most critical components of sentencing because it may allow the victims to keep from being victimized again by another child sex tourist. In the wake of the *Frank* decision, § 2251A was used in another prosecution in the Southern District of Florida that raised complex restitution implementation issues. In *United States v. Mathias*, No.09-cr-60292 (S.D. Fla. Mar. 2, 2010), the United States was able to obtain a restitution award of $200,000, with the defendant agreeing to transfer title of his property to the United States to satisfy part of the restitution order. The United States then took a novel approach to ensure that the court-ordered restitution directly benefitted the minor victims located in the Philippines by creating a trust for the benefit of the victims with a trustee based in the United States.

The *Mathias* case involved a defendant who communicated with a mother of four young children and who arranged to travel to the Philippines to engage in sexual conduct with the two eldest children. Between 2005 and 2008, Mathias and the mother exchanged hundreds of emails where they discussed

and made plans for Mathias to sexually abuse the two girls. In April 2007, when one child was twelve and the other was eleven years of age, and later in December 2007, Mathias traveled to the Philippines and engaged in sexual conduct with them while the mother videotaped the acts. During the December 2007 trip, Mathias forced the victims to sign a contract requiring them to be his "sex slaves." In December 2008, Mathias traveled a third time to the Philippines to engage in sexual conduct with the girls. When the girls learned that this trip was about to occur, they disclosed the prior abuse to a family member who, in turn, contacted Filipino law enforcement. When Mathias arrived in the Philippines, he was detained by Filipino police. Mathias was directed by the police to remain in the Philippines pending further investigation but Mathias instead returned to the United States.

After the children disclosed the abuse to authorities in the Philippines, Filipino police arrested their mother and the children were placed in the custody of the Philippines Department of Social Welfare and Development (DSWD). The two young girls were removed from their home, taken out of their school, left without a parent, and separated from their two younger siblings.

Authorities in the Philippines notified U.S. law enforcement of Mathias' conduct and in October 2009 U.S. law enforcement officers arrested him in Miami. A grand jury in the Southern District of Florida indicted Mathias on a number of charges including offering to buy children for the purpose of making child pornography, in violation of § 2251A, and traveling in foreign commerce and having sex with children, in violation of § 2423(c).

The evidence in the *Mathias* case included the emails in which the defendant described the sexual acts he wished to engage in with the victims as well as the victims' testimony that defendant engaged in sexual acts with them and recorded those acts. However, neither the Filipino authorities nor the U.S. authorities were ever able to locate the recordings of the sexual acts. Thus, the government would be required to bring the victims to the United States to testify as to the sexual acts that occurred and the recording of those acts. The victims, who had been greatly affected by being removed from home, school, and their siblings, were intimidated at the prospect of traveling to the United States and testifying against Mathias.

In contemplating plea offers made by the defense, the government was adamant that the defendant, in addition to serving an appropriate lengthy sentence of imprisonment, also pay restitution to help the victims overcome the trauma they had endured. A threshold issue was determining the appropriate restitution amount. In *United States v. Doe*, 488 F.3d 1154, 1163 (9th Cir. 2007), the Ninth Circuit upheld a restitution award for foreign victims that included costs for ongoing trauma counseling and medical treatment, vocational training, a catch-up program for a GED-type degree, formal schooling, and a management fee for an non-governmental organization (NGO) that would coordinate the services for the child victims. In upholding the amount of restitution awarded, the Ninth Circuit approved restitution costs to address both past and long term effects of sexual abuse caused by the defendant to foreign victims. *Id.* at 1159. In *Mathias*, as in the *Doe* case, the victims suffered numerous harms such as being removed from their school and their home, being separated from their family unit, and suffering psychological and physical trauma from the defendant's sexual abuse. Working with the DSWD authorities, prosecutors were able to obtain an estimated cost of schooling, housing, counseling, and medical services per year for the victims.

On December 22, 2009, Mathias, who was then 64 years of age, pled guilty pursuant to a plea agreement under Federal Rule of Criminal Procedure 11(C)(1)(c) to violating § 2423(c) and agreed to a 20-year sentence of imprisonment and to pay restitution to the victims in the amount of $200,000. He also agreed to surrender to a court-appointed receiver his interest in his real property that would be sold and proceeds applied toward his restitution obligations. Mathias also agreed that if he received any

earnings during his time in prison, such as through a UNICOR job, part of those earnings would go towards restitution for his victims.

The next challenge was to ensure that the restitution money would be used properly to administer victim services. Because the girls were still minors, the United States had to decide who would administer the girls' restitution money. The solution was that the United States would set up a trust for the benefit of the victims and would find someone in the United States to serve as trustee. The United States retained an outside trust attorney who drafted a trust document and also helped locate a suitable trustee in the United States: a NGO called the Center for Special Needs Trusts Administration (the Center), based in Clearwater, Florida. The Center offers specialized administrative services for unique trust situations, requires no minimum deposit, and has no minimum annual fee for small accounts.

The trust attorney, working with the United States and DSWD in the Philippines, drafted the trust documents. Through the trust documents, the Center serves as trustee and also grantor of the trust. The trust documents require DSWD, as the guardian of the beneficiaries, to provide an annual plan of care for the victims, outlining the items and services that the minor victims need and the estimated costs of the items and services. The annual plan covers areas such as mental health, education, residence, family, and vocation. The Center, as trustee, transfers money into an account in the Philippines on a quarterly basis. The trust documents require DSWD to provide to the Center an accounting of how the money is actually used. Each trust will be in place for the beneficiary until the child reaches the age of twenty-five or graduates from college, whichever occurs first. The creation of the trusts in the *Mathias* case required a vast amount of coordination both in the United States and overseas. With this template now in place, prosecutors should consider using this trust mechanism in cases involving the extraterritorial sexual exploitation of children to ensure that restitution is effectively used towards making foreign minor victims whole.

V. Conclusion

As demonstrated by the *Pavulak*, *Frank*, and *Mathias* cases, child sex offenders in the United States may look to foreign countries to sexually exploit children due to the ease of foreign travel and the ever-increasing availability of Internet technologies. The use of webcam technology in particular provides a new way for individuals to sexually exploit children located in foreign countries. While § 2423(c) may be an appropriate charge in child sex tourism cases, this article demonstrates that several other statutes such as §§ 2422(b), 2251, and 2251A, may also be successfully used in certain factual scenarios. Lastly, the role of restitution in cases involving the extraterritorial sexual exploitation of minor should not be overlooked in evaluating an appropriate punishment for the offender and vindication for the victims.❖

ABOUT THE AUTHORS

❑**Anitha S. Ibrahim** joined the Child Exploitation and Obscenity Section (CEOS) in the Criminal Division of the U.S. Department of Justice as a Trial Attorney in October 2007. As a CEOS Trial Attorney, Ms. Ibrahim prosecutes cases involving violations of federal child exploitation statutes, including offenses involving child pornography and the extraterritorial sexual exploitation of children. In 2008, Ms. Ibrahim served as a Special Assistant United States Attorney in the U.S. Attorney's Office for the District of Columbia, prosecuting domestic violence cases. In May 2009, Ms. Ibrahim co-authored *Report to LEPSG on the "Global Symposium for Examining the Relationship Between Online and Offline Offenses and Preventing the Sexual Exploitation of Children*."✠

❑**Ed McAndrew** is an Assistant United States Attorney and the Project Safe Childhood Coordinator for the District of Delaware. Prior to joining the Delaware office in July 2008, Ed was a CEOS Trial Attorney and a Special Assistant United States Attorney in the Eastern District of Virginia, where he prosecuted Internet crimes against children. Ed's prior publications include: *Surreptitious Recording as Attempted or Actual Production of Child Pornography*, CEOS Quarterly Newsletter (July 2011) (with co-author Jeffrey Zeeman); *Hashing Out a Child Pornography Investigation*, CEOS Quarterly Newsletter (May 2009) (with co-author Matthew Kiley); and *Undercover Mother: Sex with My Child?*, CEOS Quarterly Newsletter (September 2007).✠

❑**Wendy Waldron** has been a Trial Attorney in the Child Exploitation and Obscenity Section since 2001. She has prosecuted numerous sex tourism and child prostitution cases. Before joining the Department of Justice, she served as a law clerk to the Honorable Mark L. Wolf in the District of Massachusetts.✠

Units of Prosecution in Child Pornography Cases and Rebutting the Argument that Possession of Child Pornography is a Lesser Included Offense of Receipt

Andrew McCormack
Trial Attorney
Child Exploitation and Obscenity Section

I. Introduction

Determining the proper unit of prosecution in child pornography cases may appear to be difficult, given the variety in the amount of material that may be involved and the methods of storing, obtaining, distributing, and producing the material. One defendant may have obtained all of his material through one particular method and kept it on a single computer while another defendant may have obtained his images and videos in a number of different ways and stored them in multiple locations that may range from separate media storage devices (hard disk drives, flash drives, DVDs/CDs, etc.) to separate geographic places, such as a house, storage shed, office workspace, or car. A distributor of child pornography may be an individual who traded child pornography a few times on a few dates by simply using email or may be an individual who for years has distributed images on a variety of platforms, such as peer-to-peer networks, Internet Relay Chat, newsgroups, and Web-based bulletin boards. Similarly, producers of child pornography include individuals who take several pictures of a single victim on a single date as well as individuals who have photographed and filmed multiple victims over many years.

As a general rule, prosecutors will need to consider the nature of the offender's criminal acts and the actus reus of the statute in question when determining how many counts should be charged. This article outlines how courts have analyzed the issue of units of prosecution in child pornography cases involving: (1) production; (2) distribution, transportation, and receipt; and (3) possession. It further analyzes the related issue of what steps should be taken to avoid multiplicity arguments when both receipt and possession of child pornography are charged.

II. Units of prosecution

A. Production of child pornography

Practitioners often colloquially refer to a violation of 18 U.S.C. § 2251(a) as "production of child pornography" and a violation of § 2251(a) and (e) as "attempted production of child pornography." However, it is critically important to remember that the crime prohibited in §2251(a) is not the production of the image, but the use of a child. According to the statute, the actus reus that a defendant must engage in to commit the substantive offense is the employment, use, persuasion, or coercion of a

minor to take part in sexually explicit conduct. If the defendant engages in this conduct with the requisite mens rea (for example, for the purpose of producing a visual depiction of the conduct), he has committed the substantive offense whether or not any visual depiction was actually produced. This concept is illustrated in *United States v. Buculei*, 262 F.3d 322, 325 (4th Cir. 2001), a case involving the conviction of a 38-year-old defendant who engaged in sexual acts with a 14-year-old girl from Maryland whom he met online. The defendant traveled from New York to Maryland, took the girl to a motel room, and gave her an alcoholic drink. He positioned the camera to face the bed, placed a tape inside, and began engaging in sex with her. Ultimately, no child pornography video was made because Buculei failed to fully rewind the videotape. Even though no visual depiction was produced, the Fourth Circuit upheld Buculei's conviction for commission of the substantive offense. The court explained that Bucelei's lack of success in his attempt to actually produce a visual depiction of the sexually explicit conduct "does not . . . require his acquittal on Count Two, that he violated § 2251(a)" because, assuming the jurisdictional commerce requirement was satisfied, Buculei violated § 2251(a) "when [he] induced [the minor] into sexually explicit conduct for the purpose of producing a visual depiction thereof." *Id.* at 328.

This understanding of § 2251(a) is apparent in two circuit court decisions addressing unit of prosecution issues. In *United States v. Esch*, 832 F.2d 531 (10th Cir. 1987), the defendants were convicted of sixteen counts of violating § 2251(a) based on sixteen separate photographs. On appeal, the defendants argued that the indictment was multiplicitous. Specifically, the defendants contended "that the photographs depicted the same two children and were produced in the same photographing session and therefore constituted only one crime." *Id.* at 541. The court disagreed and explained that when determining the correct unit of prosecution, one must look in part at the key element of the federal offense. *Id.* After noting that § 2251(a) proscribes the use of a minor to engage in "any sexually explicit conduct for the purpose of producing *any visual depiction* of such conduct" (emphasis added), the court held,

> [a]s we construe the statute, each use of a minor to create a visual depiction constitutes a separate and distinct violation, and thus represents the correct unit of prosecution. . . . The fact that multiple photographs may have been sequentially produced during a single photographing session is irrelevant. Each photograph depended upon a separate and distinct use of children.

Id. at 541-42. *See also United States v. Tashbook*, 144 F. App'x 610, 616 (9th Cir. 2005) (unpub.) (holding that two photographs of a minor, taken during the same photo shoot, may be grounds for two separate offenses under § 2251(a)).

The logical corollary of *Esch* and *Tashbook* is that using two minors to create a single image would permit two counts, not one, because each use of a minor to create an image may be a separate violation. One district court declined to follow this reasoning. In *United States v. Coutentos*, 2009 WL 4730180, at *1-2 (N.D. Iowa Dec. 3, 2009), the court found that § 2251(a) was ambiguous as to whether a single video involving two child victims could be charged as two counts and thus invoked the rule of lenity to dismiss one of the counts. While prosecutors should be aware of *Coutentos*, the court's reasoning and decision were flawed. Specifically, the court failed to recognize that each separate and distinct use of a minor is the proper unit of prosecution. Moreover, the statute refers to "use of a minor," not "use of minors," indicating that one video depicting two minors would involve two uses of a minor and thus two units of prosecution.

As a practical matter, the evidence available in a particular case will likely drive the charging decision. Thus, a case involving an individual minor who was photographed over a period of time and with limited evidence on the exact dates of the abuse may be charged as one count of production

encompassing, as a single course of conduct, multiple days, months, or even years. Similarly, a case involving a defendant who photographed multiple victims may more easily be charged per victim as opposed to each photograph or video taken. By the same token, a case involving evidence that is more easily described by incident (for example, three distinct photo sessions with clear evidence of the dates when the photo sessions took place) may be better charged with a separate count for each incident. Of course, in some circumstances it may make sense for a prosecutor to charge fewer counts of production than may be technically possible in order to avoid allegations of multiplicity and, perhaps more importantly, to simplify the case for a jury.

Sentencing implications of charging decisions must also be taken into account. Multiple counts may lead to significant bumps in the Sentencing Guidelines because production of child pornography offenses do not group under the Guidelines. *See* U.S. SENTENCING GUIDELINES MANUAL § 3D1.2(d) (2011).

Single victim cases: Assume that a defendant took photographs of the same minor on five separate occasions. As discussed above, the defendant may be charged with five separate counts (or possibly more depending on the number of photographs taken on each occasion) or a single count charging a course of conduct over a period of time. However, pursuant to § 3D1.4, a conviction on five counts would result in a four level offense level increase while a conviction on one count would not. In addition, a conviction on five counts would result in a 150-year statutory maximum while a conviction on one count only carries a potential maximum sentence of 30 years. If the defendant's guideline range resulted in a recommended sentence of more than 30 years, the court may order the sentence for each count to run consecutively to each other, rather than concurrently, up to the maximum sentence of 150 years in prison. *See* U.S. SENTENCING GUIDELINES MANUAL § 5G1.2(d) (2011); *United States v. Schellenberger*, 246 F. App'x 830 (4th Cir. 2007). Further, prosecutors should remember that, pursuant to § 3D1.4, a defendant's offense level may only be increased by a maximum of five levels.

Multiple victim cases: A similar analysis must be undertaken for production cases involving multiple victims. Pursuant to U.S.S.G. § 2G2.1, if the production of child pornography involved more than one minor, the Multiple Counts provisions of the Guidelines (Chapter Three, Part D) are applied as if the exploitation of each minor had been contained in a separate count of conviction. Assume, for example, that a defendant took a single photograph of two minors on a single occasion. Regardless of whether the prosecutor decided to charge the defendant with one or two counts of production, the Guidelines would treat the conviction as two counts. As noted above, however, a single count of production would result in a statutory maximum of 30 years while two counts of production would result in a statutory maximum of 60 years.

B. Receipt, distribution, and transportation of child pornography

When determining the appropriate unit of prosecution for the receipt, distribution, and transportation of child pornography, courts focus on the method and timing of the receipt, distribution, and transportation as opposed to the number of images and/or videos received, distributed, or transported. In other words, courts focus on the act constituting the trafficking offense, not the number of images trafficked in that act. Federal courts have held that the unit of prosecution is determined by whether separate and distinct acts made punishable by the law have been committed. Thus, the unit of prosecution is the actus reus or the physical conduct of the defendant. *United States v. Reedy*, 304 F.3d 358, 365 (5th Cir. 2002).

For example, in *United States v. Gallardo*, 915 F.2d 149 (5th Cir. 1990), the defendant was charged with four counts of mailing child pornography after sending four letters containing a total of

thirteen photographs of minors engaged in sexually explicit conduct. First, he mailed one envelope. Then months later he mailed three envelopes on one day to three different addresses. Defendant claimed that all but one count was multiplicitous. The court disagreed and found that each time the defendant sent a letter through the mail, a separate offense was committed. *Id.* at 151. Similarly, in *United States v. Meyer*, 602 F. Supp. 1480 (S.D. Cal. 1985), the defendant was charged under § 2252(a)(1) with thirteen counts of transporting child pornography—one count per photograph found in a binder in his car. The court held that the government could only charge the defendant with one count of transportation because the images were transported simultaneously. *Id.* at 1482. As both *Gallardo* and *Meyer* demonstrate, the unit of prosecution is determined by the defendant's acts, not the number of images involved. In *Gallardo*, the defendant engaged in four separate and distinct acts and thus was charged with four separate counts. In *Meyer*, the defendant engaged in a single act and could only be charged with a single count regardless of the number of images involved in that single act.

A more difficult, but consistent, unit of prosecution decision is presented in *United States v. Reedy*, 304 F.3d 358 (5th Cir. 2002). In *Reedy*, the defendants were charged with transportation of child pornography for operating a sign-on, screening, and age verification system for child pornography Web sites that charged subscribers by Web site (the defendants were aware that their system was being used by child pornography Web sites). In determining whether the defendants should be charged per Web site or per image distributed by each Web site, the court first cited the following rule: " 'Whether a transaction results in the commission of one or more offenses is determined by whether separate and distinct acts have been committed.' The principle underlying this rule is that the 'unit of prosecution' for a crime is the actus reus, the physical conduct of the defendant." *Id.* at 365 (citation omitted). After failing to determine whether the term "visual depiction" from the transportation statute definitively refers to a single image or multiple images, the court next turned to *Gallardo* for the following proposition: "Where a defendant has a single envelope or book or magazine containing many images of minors engaging in sexual activity, the government often should charge only a single count." *Id.* at 367 (citation omitted). The court noted that the Reedys chose to bundle their services by Web site just as Gallardo chose to collect several pictures in an envelope and held that the district court erred by permitting the prosecution to charge the counts by individual image rather than by Web site. *Id.* at 368.

Similarly, in *United States v. Buchanan*, 485 F.3d 274 (5th Cir. 2007), the evidence consisted of one disk containing four child pornography images that had been downloaded by the defendant. The defendant was subsequently convicted of four counts of receiving child pornography. On appeal, the Fifth Circuit ruled that he could only be charged with one count because the images had all been downloaded in a single transaction. *Id.* at 282. The physical act of downloading on the part of the defendant was what was important, according to the court, and not how many images were actually downloaded. The court suggested, however, that had the defendant taken separate actions to download images—for example, one or more images at 11 a.m. and one or more additional images at 7 p.m.—multiple counts may have been appropriate. *Id.*

As a practical matter, however, it may be burdensome for prosecutors and potentially confusing for jurors to charge separate counts for each act of receipt, distribution, or transportation of child pornography. Many cases may involve dozens, if not hundreds, of distinct physical acts of receipt, distribution, and transportation. In those cases, it may be simpler to charge a single count based on a course of conduct ranging over a date range (for example, between January 1, 2009 and August 8, 2010). Another option is to charge according to the technologies involved. Thus, for example, an individual who distributed child pornography on numerous occasions using email, peer-to-peer, and Internet Relay chat may be charged with three separate counts based on the different technologies involved in the distribution.

Prosecutors should also keep in mind that multiple convictions of receipt, distribution, and transportation group, so it is not possible to increase a defendant's sentencing guideline level if he is charged with multiple counts. *See* U.S. SENTENCING GUIDELINES MANUAL § 3D1.2(d) (2011). The only possible sentencing benefit to charging multiple counts of these offenses is to permit the court to stack the sentences in the event that the defendant's total offense level exceeds the twenty-year statutory maximum for a single count, per § 5G1.2(d).

C. Possession of child pornography

Courts are split as to whether defendants may be convicted of more than one count of possession of child pornography. In *United States v. Polouizzi*, 564 F.3d 142 (2d Cir. 2009), the Second Circuit held that the defendant should have been convicted of only one count of possession under 18 U.S.C. § 2252(a)(4)(B) regardless of how many images the defendant possessed or how many different types of media were involved. *Id.* at 156. In *Polouizzi*, the defendant was charged and convicted of eleven counts of possession based on his possession of eleven computer files stored on three hard drives located in two adjacent rooms in a single location (his detached garage). The Second Circuit dismissed all but one of the counts, stating that "[b]ased on the clear language of the statute, we conclude that Congress intended to subject a person who simultaneously possesses multiple books, magazines, periodicals, films, video tapes, or other matter containing a visual depiction of child pornography to only one conviction under 18 U.S.C. § 2252(a)(4)(B)." *Id.* at 155. Similarly, in *United States v. Richards*, 2006 WL 1639103, at *3-4 (M.D. Tenn. June 12, 2006), the defendant was charged with one count of possessing child pornography for keeping material in two different locations, his home and a storage unit. The court stated that it was proper to join the multiple locations into one count of possession and further stated that had the prosecutor brought separate charges for the two locations, the second charge would be barred as multiplicitous. *Id.* at *3-4.

On the other hand, in *United States v. Planck*, 493 F.3d 501 (5th Cir. 2007), the defendant was charged with three counts of possessing child pornography in his home. The various images were stored on a desktop computer, a laptop, and over 200 diskettes. The court found that because the images were stored on three different devices, all independently capable of storing child pornography, the three counts were warranted. *Id.* at 505. "For the possession statute . . . the actus reus is the possession of child pornography . . . . Through different transactions, [the defendant] possessed child pornography in three separate places . . . and, therefore, committed three separate crimes." *Id*. Similarly, in *United States v. Flyer*, 2006 WL 2590459, at *6 (D. Ariz. Sept. 7, 2006), the court held that the defendant was correctly charged with three counts of possessing child pornography when images were found on his desktop computer, laptop computer, and various disks. The court found that the term "matter" as used in the possession statute means a "physical medium that contains a visual depiction [of child pornography]." *Id.* at *4. *See also United States v. Hamilton*, 2007 WL 2903018 (W.D. Ark. Oct. 1, 2007) (holding that two counts of possession for images located on a thumb drive and DVD were appropriate).

The result in *Planck* is consistent with the outcome in cases where courts consider the unit of prosecution for firearm possession charges. Firearms themselves are not generally considered allowable units of prosecution "*unless* they were received at *different* times or *stored* in separate places." *United States v. Hodges*, 628 F.2d 350, 352 (5th Cir. 1980) (emphasis added); *see also United States v. Hutching*, 75 F.3d 1453, 1460 (10th Cir. 1996) ("The 'simultaneous possession' of multiple firearms generally 'constitutes only . . . one offense' unless there is evidence that the weapons were stored in different places or acquired at different times." (citations omitted)). By analogy, if images were stored on multiple forms of media (for example, hard drives, thumb drives, or computer disks), one could arguably charge one count per form of media.

Finally, it is worth noting that *Polouizzi* is based on the possession language contained in § 2252(a)(4)(B). In that case, the court stated "[t]he language '1 or more' . . . indicates that a person commits one violation of the statute by possessing more than one matter containing a visual depiction of child pornography." *Polouizzi*, 564 F.2d at 155. On the other hand, *Planck* is based on the language contained in § 2252A(a)(5)(B), proscribing "knowingly possess[ing] . . . *any* book, magazine, periodical, film, videotape, computer disk, or *any other material* that contains an image of child pornography . . . ." (emphasis added). The difference in the language of the two statutes has proven critical to the evaluation of multiplicity claims under each statute. A good summary of the issue can be found in *United States v. Hinkeldey*, 626 F.3d 1010, 1013-14 (8th Cir. 2010) (citing cases). Thus, prosecutors wishing to charge multiple counts of possession should consider charging multiple violations of § 2252A(a)(5) rather than multiple violations of § 2252(a)(4).

For possession, as with all other child pornography crimes, just because a defendant can be charged with more than one count does not mean that he should be. Other than to permit the court to order the sentences to run consecutively, instead of concurrently, in the event the guideline range exceeds the single count ten-year statutory maximum penalty, there is limited sentencing benefit in charging multiple counts of possession. Thus, the time and effort to litigate multiplicity claims may outweigh any possible benefit. For that reason, as a general rule, it is usually best to opt for a single count of possession.

III. Rebutting the argument that possession of child pornography is a lesser included offense of receipt of child pornography

When an offender knowingly receives an image of child pornography, he or she simultaneously knowingly possesses that image. In such a scenario, where the possession and receipt of child pornography occur at the same moment in time, possession of that image is a lesser included offense of his receipt of the image. *See, e.g., United States v. Miller*, 527 F.3d 54 (3d Cir. 2008); *United States v. Davenport*, 519 F.3d 940 (9th Cir. 2008). Conversely, where a receipt count charges different images than a possession count, the possession count is *not* a lesser included offense of the receipt count. *See, e.g., United States v. Bobb*, 577 F.3d 1366 (11th Cir. 2009). Many cases do not, however, fall neatly into one of these two scenarios. For example, often a defendant first receives and then knowingly keeps the child pornography image over the course of days, weeks, months, or years. Such cases present the question: Under what circumstances will a possession count be considered a lesser included offense of receipt and, therefore, constitute a double jeopardy violation?

The Ninth Circuit recently addressed the issue in *United States v. Lynn*, 636 F.3d 1127 (9th Cir. 2011). In *Lynn*, the defendant used peer-to-peer file-sharing software to download child pornography onto his computer, then moved the child pornography from one file folder to another on his hard drive (from the Saved folder to the Shared folder). The defendant was charged with and convicted of both receipt and possession of the images he downloaded. On appeal, the defendant contended that his convictions for both receipt and possession of child pornography based on the same images violated the Fifth Amendment's prohibition on double jeopardy. In response, the government argued that two factors demonstrated that the receipt and possession counts were predicated on separate and distinct conduct: "(1) the indictment allege[d] that the files were received from January 10, 2008, through April 28, 2008, and possessed on May 23, 2008, the date [the defendant's] laptop computer was seized; and (2) [the defendant] received the files by downloading them . . . but he later possessed the 'depictions that he decided to retain' by moving them from one file folder on the hard drive to another . . . ." *Id.* at 1137.

Upon plain error review, the Ninth Circuit found that the district court erred by sentencing the defendant on both the possession and receipt charges. It first held that charging "different dates or date ranges for [] receipt and possession charges alone does not suffice to separate the conduct for double jeopardy purposes." *Id.* The court further explained that " '[i]f the government wishes to charge a defendant with both receipt and possession of [child pornography] based on separate conduct, it must distinctly set forth *each medium* forming the basis of the separate counts.' In other words, the indictment must allege in what form the defendant received the image and in what form he possessed it." *Id*. (emphasis added) (quoting *United States v. Schales*, 546 F.3d 965, 980 (9th Cir. 2008)). The court went on to state that "movement between folders cannot reasonably be viewed as placing images onto a different medium so as to possess them separately." *Id.* While a prosecutor may argue that moving images from one file folder to another is as distinct an act as copying the images from one medium to another, the safer course may be to rely on different images for receipt and possession counts even when the images are on different media.

In other cases, however, prosecutors have had success pointing to facts in the record that show the defendant's possession activity was not incidental to his knowing receipt of the child pornography, but rather properly supported a separate count of conviction. *See, e.g.*, *United States v. Harper*, 398 F. App'x 550 (11th Cir. 2010); *United States v. Krpata*, 388 F. App'x 886 (11th Cir. 2010); *United States v. Faulds*, 612 F.3d 566 (7th Cir. 2010); *United States v. Fox*, 357 F. App'x 64 (9th Cir. 2009).

In light of *Lynn*, prosecutors may wish to take one of the following approaches. First, prosecutors may predicate receipt and possession charges in the same indictment on different images and make this distinction clear in the charging instrument or plea agreement or through a bill of particulars or special verdict form. Second, in cases where images are received onto a hard drive, then transferred onto and possessed in another medium (for example, a thumb drive, CD, or a different hard drive), the charging instrument should clearly describe the medium that each count pertains to as well as distinguish by date when the receipt of the image(s) occurred and when the possession of the image(s) began and ended. Lastly, prosecutors may simply wish to charge one or more receipt counts rather than both receipt and possession counts.

Any one of these approaches would help avoid the scenario at issue in *United States v. Hector*, 577 F.3d 1099, 1101 (9th Cir. 2009), a case in which the Ninth Circuit held that if a defendant is convicted of a receipt charge and a possession charge, neither the defendant nor the government has the right to decide the charge that the defendant should be sentenced on if sentencing on both would create a double jeopardy violation. Rather, the court held that it is up to the sentencing court to decide which charge to dismiss. Thus, the government may lose the benefits of a mandatory minimum charge (receipt) if there is also a conviction for an offense that does not have a mandatory minimum (possession).

More recently, in *United States v. Maier*, 639 F.3d 927 (9th Cir. 2011), the Ninth Circuit reaffirmed that a district court "should" exercise its discretion to vacate the lesser-included offense, "absent unusual circumstances and compelling reasons to vacate the greater offense," noting that "[s]uch a rule safeguards against cases where a defendant charged with both possession and receipt/distribution of child pornography pleads guilty to both offenses with the hope that he will be sentenced under the lesser crime." *Id.* at 932-33. The Ninth Circuit further stated, however, that "[t]he choice of which count to vacate is fundamentally a sentencing decision" and that the district court "must choose whether the defendant's transgressions warrant a lesser penalty—a shorter statutory term of imprisonment for possession of child pornography—or a greater penalty—a longer statutory term for receipt/distribution." *Id.* at 933. In doing so, the court held that the district court's exercise of its discretion is to be guided by the factors set forth in 18 U.S.C. § 3553(a) and that "[a]n analysis rooted in these factors may also lead to

the conclusion that the greater offense should be vacated." *Id.* Summarizing the issue, the court stated the following:

> Where, as here, the defendant is factually guilty of both possession and receipt/distribution of child pornography, the district court must evaluate these factors, not the mere fact of the offense, in determining which count to vacate as well as what constitutes a reasonable sentence.

Id.

Prosecutors must therefore make careful charging decisions to avoid double jeopardy challenges in child pornography cases and the potential consequences of a successful challenge. In addition, the charging instrument should clearly articulate the image, medium, or conduct underlying a particular count to deter defendants from bringing a double jeopardy challenge.

IV. Conclusion

When determining how many counts should be charged in a child pornography case, prosecutors should consider the nature of the offender's criminal acts, the actus reus of the statute in question, the available evidence, how to best present the case to the jury, and potential sentencing implications. In production cases, each use of a minor to produce an image can be the unit of prosecution. In trafficking cases, each act of trafficking, not the number of images trafficked, can be the unit of prosecution. In possession cases, prosecutors should be aware of the two different approaches that may be taken. A prosecutor may either charge the single possession count that encompasses all of the images that the defendant possessed or charge more than one § 2252A(a)(5) count based on the images being stored in different places or acquired at different times. Finally, with respect to the possession as a lesser included offense of receipt argument, prosecutors should be familiar with the issues raised by the cases discussed above to avoid double jeopardy claims. In cases where receipt and possession are both charged, each count must be predicated on separate and distinct evidence to avoid issues of multiplicity. By considering these issues when making charging decisions in child pornography cases, prosecutors will ensure that charging documents properly account for the extent of the defendant's criminal conduct.❖

ABOUT THE AUTHOR

❑**Andrew McCormack** joined the Child Exploitation and Obscenity Section (CEOS) in the Criminal Division of the U.S. Department of Justice as a Trial Attorney in 2007. Prior to joining the Department, Mr. McCormack was an associate and counsel at the Washington D.C. office of King & Spalding.✠

Beyond the Child Pornography Sentencing Guidelines: Strategies for Success at Sentencing

Alexandra R. Gelber
Assistant Deputy Chief
Child Exploitation and Obscenity Section

I. Introduction

In an era of advisory guidelines and during a time when the child pornography trafficking and possession guideline in particular is greeted with great skepticism by the courts, an effective sentencing strategy cannot stop with the presentation of evidence that merely supports sentencing enhancements under the U.S. Sentencing Guidelines Manual. Prosecutors are more likely to get positive results at sentencing if they put together a compelling and complete case for the requested sentence, rather than spending the bulk of their energy defending the merits of the guidelines to an unreceptive audience. Ultimately, the alleged flaws in the child pornography guidelines matter much less if prosecutors provide the court with facts that support the sentence under an analysis of the factors at 18 U.S.C. § 3553(a). This article will outline strategies for an effective sentencing presentation that ensures the courts are aware of the full extent of the defendants' criminal conduct and the risk they pose to society.

II. Child pornography sentencing guidelines today: Where we are now and how we got here

Child pornography trafficking cases have been disproportionally impacted by the change to an advisory guideline system, as courts now reduce the defendant's sentence two-and-a-half times more often in child pornography cases than in all other federal cases. In FY 2010, courts downward departed or imposed a non-government-sponsored, below-guideline sentence in 44.5 percent of distribution, receipt, or possession of child pornography cases (and in 25 percent of production cases). In contrast, in the same time period, courts downward departed or imposed a below-guideline sentence without the endorsement of the government in only 18.4 percent of all other federal cases. *See* U.S. SENTENCING COMMISSION'S 2010 SOURCEBOOK OF FEDERAL SENTENCING STATISTICS, TABLE 28, at http://www.ussc.gov/Data_and_Statistics/Annual_Reports_and_Sourcebooks/2010/Table28.pdf. The high rate of below-guideline sentences in child pornography cases is unsurprising in light of a survey of district court judges conducted last year by the Sentencing Commission. Seventy percent of district court judges indicated that they felt that the guidelines result in inappropriately high sentences in child pornography receipt and possession cases (30 percent of district court judges think the guidelines are too high for distribution cases). *See* http://www.ussc.gov/Research/Research_Projects/Surveys/20100608_Judge_Survey.pdf, TABLE 8.

Although the Supreme Court's decision in *United States v. Booker*, 543 U.S. 220 (2005), was the necessary predicate to the increasing disparity in the sentences for child pornography trafficking offenses, the situation was aggravated by a memo prepared by a federal public defender entitled "Deconstructing the Myth of Careful Study: A Primer on the Flawed Progression of the Child

Pornography Guidelines" that attempts to call into question the empirical basis for the guidelines. Whatever the merits or flaws of the memo, it has clearly struck a chord with both district court and appellate judges. The Second Circuit opined that U.S. Sentencing Guidelines Manual § 2G2.2 is "an eccentric Guideline of highly unusual provenance which, unless carefully applied, can easily generate unreasonable results." *United States v. Dorvee*, 616 F.3d 174, 188 (2d Cir. 2010). In a similar vein, the Ninth Circuit claimed that "there is substantial evidence indicating that the current Guidelines-recommended sentences for possession-only offenders may be difficult to support . . . ." *United States v. Apodaca*, 641 F.3d 1077, 1084 (9th Cir. 2011). The United States, however, has successfully responded to challenges to the guidelines. *See United States v. Blinkinsop*, 606 F.3d 1110, 1123 (9th Cir. 2010); *United States v. Bastian*, 603 F.3d 460, 466-67 (8th Cir. 2010); *United States v. Morace*, 594 F.3d 340, 346-47, 350 (4th Cir. 2010); *United States v. Camiscione*, 591 F.3d 823, 836 (6th Cir. 2010); *United States v. Dyer*, 589 F.3d 520, 526-27 (1st Cir. 2009); *United States v. Cunningham*, 680 F. Supp. 2d 844, 864-65 (N.D. Ohio 2010).

To be sure, a sentencing presentation used to require little more than the introduction of evidence to establish the application of each of the specific offense characteristics. In an era of advisory guidelines, however, the guidelines are just the beginning, not the end, of the sentencing process. Defense attorneys have successfully exploited courts' freedom from the guidelines and now regularly gather and introduce evidence at sentencing in support of an argument for a reduced sentence, most often in the form of reports from psychologists that claim the defendants are not pedophiles or at risk of recidivism. Prosecutors have been slower to adapt and often still model their sentencing case on the script provided by the guidelines. It has become clear, however, that in child pornography cases, federal prosecutors are less likely to be effective and successful if they limit their sentencing advocacy to the criteria outlined in the guidelines. It is easy to understand why. As the courts are inclined to view the child pornography guidelines with skepticism at best, and with wholesale disregard at worst, premising the sentencing presentation exclusively on the specific enhancements contained in the guidelines does not give prosecutors any good facts to work with to put together a compelling argument for an appropriate sentence.

III. Addressing the real shortcomings of the child pornography guidelines

The current sentencing guidelines, while not as fatally flawed as defendants suggest, nonetheless do an inadequate job of capturing all the aggravating factors that may exist in a case. At bottom, the guidelines place a great deal of emphasis on the images, without a commensurate focus on the defendant's conduct. Of the six specific offense characteristics in § 2G2.2, half pertain to the images: the number of images and whether they depict prepubescent children or sadistic or masochistic activity. The remaining three enhancements cover types of distribution, the use of a computer, and the prior abuse of children, all of which portray only a slice of the full extent of a defendant's criminal conduct.

To counteract this imbalance, prosecutors should work with investigators to prepare a robust and complete sentencing presentation. As the guidelines dictated the relevant evidence at sentencing for many years, they became the de facto checklist for computer forensic analyses. Once all the evidence is found on a computer to trigger all possible sentencing enhancements, the analysis often stops. Under the guidelines, no added value in further investigation would exist. Thus, as prosecutors redevelop their approach at sentencing, they will need to work with investigators to get more information from the forensic exams. Evidence that can be presented in support of a sentence under § 3553(a) is described below.

A. Nature of defendant's criminal conduct

The possible factors that fully illuminate the nature and extent of the defendant's criminal conduct are near limitless. Prosecutors should think creatively for what kind of evidence will clearly demonstrate the defendant's commitment to his criminal conduct. Ironically, one good source for ideas about compelling aggravating factors is the Sentencing Guidelines themselves. Prosecutors can use enhancements provided for other crimes to argue by analogy for the requested sentence in a child pornography crime. For example, Sentencing Guideline § 2A2.1, addressing aggravated assault, calls for a higher sentence if the offense involved more than minimal planning, meaning the defendant took significant affirmative steps to conceal the offense. In a similar vein, a higher sentence may be appropriate in a child pornography case if the defendant took extensive steps to avoid detection. Sentencing Guideline § 2B1.1, which applies to larceny and theft, adds two, four, or six levels to the defendant's total offense level if more than 10, 50, or 250 victims are involved, respectively. This enhancement may be used to argue for a higher sentence when the evidence shows that the defendant exploited a large number of children, in supplement to the often criticized number of images enhancement in § 2G2.2. Likewise, § 2C1.8 increases the defendant's sentencing range for violating campaign contribution laws if he engaged in 30 or more illegal transactions. Prosecutors can argue by comparison that child pornography defendants who engage in extensive distribution or receipt activity should similarly receive a higher sentence. *See, e.g.*, *United States v. Whorley*, 550 F.3d 326, 342-43 (4th Cir. 2008) (affirming above advisory guidelines sentence in part because of defendant's "extensive history of downloading child pornography" that was not, except for one prior conviction, represented in the recommended Guidelines calculation). A number of the adjustments in Chapter Three of the Guidelines provide good fodder for sentencing arguments under § 3553(a), including the enhancement in § 3B1.1 if the defendant was an organizer or leader of criminal activity and the § 3C1.1 enhancement for obstruction of justice. *United States v. King*, 604 F.3d 125, 141 (3d Cir. 2010) (affirming application of § 3C1.1 in child pornography case when defendant destroyed hard drives); *United States v. Williams*, 250 F. App'x 725 (7th Cir. 2007) (affirming application of §3 B1.1 in child pornography case); *United States v. Reedy*, 304 F.3d 358, 370-71 (5th Cir. 2002) (same); *United States v. Tank*, 200 F.3d 627, 633-34 (9th Cir. 2000) (same).

In addition to these general suggestions, some more specific ideas to consider appear below as a starting point.

B. Extent and duration of defendant's criminal conduct

How long was the defendant collecting and possessing child pornography? How often was he downloading the material? For how many hours per day was he engaged in such activity?

This type of evidence serves many purposes. First, it can help refute the fallacy of the first time offender. Some district court judges focus very heavily on the fact that defendants convicted in child pornography trafficking cases often do not have prior criminal convictions. Evidence revealing the true extent of defendants' activity discredits this notion by showing that they have engaged in sustained, systematic criminal behavior. They are "first time" offenders only in the sense that they have never been previously caught and convicted. Furthermore, unlike many defendants in federal court, child pornography defendants are not career criminals, meaning they do not make their living through crime. This fact leads some courts to view these convicted felons as "otherwise law abiding citizens." But with evidence, for example, that a defendant was downloading child pornography hours a day, every day, prosecutors can argue that, in fact, the defendant was engaging in criminal conduct for a significant

percentage of his waking hours. *Cf.* U.S. SENTENCING GUIDELINES MANUAL § 2C1.8(b)(4) (2011) (plus two enhancements for engaging in 30 or more illegal campaign finance transactions).

For similar reasons, this evidence also responds to another common misperception about these defendants, namely, that their collection of child pornography is incidental, accidental, or casual rather than deliberate, intentional, and repetitive. *See Blinkinsop*, 606 F.3d at 1117 (fact that defendant obtained hundreds of images showing prepubescent children engaged in sadistic and masochistic sexual acts by using specific search terms contradict his contention that he was merely a "passive collector of [child] pornography" and "a marginal player in the overall child pornography business"); *United States v. Pugh*, 515 F.3d 1179, 1193 (11th Cir. 2008) (rejecting district court's characterization of defendant's conduct as incidental and passive in part because defendant "downloaded the child pornography images and videos at least 70 times over a period of several years"); *United States v. Goldberg*, 491 F.3d 668, 673 (7th Cir. 2007) (rejecting district court's characterization of defendant's collection and distribution of child pornography as "a kind of mischief" born out of boredom and stupidity, when evidence suggested he had been collecting pornography for ten years).

Finally, as the Supreme Court first recognized almost thirty years ago, the market for child pornography drives the sexual abuse of children to create more product. *New York v. Ferber*, 458 U.S. 747, 759-60 (1982). *See also Osborne v. Ohio*, 495 U.S. 103, 109-10 (1990) ("[The government] will decrease the production of child pornography if it penalizes those who possess and view the product, thereby decreasing demand."). Thus, the greater a defendant's involvement in the child pornography market, the greater his contribution to the demand for the sexual abuse of more children to provide more material. *See Pugh*, 515 F.3d at 1194-95; *United States v. Goff*, 501 F.3d 250, 259-60 (3d Cir. 2007); *Goldberg*, 491 F.3d at 672.

Much of this information is very easily obtained. For example, the date and time information that is obtained from a computer forensic examination or server-side data will reveal when the defendant began collecting child pornography (and can be as basic as the creation dates of the child pornography files or as general as a software installation date). Information may also exist in law enforcement records showing that the individual was the subject of a prior child exploitation investigation or incident report, and thus has been engaged in child exploitation activity for a longer period of time than may have been shown by the computer forensic examination. Prosecutors and law enforcement agents can contact CEOS for more information concerning these records.

C. Method of obtaining child pornography

How did the defendant search for child pornography? Was there any indication that the defendant was looking for a particular kind of child pornography, and if so, what was it? How did the defendant use the child pornography? What evidence shows that the defendant viewed, cataloged, or sorted the contraband?

All of this evidence tracks what would typically be offered at trial to establish the defendant's knowledge and intent. Because most cases are resolved by plea agreement, it may not be necessary to fully develop all of this evidence to establish guilt, especially in peer-to-peer cases where the defendant pleads to distribution or transportation. In those cases, it would not be strictly necessary to develop the evidence that shows how the defendant amassed his collection in order to obtain a conviction. However, evidence establishing how the defendant searched for the child pornography can be extremely useful at sentencing to illuminate the defendant's deliberate methodology. As noted above, many courts are receptive to the idea that a defendant's collection of child pornography was incidental, accidental, or unintentional. Courts may also accept that the defendant was collecting child pornography but may

somehow believe that the defendant did so without a genuine interest in the content of the images. Evidence that shows the time, effort, and care the defendant spent on the search for child pornography, that the defendant was acting deliberately, and that the defendant was actively using the child pornography images he obtained, will help refute this belief. Finally, this evidence can be used to negate the frequent complaint made by defendants that the specific offense characteristics pertaining to images of prepubescent children or sadistic or masochistic content apply whether or not the defendant intended to obtain such material. That complaint has no relevance to someone who was, in fact, seeking out that precise type of material.

Search terms used by the defendant and URLs typed by the defendant can be found in the Index.dat file, the computer's registry, and the computer's RAM. Information in those files can also determine whether a file was opened or played. Simple file structure can show how the child pornography was saved onto the computer. Prosecutors should pay particular attention to whether the defendant was using search terms that reflect a deeper knowledge of the market for child pornography. For example, while the phrases Lolita and pthc are unique terms in the child pornography market, they are fairly generic. In contrast, a defendant who searches for child pornography by series name shows that he has a greater depth of knowledge about child pornography generally and that he is looking for a specific kind of child pornography in particular. *Compare United States v. Ganoe*, 538 F.3d 1117, 1120 (9th Cir. 2008) (defendant convicted of knowingly receiving videos from BabyJ series) *with United States v. Buesing*, 615 F.3d 971, 977 (8th Cir. 2010) (defendant used search terms such as Lolita, pthc, and preteen).

D. Child sexual predator communities

Was the defendant participating in a community dedicated to the trade of child pornography?

Among child pornography defendants, those who find others to discuss child pornography and the sexual abuse of children are arguably more dangerous than those who are solo actors collecting the contraband in isolation (many defendants who use nothing other than peer-to-peer file sharing programs may fall into the latter category). When defendants communicate with like-minded individuals about child sexual abuse, they go through a process of bonding and normalization. Rather than feeling like an outcast who is ashamed of his sexual attraction to children, a defendant who is part of a pedophilic community instead comes to feel that his interest in children is legitimate and normal. The exchange of ideas, images, and instruction positively reinforces a defendant's sexual interest in children. Moreover, once a defendant finds a group dedicated to child pornography, he will then feel pressure to develop his standing within his new-found community. This desire to gain standing can mean amassing the largest collection, finding the rarest of images, or, worst of all, producing new material. Prosecutors should argue that this dangerous social dynamic is a significant aggravating factor because it is this dynamic that moves an individual from a collector to an abuser. *See* KENNETH V. LANNING, CHILD MOLESTERS: A BEHAVIORAL ANALYSIS (National Center for Missing and Exploited Children, 5th ed. 2001); Ethel Quayle & Max Taylor, *Model of Problematic Internet Use in People with a Sexual Interest in Children*, 6 CYBERPSYCHOLOGY & BEHAVIOR 93, 100 (2003).

If a defendant is a member of a group, prosecutors should look for evidence revealing the purposes and goals of the group. What is the group about? What does the group do? How does one become a member? What steps did the defendant have to take to find the group and gain access to it? What, if anything, did he have to offer in order to establish his bona fides to become a member? What is the hierarchy and structure of the group, and where does the defendant fit in? Are there rules of behavior that must be followed? What security procedures did members observe? What was the defendant's

contribution to the group? Prosecutors can use the evidence that answers those questions to illuminate for the court how deep a connection the defendant had to the market for images of child sexual abuse and his role and status within that market. The more formal the community and the more authority held by the defendant, the greater his dedication and commitment to the deviant subculture he has joined. *Cf. United States v. Allen*, 341 F.3d 870, 893, 897 (9th Cir. 2003) (affirming sentencing enhancement under U.S.S.G. § 3B1.1 in a civil rights case where evidence established that defendants formed a white supremacist group, developed rules and codes of conduct, taught the rules to new members, and controlled the status of group members).

If the defendant was participating in a Web-based forum, there may be references to the sites in the index.dat file, and remnants of the Web pages may be located in unallocated space. In addition, investigators should look for references to the defendant's online identity, screen name, or email address (often, the defendant's screen name specifically relates to child pornography, such as by adopting the name of the defendant's favorite series).

E. Defendant's communication with others

What did the defendant say to others, such as in chat logs or emails that capture the conversations? Did the defendant collect or write stories describing the sexual abuse of children?

More than any other evidence, the defendant's words reveal his inner thoughts and feelings about the sexual abuse of children. It is much harder for a defendant to credibly claim that he has no sexual interest in children if his own words contradict him. If nothing else, the fact that a defendant bothered to say something about child pornography shows that his interest in the material is not fleeting or incidental. In addition, chat logs or emails can reveal the bonding and normalization process described above and the encouragement that these like-minded individuals provide to each other. Such evidence may also demonstrate the defendant's distorted thinking. For example, he may have stories that describe the children reacting positively to the sexual abuse or that portray the adult in a role of a gentle educator of the child about the ways of sexuality. Defendants who labor under the false impression that children welcome sexual advances from adults are arguably more dangerous as they do not see sex between adults and children as a crime or even as something that is wrong. *See United States v. Brown*, 634 F.3d 954, 956 (7th Cir. 2011) (defendant's sentence based in part on disturbing and graphic discussions related to child pornography and sex with children, including one discussion in which the defendant said he wished he had a daughter so he could have sex with her); *United States v. Wayerski*, 624 F.3d 1342, 1354 (11th Cir. 2010) (affirming 365-month sentence for child exploitation offenses in part because defendant posted a diary entry where he described his sexual fantasies about an eight-year-old neighbor); *United States v. Overton*, 573 F.3d 679, 685, 700 (9th Cir. 2009) (defendant expressed belief that it was acceptable for adults to teach underage family members about sex and indicated he had an interest in teaching his teenaged stepdaughter about sex); *United States v. Caro*, 309 F.3d 1348, 1349-50 (11th Cir. 2002) (reversing defendant's below guideline sentence in case where defendant wrote stories describing sexual activity occurring between adults and children on a planet colonized by pedophiles, his desire to adopt a foster child so his wife could engage in sexual acts with little boys, and his wish for a seven-year-old girl so he could teach her to make love to little boys and dogs; and where defendant maintained a notebook containing hundreds of clippings of articles about young girls on which defendant had written captions describing the sex acts that he would like to perform with or see performed on the young girls).

Much of this evidence would be saved as files on the defendant's computer. If he was using a Web-based email program, such as Gmail or Yahoo, forensic examiners may be able to recover Web pages showing email text from unallocated space. Prosecutors should also consider whether to apply for

a search warrant to be served on the defendant's email provider to obtain the full existing content of the defendant's email account.

F. Use of child sexual abuse videos with sound

Is there any indication that the defendant played videos that included sounds of the child in distress or that showed the child was visibly afraid?

Experienced child exploitation prosecutors and investigators almost universally agree that videos that include the sound of child crying or screaming are the most devastating to view. In some cases, such videos would trigger the sadistic/masochistic specific offense characteristic as the child is reacting to a brutal physical assault. However, it is not difficult to imagine a scenario where a child could be audibly upset without the conduct reaching the physical extreme of sadistic abuse. Prosecutors can argue that defendants who deliberately sought, obtained, or played videos with sound should receive a higher sentence. *United States v. Abbate*, 2011 WL 3252574, *2 (5th Cir. July 29, 2011) (unpublished) (affirming upward variance in child pornography possession case in part because the defendant possessed videos in which the children could be heard screaming). Enjoying, or even tolerating, the sight and sound of a child in trauma suggests that the defendant disregards the emotional suffering of children. This lack of empathy suggests that the defendant is more dangerous. *See United States v. Maurer*, 639 F.3d 72, 78 (3d Cir. 2011) (sadists "delight in physical or mental cruelty"). As noted above, information in the registry file can show whether a file has been opened.

IV. Sophistication of the defendants' criminal conduct

Although other sentencing guidelines provide an enhancement if the defendant engaged in particularly sophisticated criminal conduct (such as the theft guideline at U.S.S.G. § 2B1.1(b)(9)(C) or the money laundering guideline at § 2S1.1), there is nothing truly comparable in the child pornography guidelines. It is an easy argument to make that more sophisticated conduct should be punished more seriously. Prosecutors can use the evidence described below to argue that the defendant's sentence should appropriately account for his sophisticated behavior.

A. Use of multiple methods to obtain child pornography

Did the defendant use different methods to obtain child pornography, such as through Web sites, Gigatribe, peer-to-peer, bulletin boards, and mail-order catalogs?

When a case begins, it is usually because the defendant has been caught acquiring child pornography a certain way. For example, an officer may have discovered the defendant making child pornography available through Limewire or the defendant may have been identified as a customer of a Web site that was selling child pornography. Prosecutors should never assume, however, that just because a defendant was caught using a given technology, that he was using that technology only. It is quite common for defendants to change their preferred method over time or to use multiple technologies at once. A defendant who is using a variety of means to collect child pornography is patently more committed to amassing a collection of contraband. Prosecutors should pay close attention to see if a defendant is using more than one technology at the same time, suggesting that the defendant is highly motivated to find child pornography. Alternatively, the evidence may show that a defendant has been serially sampling different approaches, perhaps in an effort to determine which technology gives him the most material and social interaction with the least risk of getting caught. *Cf. United States v. Landwer*, 640 F.3d 769, 770 (7th Cir. 2011) (noting the variety of methods used by defendant to commit fraud when upholding application of sentencing enhancement in mail fraud case). It can be relatively simple to

determine how a defendant is collecting child pornography. Sometimes, simply looking at the desktop of a defendant's computer will show what file gathering software programs are installed and a thorough search of the defendant's home should uncover any hard-copy material he has gathered.

B. Use of methods to avoid detection

Did the defendant use wiping software, encryption, proxies, or anonymizers to avoid detection? Did he hide his collection by storing it remotely?

It should be obvious that a defendant who is taking affirmative steps to hide his criminal activities has engaged in more serious behavior that warrants more serious punishment. Not only is such a defendant more dangerous because he is harder to find, he is more committed to his criminal activity, as he expends both the time and money to ensure that he can continue collecting child pornography. *Wayerski*, 624 F.3d at 1352 (affirming enhancement for obstruction of justice when defendants continuously changed encryption keys to decipher and encrypt material posted to newsgroups, periodically moved from one newsgroup to another and changed their nicknames, used sophisticated computer file swapping techniques requiring special instructions to reassemble files, and used special software programs that could lock down a computer or wipe it clean should law enforcement enter a member's home); *United States v. Knighton*, 307 F. App'x 673 (3d Cir. 2009). *Cf. Landwer*, 640 F.3d at 771; *United States v. Pizano*, 421 F.3d 707, 730-31 (8th Cir. 2005) (upholding application of sentencing enhancement in money laundering case when defendant engaged in extensive efforts to evade reporting requirements).

As stated above, the presence of these programs can easily be detected just by reviewing the software programs installed on the computer. If the defendant was storing child pornography on a third-party Web site, such as imagesource.ru, megaupload.com, or kodakgallery.com, references to those sites may appear in the index.dat file or hibernation files.

C. Method of distribution

Was the defendant recklessly indiscriminate in his method of distributing child pornography?

This area is one where prosecutors can argue that a defendant's lack of sophistication makes him more dangerous. Compare two scenarios. In one, a defendant hand selects a group of individuals to participate in a group online. Membership is tightly controlled and the members of the group only trade with each other. In that situation, the only people who can receive child pornography from any member of the group are other members of the group. On the other hand, consider a scenario where a defendant is making child pornography available for downloading through a commonly used peer-to-peer program such as Limewire. In that situation, anyone can obtain the images of child sexual abuse, including other children. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, FILE SHARING PROGRAMS: THE USE OF PEER-TO-PEER NETWORKS TO ACCESS CHILD PORNOGRAPHY, Report to Congressional Requesters, 3-4 (2005), *available at* http://www.gao.gov/new.items/d05634.pdf. Peer-to-peer distribution of child pornography is the moral equivalent of leaving loaded guns or a kilo of cocaine in the middle of the local mall. The indiscriminate distribution of child pornography threatens the safety and well being of innocent members of the public. This threat is an aggravating factor that is properly considered by the court at sentencing and is consistent with sentencing enhancements found in other contexts that call for increased penalties when defendants make controlled substances available to children or distribute them in protected spaces. *United States v. Clawson*, 408 F.3d 556, 558 (8th Cir. 2005) (upholding distribution enhancement when child knew location of and had access to defendant's zip disks containing child pornography). *Cf.*

U.S.S.G. § 2D1.1(b)(10) (drug distribution on premises where minor is present or resides); § 2D1.2 (drug offenses occurring near protected locations or involving under-aged individuals); and § 2K2.5 (possession or discharge of firearm in school zone). Once prosecutors determine whether and how a defendant distributed child pornography, they should work with investigators to ascertain if the program(s) would have allowed anyone to download the child pornography from the defendant.

V. Facilitation of criminal conduct

Did the defendant instruct others on how to avoid detection by law enforcement? Did he create a forum for the trading of child pornography? Did he request the production of new material?

These questions, placed in order of increasing severity, are meant to capture ways that child pornography defendants can aid and abet the criminal conduct of others. This evidence is obviously relevant because it establishes that the defendant was not acting in isolation but rather was facilitating yet more criminal activity. He was no passive participant in the child pornography market; rather, he was a leader. *Allen*, 341 F.3d at 893. Moreover, this evidence shows not just what the defendant did but how the child pornography market operates. This evidence goes to the core of the theory, first expressed in *New York v. Ferber*, 458 U.S. 747, 759-60 (1982), that demand drives supply and to provide the supply, children are sexually abused. It shows that these defendants are acting in concert by protecting each other and creating the manner and means to commit more crimes. In addition, by showing that this defendant has a strong presence in the child pornography community, it follows that he would have a community to return to once released from prison. The network is already in place for him to resume his criminal activity, suggesting that the defendant will continue to be a danger upon his release. All of these factors can be used in support of the appropriate sentence under § 3553(a). *United States v. Simkanin*, 420 F.3d 397, 418 (5th Cir. 2005) (in case involving failure to pay and collect taxes, it was appropriate for sentencing court to consider defendant's association with anti-tax organizations when assessing the likelihood that the defendant would engage in future criminal activity); *United States v. Tampico*, 297 F.3d 396, 403 (5th Cir. 2002) (in child pornography case, affirming upward departure based in part on defendant's membership in the North American Man Boy Love Association, because his association with NAMBLA suggests an increased likelihood of recidivism and decreased recognition of the gravity of the offense).

VI. Atmospheric evidence

Atmospheric evidence is the kind of evidence that is not illegal per se, but provides insight into the defendant's state of mind. In certain instances, atmospheric evidence can be something that is completely innocuous, even mundane, that in the defendant's hands becomes something alarming. For example, in one case, the defendant cut out images of children in underwear from the J.C. Penney catalog and put them in plastic sleeves in a binder. In another, the defendant, who had multiple prior convictions for contact offenses against children, had a simple video of children getting dropped off by a school bus. Other such evidence could include children's clothing in the home when no children live there; evidence suggesting the defendant had been masturbating at his computer (lotions, tissues, etc.); or employment or volunteer activities that bring the defendant into contact with children of a similar age and sex of those in the images. *See United States v. Wayerski*, 624 F.3d 1342, 1354 (11th Cir. 2010) (affirming 365-month sentence for child exploitation offenses in part because defendant was surreptitiously recording neighborhood children and was found in possession of a pair of panties stolen from an eight-year-old neighbor); *United States v. Buesing*, 615 F.3d 971, 976 (8th Cir. 2010) (defendant's possession of a video tutorial on how to molest a teenage daughter was considered as an aggravating factor at sentencing); *United States v. Ickes*, 393 F.3d 501 (4th Cir. 2005) (during border search of defendant's car, agent's

discovery of a video of a tennis match that focused almost exclusively on a young ball boy prompted a more thorough search that yielded extensive evidence of child pornography crimes).

The above list of evidence is not meant to be exhaustive, but rather offers some ideas about information that can be available to paint a fuller picture of the defendant's conduct. Prosecutors and investigators should assess each case to identify all possible aggravating factors that would support the requested sentence. Even if this approach does not completely stop the court from imposing a below guideline sentence, it may at least reduce the degree of the departure.

VII. Conclusion

The crescendo of skepticism from the courts about the seriousness of child pornography offenses should be taken as an opportunity. This pressure can be the catalyst for a major advancement in the quality of the government's sentencing advocacy in these cases. There is no doubt that those who investigate and prosecute these cases have the skill, dedication, and motivation to elevate their game at this critical juncture. Working together, we can develop the full facts of the case, freed from the limitations in the guidelines, and present a complete and compelling case to the courts that will help them understand not only the dangerousness of the defendant, but the seriousness of the crime.❖

ABOUT THE AUTHOR

❑**Alexandra R. Gelber** joined the Child Exploitation and Obscenity Section in the Criminal Division of the U.S. Department of Justice as a Trial Attorney in 2004. Since 2008, she has served as the Assistant Deputy Chief for Policy and Legislation. Prior publications include *Federal Jurisdiction in Child Pornography Cases*, U.S. Attorneys' Bulletin, November, 2006; *Establishing Federal Jurisdiction in Child Prostitution and Sex Tourism Cases* (with co-author Wendy Waldron), U.S. Attorneys' Bulletin, November, 2006; and *A Response to "A Reluctant Rebellion,"* Department of Justice, July 1, 2009.✠

The Fallacy of Simple Possession: The Impact of Targeting, Charging, and Plea Bargaining at Sentencing

Drew Oosterbaan
Chief
Child Exploitation and Obscenity Section

I. The debate

In nearly twenty five years as a prosecutor, I have handled a broad array of criminal offenses, from simple larceny to international drug trafficking. I have incarcerated rapists, airline hijackers, armed career criminals, and corrupt federal agents. In these cases, an offender's motive, intent, and purpose are generally clear from the facts and readily grasped. The grade of seriousness attributed to these offenses is not a matter of real dispute. When it comes to sentencing factors, prosecutors, defense lawyers, probation officers, and sentencing judges typically disagree only at the margins. Child pornography collectors, however, seem to stand in distinct contrast to this norm because the nature and seriousness of their crimes are not as easily understood. Indeed, within the realm of judges, lawyers, and other practitioners, child pornography collectors are currently the subject of significant debate largely flowing from differing opinions concerning how dangerous these offenders are and how serious their crime is. For those of us who are witness to these crimes through investigation and prosecution, however, evidence suggests that many of these offenders are quite dangerous and that their crime is severe.

The truth of perception, however, is in the evidence. Misapprehension thrives in the absence of indication and can be a considerable obstacle to appropriate sentencing in child pornography cases. As most experienced federal prosecutors will attest, battling misperception has long been a part of handling these cases, especially in securing resource commitments. This battle was a particularly serious problem in the 1990s when the Internet was taking hold. In the early 2000s, however, a collective and concerted effort to raise awareness amongst policy-makers and the public resulted in a dramatic increase in efforts to address child sexual exploitation crimes. This effort culminated in the launch of Project Safe Childhood in 2006 that targeted technology-facilitated child exploitation crime. At the Child Exploitation and Obscenity Section, we worked to raise awareness of this crime by leveraging our functional partnerships with United States Attorneys' offices and our proximity to policy makers and media outlets to generate broader recognition that child pornography offenders pose a serious threat to all children and merit a vigorous response by all levels of law enforcement. From this effort by the Department and other stakeholders, it seems, the public in general came to value and support our efforts to protect our children through child pornography enforcement, even if substantiation of the nature and seriousness of the crime was not fully available to them.

With growing public awareness, and perhaps as a result of it, politicians responded. Over the last decade Congress has taken firm legislative steps such as increasing penalties for child exploitation offenders and mandating that the U.S. Sentencing Commission make certain changes to the child pornography Sentencing Guidelines. Congress' reaction has had mixed results. On the one hand, Congress provided enhanced tools and sentencing features, of which prosecutors have taken full

advantage. On the other, Congress' response has been interpreted by some outside law enforcement circles as motivated more by politics than by any actual threat to children. In the absence of clear evidentiary support, it is easy for those so inclined to question mandatory sentencing designations, sentencing guidelines, and other legislative stricture as merely the result of legislators burnishing reputations for moral potency.

We have seen this sentiment increasingly expressed in exhortative public objections to the Guidelines from judges and defense counsel, and impact is emerging. In February of this year, the Associated Press published an article on the debate that is simmering. Among other things, the article claimed, "[d]efense attorneys, legal scholars and even some federal judges bemoan the prosecution and sentencing developments as draconian for failing to distinguish between hardcore producers of child pornography and hapless Web surfers with mental problems." PAUL ELIAS, CHILD PORN PROSECUTIONS SOARING (2006), *available in* Westlaw, 2/5/11 APALERTCA 19:05:25. An article appearing in the ABA Journal, titled "*A Reluctant Rebellion*," raised questions about the child pornography sentencing guidelines. MARK HANSEN, A RELUCTANT REBELLION (2009), *available at* http://www.abajournal.com/magazine/article/a_reluctant_rebellion/.

The author acknowledges that producers of child pornography—those known to be molesting a child—are committing serious offenses. However, the author cites a number of critics who depict the individuals collecting, trading, viewing, and possessing these images as "otherwise law abiding" citizens who merely enjoy an odd and even deviant form of sex, but who do so in the "privacy of [their] own home." The article suggests that serious sentences for these offenses are motivated by a puritan ideal and by "polite society's disgust and revulsion" with pornography. This sentiment is summed up by one jurist who commented, "our federal legal system has lost its bearings on the subject of computer-based child pornography. Our 'social revulsion' against these 'misfits' downloading these images is perhaps somewhat more rational than the thousands of witchcraft trials and burnings conducted in Europe and here from the Thirteenth to the Eighteenth Centuries, but it borders on the same thing." *United States v. Paull*, 551 F.3d 516, 533 (6th Cir. 2009) (Merritt, J., dissenting).

II. The impact

It may not be a "rebellion," but the intellectual debate about the nature of child pornography offenses, what penalties are appropriate for those crimes, and the risks posed by those who commit them is rising. The debate is understandable, at least to some degree, because research concerning issues such as the link between child pornography offenses and contact sexual abuse offenses and the extent to which child pornography offenses stimulate a demand for the production of new child pornography images has not yet definitively resolved these questions.

For prosecutors and investigators this is far more than an academic debate. The arguments of objectors have held sway at judicial and sentencing conferences and members of the U.S. Sentencing Commission have taken note. Commission staff members have reviewed sentencing statistics in child pornography cases and found inconsistency, a finding that even without the benefit of national statistics a growing body of federal prosecutors handling child pornography cases could have forecasted. Whether as a result of now advisory (and perhaps flawed) Guidelines or the uncertainty engendered by growing debate, prosecutors across the country handling child pornography cases are experiencing a disproportionate rejection of the Sentencing Guidelines by judges. This condition and strategies to address it are discussed at length in Alexandra Gelber's article titled, "*Beyond the Child Pornography Sentencing Guidelines: Strategies for Success at Sentencing*," also published in this issue of the Bulletin.

Of course, not all child pornography cases are affected in this way. Prosecutors usually have no trouble securing appropriate sentencing results in production cases, for instance. However, U.S. Sentencing Commission statistics show that "simple" possession cases, the count of conviction in the vast majority of child pornography cases, yield widely varied results across the country and a strongly disproportionate number of below-Guideline sentences. And, of course, the penalties in "simple" possession cases are those that draw the harshest criticism from detractors.

Those experienced in investigating and prosecuting child pornography cases readily reject the criticism levied against possession cases. Indeed, many in law enforcement bristle at the term, "simple possession," and for good reason. "Simple" possession is fallacy—in truth, there is no such thing. Illuminating this point, however, requires a return to the discussion above about evidence. Prosecutors and investigators experienced in child pornography cases are convinced that a collector of child pornography presents a danger to the community because this threat has been proven in thousands of cases over years of progressively effective investigative work. Ours is a deeply experienced, expansive, and collective view derived from vast amounts of evidence. More to the point, however, ours is a highly specialized and unique view shared with the unaware through only one means: prosecution. The courtroom is not only where we make the case about an individual offender to the judge but is also where we develop the evidence for a broader dialog with the public. If we fail to make the case for the seriousness of the offender in the courtroom, we are effectively taking our voice out of the national debate.

III. Making the case for a more serious offender

If taken in full view, ample evidence is present that collectors of child pornography inherently pose an unacceptable risk of contact offenses against children and should be treated as serious offenders at sentencing. Law enforcement in the United States has been bringing prosecutions against child pornography possessors for decades and our record indicates that many collectors are abusing children as well. But there are more primary reasons to address child pornography collectors. If collectors of sexually abusive images of children never molested children (which, of course, is not the case) they would still directly contribute to the exploitation and even the sexual abuse of children and would merit strong criminal justice action. The Supreme Court long ago noted that the heart of a child pornography case is the endless sexual exploitation of a child through the ongoing mass circulation of images of their abuse. *New York v. Ferber*, 458 U.S. 747, 758 (1982) ("[T]he use of children as subjects of pornographic materials is harmful to the physiological, emotional, and mental health of the child."). In the words of one victim who was repeatedly bound and raped by her father for two years, starting when she was ten:

> thinking about all those sick perverts viewing my body being ravished and hurt like that makes me feel like I was raped by each and every one of them. I was so young. . . . It terrifies me that people enjoy viewing things like this. . . . Each person who has found enjoyment in these sick images needs to be brought to justice . . . even though I don't know them, they are hurting me still. They have exploited me in the most horrible way.

The Supreme Court also observed that perhaps the only practical way to stop the production of child pornography is to give severe sentences to child pornography offenders, the individuals who stimulate the demand for a constant stream of new images that can only be produced by sexually abusing a child. *Ferber*, 458 U.S. at 760 ("The most expeditious if not the only practical method of law enforcement may be to dry up the market for this material by imposing severe criminal penalties on persons selling, advertising, or otherwise promoting the product."). The traffic of child pornography on the Internet indeed exhibits the characteristics of a marketplace and each person who draws from this

virtual market is compelling the production of new images. Many offenders compulsively collect images. The collections are often meticulously organized by name of the child, sex of the child, age of the child, or type of sexual activity depicted in the image of the child. Collectors use these images much like currency, trading images for new ones that are highly coveted. The drive in this underground market is to collect new images. It is easy to see how this would drive the abuse of children to satisfy the never-ending demand for new images and would turn some collectors into producers, creating images of their own sexual abuse of children in order to have new, and therefore valuable, currency on the Internet.

This risk presented by child pornography collectors is especially evident when offenders participate in online groups, forums, or social networking sites centered on pedophilic interests. In these online forums, the discussion of child sexual abuse flows as freely as might the discussion of hydrangeas in a gardening forum. The talk in child abuse forums, however, is distinctively worrisome. In one online group investigated recently, for instance, a member posted a survey asking, "have you thought about whether or not you would abduct a preteen girl/boy?" Over fifty percent of the responders answered, "I would absolutely do it" or "if the circumstances were right, I'd do it." In another investigation, a member of an online assemblage of producers and traders of child pornography talked about how he was eagerly anticipating the opportunity to molest his daughter, who had not been born yet. He posted a message exclaiming, "o man do i have some news i have a new baby about to be added to the game i will share her pics when i get some." Shortly thereafter, a sonogram image of his unborn daughter in the womb was posted. A member of yet another online forum posted a solicitation to his fellow members offering to pay $1,000 dollars per hour, up to a maximum of $50,000, for access to a child, with the restriction that the child be a blond-haired, blue-eyed girl between seven and nine years of age.

Forums with large memberships dedicated to the sexual abuse of children and the exchange of its graphic imagery are ubiquitous on the Internet. Indeed, groups of people with pedophilic interests have taken extensively to social networking platforms. In all of these groups, we consistently find certain common characteristics: the sites constitute a thriving marketplace for the exchange of child pornography; they are hierarchical and members' upward progression is achieved most readily by producing child pornography and distributing it to other members; and communication between members typically normalizes, encourages, and facilitates the sexual abuse of children. Given these characteristics, law enforcement officers addressing child pornography are confident that online collectives like these, and the individuals who belong to them, are worthy of careful attention because they indicate a real risk to children.

For the last few years, the Child Exploitation and Obscenity Section has addressed child pornography offenders operating in online groups in close partnership with the Federal Bureau of Investigation's Innocent Images National Initiative, the Bureau of Immigration and Customs Enforcement Child Exploitation Section, and the U.S Postal Inspection Service's child exploitation unit, as well as our foreign law enforcement colleagues because online child exploitation offenses are increasingly international in scope. Through coordinated enforcement operations, more than a dozen such groups, including some with more than 1,000 members, have been identified and dismantled. Leads generated from these operations have resulted in countless prosecutions across the country, either as cases against individual offenders, or as large child exploitation enterprises and conspiracy prosecutions where a considerable number of defendants have been convicted in a single case. Given the commitment by each of the federal investigative agencies to these large-scale international investigations, it is fair to say that the number of individual cases generated by these operations will continue to rise.

IV. A way forward: Prioritization

Individual prosecutors may be without capacity to remedy intractable issues such as inadequate computer forensics support, increasingly-questioned sentencing guidelines, or deeply-held questions about the gravity of child pornography offenses, but prosecutors do have the means to right the ship on sentencing. Indeed, I believe that only prosecutors can reverse the downward sentencing trend. Ms. Gelber's article discusses sentencing strategies that are critically necessary to any such effort, but the foundation for an appropriate sentence is built well before the sentencing hearing with deliberate targeting, charging, and plea bargaining.

In the federal system, prosecution guidelines emphasize prioritization. Limited resources and judicial economy require that we bring cases with the most prospective impact. Even if United States Attorneys were to find themselves flush with resources, District Court judges generally have little time and capital for small cases. Priority targeting of child pornography cases can ensure that judges are consistently seeing evidence that reveals the behavioral characteristics of these offenders and paints a clear picture of risk. With these things in mind, federal prosecutors and investigators handling child pornography cases should develop a method of prioritizing among offenders based on factors more indicative of an individual offender's risk to society than the size of the his collection and the age of the children in the images. Certain criteria rise naturally to the top, such as pertinent criminal history, access to children, or production of child pornography, but other factors also exist and serve as true indicators of risk and gravity.

In weighing such factors, we should remember that the conduct of child pornography offenders evolves over time. Given resource limitations, a reasonable approach would be to target offenders who are farther along in offending. Many offenders seen online today have been involved with child pornography for ten years or more. The child abuse material they found adequately satisfying when they first found access to it has lost its affect. The sexual abuse images and videos they seek now are more diverse and certainly more extreme, and the methods they use to collect it are more sophisticated. One additional and critically important aspect to understand about these offenders is that their evolution is social. Offense conduct typically begins in isolation, but offenders quickly connect with others online and find acceptance and status not present in their lives offline. An offender's behavior becomes strongly influenced by a group dynamic offering a unique source of inspiration, normalization, validation, encouragement, and social significance. In short, an offender can transform and become more dangerous in the process.

Despite the move to address online groups, forums, and communities, online collectives often receive less investigative attention than individual offenders who trade anonymously through Peer-to-Peer programs. Thus, the federal system will continue to register convictions for a large number of child pornography possessors who were discovered through Peer-to-Peer investigations. Currently, a significant majority of federal cases are developed through Limewire P2P investigative programs. These investigations use software designed to find images of child pornography on the Limewire network and identify the individual offering it for download to other Limewire users. These programs are particularly popular with the Internet Crimes Against Children Task Forces and other state and local law enforcement agencies because the software finds and identifies collectors residing within their jurisdiction quickly, easily, effectively, and cheaply. One potential problem with these programs, however, is that they often result in prosecution packages containing very little evidence that may be helpful in assessing the defendant's risk to society and the seriousness of his conduct. By design, these cases are built for speed. Forensic examination of the computer evidence in these cases can be very narrow, resulting in image extraction and just enough information to establish the identity and knowledge of the defendant. Forensic

evidence probative of motive and purpose that can be difficult to obtain in even the most significant cases is frequently found lacking in P2P cases. Overcoming forensic shortfalls is made appreciably more difficult by the applicable sentencing guideline scheme that provides no incentive to develop such evidence. A lack of salient evidence like this becomes a critical impediment to a worthy sentence when the case falls before a skeptical judge.

Even in districts where forensic examinations are more robust, however, investigative programs that disproportionately target Limewire users may not be optimal. As a general matter, it is unlikely that the truly dangerous child pornography collectors are using Limewire exclusively because: (1) it offers no opportunity for social interaction; (2) users of Peer-to-Peer programs are vulnerable because it is relatively easy for officers to identify individuals who are offering known child pornography for trading; and (3) astute offenders will know that law enforcement efforts are focused on Limewire, so they will understandably opt to use other technologies or even other P2P networks that enjoy far less police scrutiny. This is not to say that P2P investigations never identify extremely dangerous offenders or that such investigations should be abandoned altogether. Rather, the key points are these: a case that begins as a P2P investigation does not mean it must end as a P2P investigation, as further investigation may uncover evidence of more extensive activity; and a comprehensive investigative response to child pornography offenses cannot be predicated on P2P cases alone.

Prosecutors should consider another unintended negative consequence of premising too many federal cases on the same pattern of conduct. The near exclusive focus on Peer-to-Peer cases results in systemic conditioning of the entire federal criminal justice system. From the investigators and computer forensic analysts to the prosecutors, to the defense bar, and to the judge and probation officer, this one kind of offender comes to represent the entire universe of child pornography offenders. It stunts everyone's ability to see the hierarchy of offenders and the full range of their criminal conduct when all the cases brought to court involve the same criminal activity. This condition is especially harmful where forensic examination and other investigation fail to address risk because defendants can freely present themselves as "hapless Web-surfers with mental problems" with no evidence in contradiction.

To counteract this systemic conditioning, prosecutors and investigators should widen the net and ensure that investigative priorities and methods are purposefully calibrated. Prioritization based on the risk of offenders and the seriousness of conduct requires taking a hard look at the scope and methodology of the investigations conducted in each district. Is law enforcement looking in the places where they are likely to find the most serious offenders? Complex, proactive investigations are being conducted throughout the country, netting as many defendants in a single case as might be prosecuted in an entire year of Limewire cases. These operations target sophisticated group-dwellers who pose an ever-growing threat to children. Unlike the one-dimensional offender too often presented in Limewire cases, group-dwellers encourage each other to exploit innocent children to produce what they all seek, new and more extreme child sexual abuse images. The investigations are difficult because members operate in security-conscious online communities, using complex technologies, such as encryption and anonymization, to cloak their crimes, but this is only more reason to pursue them. Operations like these will not and should not replace P2P based investigations, at least not in the near term, but they should become an integral part of a broad-based investigative strategy to eradicate this crime and bring the most serious offenders before federal courts.

V. Beyond targeting: Local investigation, charging, and plea agreements

Priority targeting increases the likelihood that more serious or risky offenders will be prosecuted, but it does not guarantee it. Evidence collected at the on-site investigative stage can be invaluable in

establishing risk and seriousness at sentencing, and nothing is more valuable at this stage than a full and detailed confession. When interviewing a defendant, investigators should ask the defendants detailed questions designed to paint a clear picture of his conduct, method, and motivation. How did the defendant obtain child pornography? What was he looking for? How did he look for it? How long had he been collecting child pornography? Why? Does he communicate with others online about child pornography? What do they talk about? Does this group or forum have a name? Is there a hierarchy and, if so, how are the levels determined? In this area, details matter. A significant difference exists between a confession where a defendant says he was downloading inappropriate images of children and one where the defendant admits he deliberately sought and knowingly downloaded material that shows toddlers engaged in sex acts with animals. In the minds of judges at sentencing, this kind of detail transforms a case from "simple" possession into something much, much more.

Investigators should be counseled to assess the risk posed by a child pornography offender throughout the investigation and to develop evidence of this risk where possible. At the search scene, investigators should look for evidence of an obsessive interest in children that may be found by investigating the offender's reading material, movies, photographs, and writings. Additionally, an offender's volitional involvement with children may be very probative in assessing the gravity of risk. While an offender's occupational contact with children will likely be readily apparent, such as in the case of pediatricians, contact with children through volunteer activities, such as church-based youth counseling, may not be. Investigations should always include a thorough search for a defendant's volunteer or informal activities involving children.

A targeting strategy fails in the end if charging decisions and the government's plea posture fall short of the principles that the strategy is based on. Charging and plea agreements should reflect the conduct for which the defendant should be sentenced. As discussed above, investigations should extract detail about the defendant's offense conduct going well beyond the images and videos he possessed. Evidence establishing the length and breadth of an offender's conduct and his motivation is almost always available in some form and to some extent. Counts of conviction should reflect this evidence and the factual resume of a plea agreement should include as much of this detail as possible. The best way to ensure that a defendant receives the sentence he deserves is to ensure that he faces sentencing on the most serious charges.

VI. Conclusion

The rising debate about the nature, seriousness, and risk associated with child pornography offenders has had an impact on sentencing in the United States. In the federal system, the arguments of those who feel that the Sentencing Guidelines are baseless and their prescripts too severe have been influential. Whether as a result of uncertainty engendered by the debate or as a condition of advisory Sentencing Guidelines, there has been a disproportionate rejection of the guidelines by judges in child pornography cases. While there is ample evidence that child pornography collectors warrant serious concern for the risks they present to society and that their offenses warrant severe punishment, such evidence is not always made available to judges at sentencing. As a result, sentences in child pornography possession cases, in particular, appear to be experiencing an unjustified downward trend. Investigators and prosecutors can reverse this trend and ensure appropriate sentences if their investigations reflect a priority for more serious offenders and a concerted effort to obtain evidence that will establish risk and seriousness at sentencing. Prosecutors' charging decisions and plea posture must also reflect defendants' most serious conduct. We cannot ask the court to treat the defendant as a serious criminal if we do not ourselves hold the defendant accountable for his most serious conduct.❖

ABOUT THE AUTHOR

❑**Drew Oosterbaan** has been the Chief of the Child Exploitation and Obscenity Section since 2001. Before becoming Chief, he served as Deputy Chief of the Child Exploitation and Obscenity Section. Mr. Oosterbaan served at the U.S. Attorney's Office in the Southern District of Florida, from 1990 through 1999, as Chief of the Special Investigations Unit, Deputy Chief of the Special Prosecutions Section, and as an Assistant United States Attorney in the Major Crimes and Public Corruption Sections. Before joining the U.S. Attorney's Office, Mr. Oosterbaan was a prosecutor with the U.S. Army Judge Advocate General's Corps in Germany. In 2009, the President honored Mr. Oosterbaan with the Presidential Distinguished Rank Award of Distinguished Executive, the nation's highest civil service award.✠

The author would like to acknowledge the assistance of Alexandra R. Gelber, Assistant Deputy Chief, Child Exploitation and Obscenity Section, in the preparation of this article.