

I N S I D E T H E M I N D S

Strategies for Defending Internet Pornography Cases

*Leading Lawyers on Analyzing Electronic
Documents, Utilizing Expert Witnesses, and
Explaining Technological Evidence*



ASPATORE

©2009 Thomson Reuters/Aspatore

All rights reserved. Printed in the United States of America.

No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, except as permitted under Sections 107 or 108 of the U.S. Copyright Act, without prior written permission of the publisher. This book is printed on acid free paper.

Material in this book is for educational purposes only. This book is sold with the understanding that neither any of the authors or the publisher is engaged in rendering legal, accounting, investment, or any other professional service. Neither the publisher nor the authors assume any liability for any errors or omissions or for how this book or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this book. For legal advice or any other, please consult your personal lawyer or the appropriate professional.

The views expressed by the individuals in this book (or the individuals on the cover) do not necessarily reflect the views shared by the companies they are employed by (or the companies mentioned in this book). The employment status and affiliations of authors with the companies referenced are subject to change.

Aspatore books may be purchased for educational, business, or sales promotional use. For information, please email West.customer.service@thomson.com.

For corrections, updates, comments or any other inquiries please email TLR.AspatoreEditorial@thomson.com.

First Printing, 2009

10 9 8 7 6 5 4 3 2 1

If you are interested in purchasing the book this chapter was originally included in, please visit www.Aspatore.com.

Internet Pornography Laws, Precedents, and Defense

Kathleen M. Sweeney

Attorney

Sweeney Law Group LLC



ASPATORE

Government

The primary federal law enforcement agencies that investigate domestic crime on the Internet include the Federal Bureau of Investigation, the U.S. Secret Service, U.S. Immigration and Customs Enforcement, the U.S. Postal Inspection Service, and the Bureau of Alcohol, Tobacco, and Firearms. All of these agencies will coordinate with the local U.S. attorney's office.

The child exploitation and obscenity section in the Department of Justice's criminal division is responsible for enforcing Internet pornography laws. In May 2006, the then U.S. Attorney General Albert Gonzales launched an initiative titled "Project Safe Childhood." Through the coordinated efforts of federal, state, and local law enforcement agencies, President George W. Bush and Attorney General Gonzales promised to "prosecute predators and rescue their victims." Office of the Attorney General, "Project Safe Childhood: Protecting Children from Online Exploitation and Abuse," May 2006, available at www.projectsafechildhood.gov. The Internet division, in particular, consists of a network of forty-six task forces, established throughout the United States, to investigate, enforce, and prevent Internet crimes.

Every U.S. attorney's office in the country has a task force dedicated to investigation and prosecution of child pornography. Typically, agents enter chat rooms under pseudonyms and participate in discussions about obtaining pornographic images. After gaining a client's trust, and numerous images are exchanged over time, the agent seeks a subpoena to determine the subscriber information, and a warrant to seize the computer from which the images were sent. Once the client's hard drive has been examined, frequently new targets are located through the e-mail files. And the sting goes on.

A D.C. court of appeals has determined that 18 U.S.C. §2252(A)(5)(B) (2008) is a valid exercise of Congress's right to regulate commerce under the Commerce Clause of the Constitution. *U.S. v. Sullivan*, 451 F.3d 884 (DC App. 2006); *see also U.S. v. Rodia*, 194 F.3d 465 (3rd Cir. 1999) *cert. denied* 2000. Furthermore, 18 U.S.C. §2252(a)(4)(B) (2008) was held to be a proper exercise of Congress's power under the Commerce Clause, since it

contained explicit jurisdictional element. The fact that laws prohibiting child pornography were consistent with community moral standards ensured probability of notice—government need not have proven that the defendant had actual knowledge of jurisdictional element of §2252(a)(4)(B). *U.S. v. Robinson*, 323 F.2d 1114 (9th Cir. 2003).

However, there is no jurisdiction if the Commerce Clause is not implicated. Therefore a stepdaughter could not satisfy the requirements of 18 U.S.C. §2252 absent evidence that her stepfather shipped or intended to ship sexually explicit videotape he made of her when she was a minor. *Smith v. Husband*, 428 F. Supp. 2d 432 (E.D. Va. 2006).

Congress declared that in enacting Sections 2252 and 2256 of Title 18 of the U.S. Code, it was the intent of Congress that “the requirements in Section 2252(a)(1)(A), (2)(A), (3)(B)(i), and (4)(B)(i) that the production of a visual depiction involve the use of a minor engaging in ‘sexually explicit conduct’ of the kind described in Section 2256(2)(E) are satisfied if a person photographs a minor in such a way as to exhibit the child in a lascivious manner.” Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, Title XVI, §160003(a), 108 Stat. 2038 (1994).

“Lascivious” is not unconstitutionally vague, since it has the same meaning as “lewd,” which has been held to be constitutional by the U.S. Supreme Court. “Lascivious exhibition of the genitals” is not limited to depictions of minors presenting sexual activity or willingness to engage in it, but includes all depictions featuring children as sexual objects, so presented as to arouse or satisfy sexual cravings of a voyeur. *U.S. v. Wiegand*, 812 F.2d 1239 (9th Cir. 1987), *cert. den.* 484 U.S. 856 (1987).

More than mere nudity is required before images can qualify as lascivious within meaning of 18 U.S.C.S. §2256(2)(E)(West 2008). A picture is lascivious only if it is sexual in nature. Thus, the statute is violated, for instance, when a picture shows a child nude or partially clothed, when the focus of the image is the child’s genitals or pubic area, and when the image is intended to elicit a sexual response in the viewer. *U.S. v. Kemmerling*, 285 F.3d 644 (8th Cir. 2002), *cert. den.* 537 U.S. 860 (2002).

Internet crimes such as computer intrusion (i.e., hacking), identity theft, password trafficking, and counterfeiting involve the theft and/or movement of money and/or valuable data. Central in the investigation of these types of crimes is unraveling the layers of secrecy that the Internet allows. The shroud of secrecy makes it difficult for investigators to determine who is involved in the scheme, and even the precise parameters of any scheme.

In contrast, Internet pornography can be divided into two categories: obscenity and child pornography/child exploitation. Obscenity law, as defined by the U.S. Supreme Court (the Miller test), is material that is patently offensive to an average person based on community standards. Obscenity prosecutions historically involved the local dirty bookstore and hardcore magazines or videos. The community standard then was what the twelve citizens of that city or town decided they were. But in an Internet obscenity prosecution, it is frequently argued that there is no community standard that can apply. Or if there is a community standard, which community should be chosen? The community from which the image was produced, the community from which the image was transmitted, or the community where the image was received? As a result, typically only the most extreme examples of commercial Internet obscenity have been prosecuted. In the cases that are prosecuted, pre-trial litigation of the applicable community standard is an important focus in the defense. Any defense of Internet pornography should also focus on what is available for purchase from local cable companies. One untapped area is the use of focus groups prior to trial, typically not utilized in criminal cases.

Because of the difficulty of prosecuting Internet obscenity cases, most Internet pornography prosecutions will involve child pornography—its possession, receipt, and production. Defense of these cases can be challenging, because the law concerning Internet sex crimes is somewhat new and the allegations of committing such a crime carry a much greater stigma than any other area Internet criminal defense.

Internet child pornography also involves many types of illegal activities, not just one illegal act, as is the case in most other Internet crimes. For example, a defendant charged with Internet child pornography may be prosecuted for:

- Internet child pornography under the statutes
- Downloading or uploading child pornography
- Answering an advertisement for child pornography
- Unlawful contact with a minor or underage teen
- Online solicitation or enticement

This particular area of Internet crimes is particularly difficult to navigate, due to the slippery slope of the freedoms sacrificed versus the punishment of the few transgressors. Therefore, constitutional issues are at stake in every litigated case, and the outcomes of these cases may have great repercussions on mandated censorship and other First Amendment issues.

Internet child pornography cases also involve a greater likelihood of a mistake or error, since images are frequently downloaded from Web sites in bundles, or information is automatically downloaded to a computer with software from newsgroups or other unscreened public areas, and therefore the potential that a defendant was not aware of the files being on his or her computer are substantial.

Most other Internet crimes typically involve an affirmative act taken by the defendant, and can be easily proven or disputed. Other crimes also present the defendant with an opportunity to prove his or her innocence and continue with their lives. However, due to the stigma attached to child pornography, popularity of shows such as the Dateline “Crime Stoppers,” and general community disapproval of such behavior, an accusation that an individual possessed child pornography, even if he or she is proven to be innocent, will destroy that person’s reputation and standing in the community for the remainder of his or her life.

Most of the Internet crimes really do carry the presumption of innocent until proven guilty. However, like the defense of those accused of child molesting, the mere accusation tends to create a presumption of guilt among potential jurors. Significant time should be spent in *voir dire* on the venire’s reactions to and presumptions about your client, once they learned of the crimes charged.

Currently, the most difficult pornography laws to enforce involve the prosecution of obscenity. It is difficult to define obscenity, given the degree of explicit conduct shown and discussed on cable stations and even portrayed in daily advertisements. Additionally, given the borderless community of the Internet, community standards are just as difficult to define.

Child pornography cases are the most often tested cases. Year after year, federal and state legislators expand prohibited conduct that is more geared to sound bites than to well-constructed and directed laws. One example is the 2003 Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act (the PROTECT Act) passed by Congress. The PROTECT Act lengthened the statute of limitations for child abduction crimes and expanded the definition of pornography, and made other modifications to 18 U.S.C. § 2252. In 2006, the Eleventh Circuit found that the act's pandering provision was unconstitutional on its face because it was overbroad and vague. *U.S. v. Williams*, 444 F.3d 1286 (11th Cir. 2006).

History of Pornography Law

On October 18, 1986, President Ronald Reagan signed P.L. 99-500 (H.J. Res. 738), a bill that laid the foundation for the current 18 U.S.C. §2252. It was soon discovered that certain provisions had been omitted from the bill, and a corrected version thereof was signed on October 30, 1986, as P.L. 99-591.

On May 21, 1984, the statute was amended by substituting "visual depiction" for "visual or print medium," and significantly decreased the monetary penalties to be imposed on violating persons. On October 18 and October 30, 1986, the prison term was reduced from "not less than five years" to "not less than two years." On November 18, 1988, in the introductory matters of Subsection (a), in paragraphs (1) and (2), the phrase "by any means including by computer" was inserted, wherever appearing. On September 13, 1994, the phrase "or attempts or conspires to violate" was inserted in Subsection (b)(2). On October 30, 1998, Congress added Subsection (c) and substituted "aggravated sexual abuse, sexual abuse, or abuse sexual conduct involving a minor or ward, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation

of child pornography” for “the possession of child pornography.” On April 30, 2003, in Subsection (b)(1), Congress substituted twenty years for fifteen, and in Subsection (b)(2) substituted ten years for five and twenty years for ten in regards to imprisonment for persons with prior convictions under this or other related chapters. On July 27, 2006, in Subsection (b)(1), the phrase “or sex trafficking of children” was inserted.

Additionally, there have been numerous attempts to regulate Internet speech to protect minors from sexually explicit material. In 1996, Congress passed the Communications Decency Act, which made it a criminal offense to transmit or make available to minors “obscene or indecent” communications over the Internet. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified at 47 U.S.C.A. §223). However, in *Reno v. ACLU*, 521 U.S. 844, 870-71 (1997), the court held that the Communications Decency Act’s indecency prohibition was a content-based regulation of speech that was written so broadly that it unconstitutionally chilled free speech. The Communications Decency Act now only prohibits transmissions to minors, which would qualify as obscene under *Miller v. California*, 418 U.S. 915 (1974). See also *Nitke v. Ashcroft*, 253 F. Supp. 2d 587, 594 (S.D. N.Y. 2003).

In 1996, Congress also passed the Child Pornography Protection Act, which criminalized the possession, transmission, or pandering of child pornography. Child Pornography Protection Act of 1996, P.L. 104-208, Title I §121, 110 Stat. 3009 §121, 110 Stat. 3009 §121 (1996) (codified at 18 U.S.C.A. §§2251-52; 56). In *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002), the court overturned two sections of the Child Pornography Protection Act: Section 2256(8)(B), which prohibited “any visual depiction” that “is, or appears to be, of a minor engaging in sexually explicit conduct,” and Section 2256(8)(D), which criminalized the pandering of any image that is presented or advertised as being of a sexually engaged minor. The court found that these regulations of virtual child pornography were unconstitutionally overbroad because they failed to implicate the state interests that justify banning actual pornography: obscenity and abuse of children.

Congress responded to the court’s decision in *Free Speech Coalition* with the PROTECT Act. See PROTECT Act, Pub. L. 108-21, 117 Stat. 650 (2003)

(codified at 18 U.S.C.A. §2251). The PROTECT Act regulates virtual child pornography by prohibiting pornographic materials that are “indistinguishable from” child pornography, and by offering defendants the affirmative defense that the pornography was produced without using an actual minor.

Federal and state laws applicable to Internet pornography cases include:

18 U.S.C. §2252

Regarding certain activities relating to material involving the sexual exploitation of minors (distribution, receipt, and possession of child pornography), this law provides that:

(a) Any person who—

(1) knowingly transports or ships in interstate or foreign commerce by any means, including by computer or mails, any visual depiction, if—

(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and

(B) such visual depiction is of such conduct;

(2) knowingly receives or distributes any visual depiction that has been mailed, or has been shipped or transported in interstate or foreign commerce, or which contains materials which have been mailed or so shipped or transported, by any means including by computer...

18 U.S.C. §2422

Regarding the transportation for illegal sexual activity and related crimes, this law provides that:

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

18 U.S.C. §2256

This law criminalizes depictions that “appear to be” of a minor engaging in sexually explicit conduct. However, the Supreme Court has struck down that portion as unconstitutionally overbroad. *Ashcroft v. Free Speech Coalition*, 535 U.S. 234 (2002). For the purposes of this statute:

- (1) “minor” means any person under the age of eighteen years;
- (2) (A) Except as provided in Subparagraph (B), “sexually explicit conduct” means actual or simulated—
 - (i) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex;
 - (ii) bestiality;
 - (iii) masturbation;
 - (iv) sadistic or masochistic abuse; or
 - (v) lascivious exhibition of the genitals or pubic area of any person;
- (B) For purposes of Subsection 8(B) of this section, “sexually explicit conduct” means—

- (i) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited;
- (ii) graphic or lascivious simulated;
 - (I) bestiality;
 - (II) masturbation; or
 - (III) sadistic or masochistic abuse; or
- (iii) graphic or simulated lascivious exhibition of the genitals or pubic area of any person;
- (3) “producing” means producing, directing, manufacturing, issuing, publishing, or advertising;
- (4) “organization” means a person other than an individual;
- (5) “visual depiction” includes undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image;
- (6) “computer” has the meaning given that term in section 1030 of this title [18 U.S.C.S. §1030];
- (7) “custody or control” includes temporary supervision over or responsibility for a minor whether legally or illegally obtained;
- (8) “child pornography” means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture,

whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where—

(A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

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

(C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

(9) “identifiable minor”—

(A) means a person—

(i)

(I) who was a minor at the time the visual depiction was created, adapted, or modified; or

(II) whose image as a minor was used in creating, adapting, or modifying the visual depiction; and

(ii) who is recognizable as an actual person by the person’s face, likeness, or other distinguishing characteristic, such as a unique birthmark or other recognizable feature; and

(B) shall not be construed to require proof of the actual identity of the identifiable minor.

(10) “graphic,” when used with respect to a depiction of sexually explicit conduct, means that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted; and

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

18 U.S.C.A. §2251

Regarding the sexual exploitation of children, this law seeks to punish:

(a) 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, or who transports any minor in interstate or foreign commerce, or in any territory or possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct, shall be punished as provided under Subsection (e), if such person knows or has reason to know that such visual depiction will be transported in interstate or foreign commerce or mailed, if that visual depiction was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported in interstate or foreign commerce or mailed.

(b) Any parent, legal guardian, or person having custody or control of a minor who knowingly permits such minor to engage in, or to assist any other person to engage in,

sexually explicit conduct for the purpose of producing any visual depiction of such conduct shall be punished as provided under Subsection (e) of this section, if such parent, legal guardian, or person knows or has reason to know that such visual depiction will be transported in interstate or foreign commerce or mailed, if that visual depiction was produced using materials that have been mailed, shipped, or transported in interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported in interstate or foreign commerce or mailed.

Challenges and Preparing for Defense

In an Internet obscenity prosecution, the focus is on community standards, the wide availability of obscenity/pornographic materials on local cable, and even in accepted current literature, graphic novels, and video games. The greatest challenges lie in the defense of Internet child pornography and child exploitation cases. Very few people in the United States take exception with the child pornography laws currently in place, even if they may infringe on the First Amendment protections of free speech. Therefore, one of the most difficult challenges an attorney representing a defendant charged with a violation of child pornography laws will face is the hostility they will inevitably encounter from the prosecution, the judge, and the jury.

Another challenge in defending against Internet crimes is the fact that our courts have held that neither 18 U.S.C. §2252 (West 2008) nor 18 U.S.C. §2422(b) (West 2008) are overbroad in light of Internet-specific principles laid down by the U.S. Supreme Court, since they cover situations in which “nothing but unprotected speech was either threatened or chilled.” *U.S. v. Dvinellis*, 508 F. 3d 63 (1st Cir. 2007). Therefore it is important to discuss with the defendant where the communication took place (i.e., adult versus child Internet chat room), what the conversation entailed (i.e., protected versus unprotected speech), and whether any reasonable steps were taken to either exchange photography, video, or other materials, or meet in person.

Furthermore, under 18 U.S.C. §2422(b), an “actual minor victim is not required for attempt conviction.” *U.S. v. Meek*, 366 F. 3d 705 (9th Cir. 2004). Therefore, if an agent from the Federal Bureau of Investigation impersonates a minor and the defendant has had telephone conversations and Internet communications with the agent, it is important to establish whether the defendant believed the agent to be a minor and, if a substantial step was taken toward the commission of a crime (i.e., arriving at a meeting place), whether the defendant went to the meeting place under the belief that the meeting would be with a minor.

While the prosecution does not need to prove that the defendant intended to perform actual acts with the minor, it does have to prove that the defendant had intent to persuade or attempt to persuade minors to engage in illegal sexual activity. *U.S. v. Bailey*, 228 F. 3d 637 (6th Cir. 2000). Therefore it is important to analyze the conversations between the minor and the defendant under 18 U.S.C. §2422 to establish exactly what was said and implicated, since if the intent to persuade was not there, the defendant is innocent.

For example, once the defendant moved from simply sending e-mail messages referring to sexual matters, to asking young women to meet him in sexual activities, a substantial step toward persuading and inducing women to engage in illegal sexual conduct was taken under 18 U.S.C. §2422(b). *U.S. v. Gravenhorst*, 2006 U.S. App. LEXIS 32373 (1st Cir. 2006), cert. den. 127 S. Ct. 997 (2007).

Also, “direct communication with minor or supposed minor is unnecessary under text of 18 U.S.C. §2422(b).” *U.S. v. Murrell*, 368 F.3d 1283 (11th Cir. 2004). In other words, so long as the defendant has taken a substantial step toward engaging in illegal sexual conduct with a minor (i.e., contracting with minor’s father), the requisite element of intent is present. It is therefore crucial to establish what communications took place, with whom, and for what purpose.

In cases when it is advantageous (e.g., where there are allegations of sexual assault), defense attorneys should obtain a credible polygraph examination from a respected professional. Willingness to take a polygraph examination,

even if limited to specific questions or allegations in the charge, may carry great weight with the jury.

It is also important to determine which state has jurisdiction, since activities that are illegal in some states may not be criminal in others. For example, since the defendant said he would come to North Dakota to meet a girl he believed to be sixteen years old (actually an undercover officer), since she claimed she did not have a vehicle, the jury could have reasonably inferred that the defendant intended to persuade the girl to engage in sexual activity in North Dakota, where the sexual contact would have been criminal, and not in Minnesota, where the defendant actually lived and wherefrom he communicated with the “girl” via the Internet, where the contact may not have been criminal. *U.S. v. Patten*, 397 F.3d 1100 (8th Cir. 2005). Transcripts of Internet chats and telephone conversations were sufficient evidence to permit a reasonable jury to find that a defendant intended to persuade a “sixteen-year-old girl” (who was actually an undercover officer) to engage in sexual activity. *Id.*

Defense of Internet pornography does not typically have strong focus on documents. Some documents can be important, such as records showing electronic messaging, Internet file sharing, or participation in a chat room. The defense of Internet pornography is more forensically focused. Access to the computer where the images were found is critical and is one of the most important inquiries with a client. Also important is an inquiry about the images themselves. How many, how frequently there were downloads, where they were stored, how violent they were (can affect sentencing guidelines), and whether the client participated in trading images with others.

Independent examination of an accused computer hard drive is absolutely required. Without an independent examination, there can be no determination if pornographic images were downloaded through spyware or other unknown viruses. In an Internet obscenity or pornography case, a simple request under case Rule 16 of the Federal Rules of Criminal Procedure should suffice. This rule directs the government to provide counsel with copies of documentary evidence.

However, Rule 16 is superseded by 18 U.S.C. §3509(m) (West 2008) in child pornography cases. 18 U.S.C. §3509 (m) precludes the making of any copy or reproduction of the image. Moreover, defense counsel is allowed only to review and/or examine the images at the location of the government's choosing. This restriction is an issue when the defense chooses to have a forensic examination performed on the computer and contents.

With the enactment of this restriction, the government only allowed forensic defense experts to examine the computer in the presence of a government agent. Defense lawyers successfully challenged this supervision as a violation of the attorney work product doctrine. Accepted procedures include the Federal Bureau of Investigation sending a mirror image of the seized computer to a police lab near an out-of-state expert. *U.S. v. Sturm*, No. 06-CR-00342-LTB, 2007 WL 1453108 (D. Colo. May, 17, 2007). Another method is to request that the government provide a room with two computers. A copy of the original drive is made and provided to the defense expert. The defense expert is allowed to take the copy to the workroom and perform analysis. The drive is locked in a safe to which defense counsel may have access. The defense expert creates reports or spreadsheets based on analysis, and takes that information from the room.

With the arrival of federal agents at their door to seize computers, disks, videos, and so on, the client is both stunned and humiliated. These feelings invariably lead many targets to give a full confession. As a result, defense lawyers should spend considerable time interviewing the client surrounding the circumstances of the interview. How many agents were present? Were they wearing SWAT gear? Were weapons drawn? What was the time of day or night? Were they allowed access to an attorney? Answers to these questions may provide the basis for suppression of the client's statement.

The law enforcement investigation is the single most important part of devising a defense strategy. If there was a search warrant, reviewing for probable cause and any errors is a front-line defense. A defense forensic expert will be examining the client's computer in large part to determine what the investigator missed. It is not uncommon for an investigator to have looked only at the computer activity on the dates that were charged in the indictment. A defense investigation should be more comprehensive, and

would include a search for viruses and history of downloads by others when the client was not using the computer.

Every client must draft a chronology of events surrounding the use and access of the computer, the use of all e-mail accounts, their knowledge of the computer, and circumstances surrounding the execution of any search warrant and/or statement they may have given to investigators. If feasible, the images and/or hard drive should be independently examined. The Internet history, temporary files, and so on should all be forensically examined.

The Steps Usually Followed in Handling Defense

First Step

Evaluate applicable statutes and charging information to see if all the necessary elements are met. If they are not, try to get the charge thrown out. Also, make a thorough review of the charging document, search warrants, and so on to see if the search of the defendant's property was valid.

Second Step

If the charging information is sufficient, try to establish if your client may have affirmative defenses. If so, assert an affirmative defense. A few examples include:

Affirmative Defenses

18 U.S.C. §2252(c) (2008) states that it shall be an affirmative defense to a charge of violating the statute under paragraph (4) of Subsection (a) (knowingly possessing one or more books, magazines, periodicals, films, videotapes, or other matters that contain any visual depiction) that the defendant—

- (1) possessed less than three matters containing any visual depiction proscribed by that paragraph; and

(2) promptly and in good faith, and without retaining or allowing any person, other than a law enforcement agency, to access any visual depiction or copy thereof—

(A) took reasonable steps to destroy each visual depiction; or

(B) reported the matter to a law enforcement agency and afforded that agency access to each such visual depiction.

Jurisdiction

If there is not a sufficient nexus with interstate commerce, the defendant may not be prosecuted under 18 U.S.C. §2252, such as in a case where the defendant took consensual photographs of a nude seventeen-year-old, only months from reaching majority, for his private viewing. *U.S. v. Corp*, 236 F.3d 325 (6th Cir. 2001).

Third Step

Also, review the statute under which the defendant is charged. If the statute seems vague, overbroad, or otherwise constitutionally impermissible, bring this to the court's attention as soon as possible and try to avoid the arrest and prosecution. Most of the statutes relating to child Internet pornography are new and still being amended. Therefore, some arguments in this vein have been successful.

Fourth Step

Examine all the evidence the prosecution intends to present at trial, and try to exclude it through motions *in limine* and pre-trial suppression hearings. Some examples of cases where prejudicial evidence was excluded include:

Relevancy

In prosecution of a defendant for receiving child pornographic videos through mail, presentation of evidence concerning contents of some adult

x-rated videotapes seized from the defendant's residence was unnecessary, irrelevant to trial issues, and so prejudicial that it denied him his right to a fair trial. *U.S. v. Harvey*, 991 F.2d 981 (2nd Cir. 1993).

Illegal Search

Where a postal inspector presented application and affidavit for an anticipatory search warrant seeking a search of a defendant's residence based upon the defendant's ordering of videotape depicting illegal child pornography and where affidavit, but not warrant, stated triggering conditions to make the warrant valid, warrant was inoperative and search was illegal because the affidavit was not presented to the defendant along with warrant when the search was conducted. *U.S. v. Grubbs*, 377 F.3d 1072 (9th Cir. 2004); *see also U.S. v. Gourde*, 382 F.3d 1003 (9th Cir. 2004). Because officers failed to present other target-specific corroborating information linking the defendant's two-month membership to a mixed child pornography/adult pornography Web site to his probable possession of child pornography, they acted objectively unreasonably in applying for and executing a warrant. Therefore they were not entitled to a good-faith exception of the exclusionary rule, and the trial court erred in refusing to suppress evidence seized from the defendant's computer. *See also United States v. Cochran*, 806 F. Supp. 560 (E.D. Pa. 1992) "good faith" exception is inapplicable to save invalid portion of a warrant and evidence seized pursuant thereto because warrant was clearly overbroad and police officers reasonably should have known they could not legitimately search for and seize all nude pictures of children without limitation (such as adult pornography and sexual aids)).

Knowledge/Intent

Defendant has to know that at least one person involved in the sexually explicit conduct was a minor. *U.S. v. Cedelle*, 89 F.3d 181 (4th Cir. 1999).

Fifth Step

Make sure the jury is aware that the government carries the burden of proof, and ensure that the jury instructions clearly reflect this standard. For example, the prosecution has to prove the requisite intent, and that the

images are of real children, not merely altered versions of something that is perfectly legal.

Defense

The Internet and the use of computers are the largest factors in the difference between defense strategies for Internet pornography and traditional pornography. Most of our computers, either on the hard drive or within the temporary Internet file folder, have downloads and files that were unintentionally saved and downloaded onto our computers without us knowing it. This is a result of search engines that simply cannot filter out all unanticipated or irrelevant results. For example, a search for songs from the Sex Pistols or a download of the movie *Freddy Got Fingered* will inevitably result in some returns containing sexually explicit materials. With most shareware software, you will not be able to view the search results until the files are downloaded onto your hard drive. Once the files are downloaded, however, even if you realize the file is not what you were looking for and quickly delete it, it may be permanently etched into your computer's hard drive and will not be erased unless it is professionally "cleaned." Such downloads, however, do not support the required intent to possess child pornography.

Therefore, a defense attorney in an Internet pornography case, versus a traditional pornography charge, will need to be well versed on the intricacies of the Internet, to explain to the jury how temporary files may be transferred to the computer without the owner realizing it is occurring, and focus on the fact that the accused simply did not have the requisite intent under the statutes.

The defense strategy in these types of cases is to first closely examine the jurisdictional elements and the investigation, and to file pre-trial motions accordingly so a strong appellate record is made and preserved. Critical to this record is framing jurisdictional and pre-trial motions as constitutional violations, rather than violations of mere statutes or rules.

Components and Outcomes of Recent Defenses

Jurisdictional Element

In 18 U.S.C. §2252(a)(4)(B), jurisdictional element provided no support for the United States' assertion of federal jurisdiction over a mother who possessed pornographic photo of her daughter, where jurisdictional hook was the mother's use of camera and film made somewhere outside of California. 18 U.S.C. §2252(a)(4)(B) was found to be unconstitutional under U.S. Const. art. I, §8, cl. 3, as applied to the mother's simple intrastate possession of a pornographic photo of her daughter where the picture had not been mailed, shipped, or transported intrastate and was not intended for interstate distribution. *U.S. v. McCoy*, 323 F.3d 1114 (9th Cir. 2003).

Right to Privacy

A defendant's motion to dismiss indictment for possession of photographs of a fourteen-year-old female engaged in sexually explicit conduct in violation of the Child Protection Act, 18 U.S.C. §2252(a)(4)(B), and production of photographs depicting minor female engaged in sexually explicit conduct in violation of 18 U.S.C. §2251(a), was denied because (1) the fact that under Puerto Rico law the defendant could have had a relationship with the girl without committing criminal conduct did not preclude his prosecution under federal law for production and possession of sexually explicit photographs, and (2) his relationship with the girl was not sheltered by the right to privacy afforded to married couples, since his relationship was not legally sanctioned marriage. *U.S. v. Ortiz-Graulau*, 397 F. Supp. 2d 345 (DC Puerto Rico 2005).

Commerce Clause

In a child pornography case, 18 U.S.C. §2252(a)(4)(B) contains express requirement that visual depictions have been mailed, shipped, or transported in interstate or foreign commerce, or were produced using materials that have been mailed or so shipped or transported, by any means including by computer, statute does not permit jurisdiction based upon inference from inference. Instead, actual showing of interstate transportation is the element of proof imposed upon the government. Thus

Congress, in enacting §2252(a)(4)(B), regulated only materials actually in interstate commerce pursuant to the Commerce Clause, U.S. Const. art. I, §8, cl. 3; *U.S. v. Halter*, 402 F.Supp. 2d 856 (S.D. Ohio 2005).

Intended Scope

A court invoked the rule of lenity because reasonable doubt existed about intended scope or unit of prosecution to be asserted under 18 U.S.C. §2252, so that charges against defendants that provided access to child pornography Web sites should have been assessed based upon the number of impermissible Web sites that were accessible, and not based upon the number of impermissible images that could be downloaded from each Web site. *U.S. v. Reedy*, 304 F.3d 358 (5th Cir. 2002).

Knowledge

Not only must receipt be knowing under 18 U.S.C. §2252, but the defendant must have knowledge of sexual explicitness of contents and minor age of persons depicted. *U.S. v. Gendron*, 18 F. 3d 955 (1st Cir. 1994); *see also United States v. Myers*, 355 F.3d 1040, 1044 (7th Cir. 2004) (not knowing that material depicts minors is an affirmative defense); *U.S. v. Kleiner*, 663 F. Supp. 43 (S.D. Fla. 1987) (comparing to knowledge requirement of White Slave Traffic Act); *Breitfeller v. Playboy Entm't Group Inc.*, No. 8:05CV405T30TGW, 2005 WL 2088418 (M.D. Fla. Aug. 30, 2005) (RICO claims for distribution were dismissed because defendants did not know plaintiffs were minors at the time of wet T-shirt contest).

Double Jeopardy

Charges against defendants under 18 U.S.C. §2252A for operating credit card verification service that provided customers access to Web sites containing child pornography were duplicative of charges brought against defendants for the same activity under 18 U.S.C. §2252, and the matter was remanded to district court for re-sentencing without consideration of charges under 18 U.S.C. §2252A. *U.S. v. Reedy*, 304 F.3d 358 (5th Cir. 2002); *see also U.S. v. Buchanan*, 485 F. 3d 274 (5th Cir. 2007) (government could not show that defendant took more than one action to receive four images

of child pornography, and therefore four convictions under 18 U.S.C. §2252(a)(2) violated double jeopardy).

Selective Prosecution

A defendant's motion to dismiss indictment for receiving child pornography through mail in violation of 18 U.S.C. §2252 is denied, where it is unclear whether or to what extent an individual's possession of child pornography in their home is protected by the First and Fourth Amendments, because the defendant could not prove that his prosecution amounted to impermissible "selective prosecution," since other child pornography materials were found in his home in addition to those received through the Postal Service sting operation. *U.S. v. Boffardi*, 684 F. Supp. 1263 (S.D. N.Y. 1988), *aff'd* without op. (2nd Cir. 1989), 872 F.2d 1022.

First Amendment

A reporter's prosecution in violation of 18 U.S.C. §2252 may proceed, where the court does not believe the only way the reporter can confirm that child pornography is available on the Internet is to obtain and distribute images himself, because the reporter has no viable First Amendment defense under either the free speech clause or the free press clause. *U.S. v. Matthews*, 11 F. Supp. 2d 656 (DC 1998), *aff'd* 209 F.3d 338 (4th Cir. 2000).

Entrapment

The government failed to establish that a fifty-six-year-old farmer was predisposed to purchase child pornography prior and independent to the government's investigation of him, where (1) his purchase of two magazines found in his home was at that time legal, and he did not know until they arrived that they depicted minors; (2)(a) his responses to government "mailings" over a twenty-six-month period were "at most indicative of certain personal inclinations," that (b) there was strong inference that by waving a "banner of individual rights," the government may have actually encouraged the defendant to purchase such materials as part of a fight against censorship; (3) Congress did not intend for the government to lure otherwise innocent persons into violation of 18 U.S.C. §2252. *Jacobson v. U.S.*, 503 U.S. 540 (1992).

Fake Images

Based on evidence presented about the advanced state of technology, a question arose about whether the images in the instant case were real or fake, and neither the expert witness nor the lay jury could have determined whether the images in the case were real or virtual, to the level of certainty required in criminal prosecution under 18 U.S.C. §2252(a)(4)(B), based on only visual means. *U.S. v. Fabrizio*, 445 F. Supp. 2d 152 (D.C. Mass. 2006), *subsequent app. remanded*, 459 F. 3d 80 (1st Cir. 2006).

Insufficient Evidence

Conviction for transportation of child pornography across state lines was improper under 18 U.S.C. §2254(a)(1) (2008), where the jury did not view the pictures at issue since the jury must see the photographs to consider many details that determine whether they depict lascivious exhibition. Mere testimony describing the photographs is insufficient. *U.S. v. Villard*, 700 F. Supp. 803 (D.C. N.J. 1988), *aff'd* 885 F. 2d 117 (3rd Cir. 1989).

Probable Cause

A conclusory statement that a computer contains “images and...that all” appeared to be within the statutory definition of child pornography, specifically, “photographs of a pre-pubescent boy lasciviously displaying his genitals” fails to establish probable cause, even with proof that the government can link the images to the particular computer, because “the identification of images that are lascivious will almost always involve, to some degree, a subjective and conclusory determination on the part of the viewer. That inherent subjectivity is precisely why the determination should be made by a judge, not an agent. The Fourth Amendment requires no less.” *U.S. v. Brunette*, 256 F. 3d 14, 18 (1st Cir. 2001).

Staleness

A thirteen-month delay in viewing downloaded child pornography and no evidence of ongoing criminal activity sufficed in the court’s ruling that “a line must be drawn in Internet child pornography cases. I find that the line is one year absent evidence of ongoing criminal activity.” *U.S. v. Greathouse*,

297 F. Supp. 2d 1264, 1272-73 (D. Or. 2003); *see also U.S. v. Zimmerman*, 277 F. 3d 426, 433-34 (3rd Cir. 2002) (the viewing of a pornographic video file on the computer six months before the search warrant was too stale, absent any evidence that the defendant had actually downloaded the video clip and absent proof of continuous criminal activity).

Jury Instructions

A defendant's convictions on four charges had to be vacated because the jury returned a general verdict and the trial court's jury instructions given pursuant to the Child Pornography Prevention Act of 1996, 18 U.S.C.S. §§2251 et seq., which defined "child pornography" pursuant to act, contained both constitutional and unconstitutional definitions of "child pornography," and thus it was possible that the defendant's four convictions rested on unconstitutional definition of "child pornography." *U.S. v. Pearl*, 324 F.3d 1210 (10th Cir. 2003), *cert. den.* 539 US 934 (2003).

Inducement

Activities of a commercial photo processor in allegedly processing obscene photographs and mailing photographs back to customers cannot subject the processor to criminal liability under 18 U.S.C.S. §2251 in absence of indication that the processor's conduct aided customers in procuring participation of children, notwithstanding that some of the processor's customers may have been repeat customers and despite contention that film processing is an integral part of production of child pornography indistinguishable from that of the person inducing the minor to be photographed. *U.S. v. Petrov*, 747 F. 2d 824 (2nd Cir. 1984), *cert. den.* 471 US 1025 (1985).

Mistake of Age

Although 18 U.S.C.S. §2251 on its face does not permit reasonable mistake of age of minor depicted to be an affirmative defense, the statute must be construed to incorporate defense in order to save it from collision with the First Amendment. The defendant may avoid conviction only by showing by clear and convincing evidence that he did not know, and could not

reasonably have learned, that the actor was under eighteen. *U.S. v. U.S. Dist. Court of Cent. Dist.*, 858 F.2d 534 (9th Cir. 1988).

Defense lawyers are able to use the Constitution as part of their defense strategy, with careful application of the First, Fourth, and Fifth Amendments. Procedurally, these issues must be raised prior to trial, but not before a defense investigation has been completed. Federally, you cannot conduct depositions in criminal cases, but in some states, such as Indiana, you can. For example, some clients are charged with just merely receiving a few images as e-mail attachments. Accidental receipt may be a defense. In this case, a statement from the client to police becomes the evidence that refutes accidental receipt. In this situation, careful questioning concerning the circumstances in which the statement was obtained from the client is critical for a Fourth Amendment attack. Frequently the clients are interviewed when the search warrant for the computer is being executed. So the notion of coercion and painting the atmosphere as custodial is the keystone for the constitutional attack. How many police were there? Were they wearing flak jackets? Were you allowed to move around your house? Were you kept outside the house? Were you allowed to contact your lawyer? Did the officer or agent talk to you prior to seeking the formal statement? What about and for what period of time?

Federal constitutional arguments can be raised in state court prosecutions. However, some lawyers overlook the protections of their state constitutions. In Indiana, for example, the state constitutional search and seizure provision is verbatim of the federal Fourth Amendment. However, the state supreme court has found that the Indiana provision provides greater protections than the federal counterpart. *Campos v. State*, 885 N.E.2d 590 (2008).

Other Examples

Application of 18 U.S.C. §2252 to a person who knowingly receives child pornography for personal use does not violate the First Amendment, since the right to possess obscene material in the privacy of the home does not create a correlative right to receive, transport, or distribute it. *U.S. v. Marchant*, 803 F.2d 174 (5th Cir. 1986); *see also Andersson v. U.S.*, 479 U.S. 1069 (1987).

18 U.S.C. §2252 is unconstitutional on its face, since it does not require as an element knowledge of the minority of at least one of the performers who engage in or portray specified conduct, as required by the First Amendment. *U.S. v. X-Citement Video*, 982 F.2d 1285 (9th Cir. 1992).

Because the government did not offer proof that the defendant took more than one action to receive four images of child pornography, his four convictions under 18 U.S.C. §2252(a)(2) were in violation of double jeopardy under the Fifth Amendment. *U.S. v. Buchanan*, 485 F. 3d 274 (5th Cir. 2007).

Building a Strong Defense

Negotiations can be an integral part of the defense strategy. Negotiations depend on the strength of the underlying investigation. Was the investigation weak, such that a lesser charge could be considered? Since most child pornography cases tend to be federal, a focus on the applicable sentencing guidelines is critical to the success of any negotiations. If the client did make a full confession and there are no evidentiary weaknesses, counsel should consider having the client evaluated on issues of dangerousness, pedophilia, and so on.

If the client is in a posture of wanting a negotiated outcome, counsel should recommend some type of counseling to show acceptance of responsibility at sentencing. This option should only be utilized if there is no chance of a trial on the merits, because some counselors may believe they have a responsibility to make a report of child abuse, as absurd as this seems in the case of possession of pornographic images, to Child Protection Services. Other areas of negotiation include the number of images the prosecutor will require the client to admit to possessing or producing, and the relevant conduct that will be included in any plea agreement. One technique is to negotiate a written factual basis that will act as the sole recitation of the relevant facts.

Plea negotiations depend upon the circumstances surrounding your client's case. Was there a full confession you have been unable to suppress? If so, negotiations can show the ability for rehabilitation and effort the client has made in accepting responsibility prior to indictment. Another approach can

revolve around the number of images and type of images the government may be demanding the client admit to. The positive aspects of your client can influence these negotiations, so fully understanding him or her is an asset.

One of the most common mistakes made by defendants is that they make statements before consulting an attorney. Typically, this is done in a misguided attempt to help law enforcement. However, these statements may be twisted and used against the defendant in a court of law. Therefore, the best defense begins before a client is ever charged, and no interview should ever be conducted without an attorney present.

Also, defense attorneys do not take enough advantage of the telltale evidence present in an electronic file, such as where it came from, the date it was downloaded, and so on. Using this evidence, or pointing to law enforcement's lack of investigation and acquisition of potentially exculpatory information, is one of the easiest ways to prove actual innocence. The file may have been hidden (Trojan horse) or attached to a perfectly legal file downloaded from the Food Network Web site by your client's grandmother, in preparation for Thanksgiving dinner.

Another pitfall is that an attorney may not sufficiently prepare for the cross-examination of the prosecution's expert. It is important to be able to counter the reports of computer professionals, caseworkers, and "experts" who examine pornographic evidence. Therefore, it is crucial for the attorney to educate himself or herself on the expert's education, work history, published works, and most importantly, testimony in prior cases. If you can anticipate it, the expert's published works or testimony may be easily contradicted by your own experts or the presentation of contradictory expert opinions.

An understandable mistake made by some attorneys, since the U.S. Supreme Court invalidated all laws that prohibit private possession of obscene material, *Stanley v. Georgia*, 394 U.S. 557 (1969), is the attempt to employ traditional First Amendment defenses to a child pornography prosecution. This defense strategy is almost always ineffective, since in *Osborne v. Ohio*, 495 U.S. 103 (1990), the court held that the Miller tripartite obscenity standard does not apply where a child pornography violation is concerned.

A verdict can be appealed after the defendant is sentenced. In the federal courts, a notice of appeal must be filed no later than ten days after the entry of the judgment and conviction. In federal courts, a defendant may plead guilty and still preserve the right to appeal a pre-trial ruling like denial of suppression. Even in the context of a guilty plea, the sentence imposed is frequently appealable. The filing deadline for appealing after a plea of guilty is the same as if one had been convicted after a trial. The procedures for appealing verdicts or sentences in state court are determined by each state's legislature. In Indiana, for example, the notice of appeal is subject to a thirty-day deadline. Moreover, a defendant cannot preserve an issue for appeal in plea agreement.

Every person convicted of a crime is entitled to appeal. An attorney is not under the same ethical obligations to determine whether an appeal of a conviction or sentence is frivolous in the way that an attorney representing a civil litigant is required to do.

The best trial record for appeal is a record that contains as many constitutional arguments as possible. Constitutionalizing objections to evidence, as well as to the statute itself, is typically the best option for argument. In recent years, the Supreme Court has remained vigilant in finding that an accused's constitutional rights to counsel and to meaningfully confront evidence and witnesses against them prevail over any conflicting rule of evidence. *Crawford v. Washington*, 541 U.S. 36 (2004).

Also remember that merely because the verdict has been rendered, the litigation may not be complete, particularly relating to sex offender registry requirements. For instance, depending on the offense, clients may be labeled as sexually dangerous persons, which could lead to a civil commitment. *See* 18 U.S.C. §4248 (2008).

State and federal legislators appear to continue the tradition of drafting crimes *du jour* for publicity and “tough on crime” campaign tag lines. This is especially true regarding Internet crimes and pornography. Defense lawyers can best be prepared to fight these never-ending new crimes by staying current with the technology, terminology, and changing structure of the Internet.

A graduate of Indiana University School of Law at Bloomington and Saint Mary's College at Notre Dame, Kathleen M. Sweeney has been practicing law in Indianapolis for more than twenty years. She has served as an assistant U.S. attorney, local sex crimes prosecutor, chief counsel to the county department of children services, and training director for the county public defender agency. Currently she concentrates her practice in criminal defense and employment law. She is both a trial and appellate lawyer, and she most enjoys litigating cases with constitutional issues.



ASPATORE

www.Aspatore.com

Aspatore Books is the largest and most exclusive publisher of C-Level executives (CEO, CFO, CTO, CMO, Partner) from the world's most respected companies and law firms. Aspatore annually publishes a select group of C-Level executives from the Global 1,000, top 250 law firms (Partners & Chairs), and other leading companies of all sizes. C-Level Business Intelligence™, as conceptualized and developed by Aspatore Books, provides professionals of all levels with proven business intelligence from industry insiders – direct and unfiltered insight from those who know it best – as opposed to third-party accounts offered by unknown authors and analysts. Aspatore Books is committed to publishing an innovative line of business and legal books, those which lay forth principles and offer insights that when employed, can have a direct financial impact on the reader's business objectives, whatever they may be. In essence, Aspatore publishes critical tools – need-to-read as opposed to nice-to-read books – for all business professionals.

Inside the Minds

The critically acclaimed *Inside the Minds* series provides readers of all levels with proven business intelligence from C-Level executives (CEO, CFO, CTO, CMO, Partner) from the world's most respected companies. Each chapter is comparable to a white paper or essay and is a future-oriented look at where an industry/profession/topic is heading and the most important issues for future success. Each author has been selected based upon their experience and C-level standing within the professional community. *Inside the Minds* was conceived in order to give readers actual insights into the leading minds of business executives worldwide. Because so few books or other publications are actually written by executives in industry, *Inside the Minds* presents an unprecedented look at various industries and professions never before available.



ASPATORE