

Defending Child Pornography Cases

Challenges & Issues

In this Chapter I invite the practitioner to consider the various challenges and issues confronting the typical child pornography case. It is not a step-by-step guide on how to defend child pornography cases, nor is it a scholarly work intended for the law library; such works are far beyond the scope of this humble Chapter. Rather, I present below the thoughts and strategies I have employed in the cases that I've encountered, with the hope that some useful ideas will emerge and find their way toward the delivery of justice in your cases.

Among the many unique challenges facing lawyers defending Internet pornography cases, is the dramatically amorphous nature of "possession" on a computer. Laws criminalizing classic pornography (e.g., magazines, photos) target physical possession of tangible, self-evident objects, an easy concept to understand. But what does it mean to "possess" a stream of binary digits that lie latent and innocuous somewhere on a computer's hard disk until they are interpreted and rendered by software located elsewhere on the computer? Of what significance is the ability to render these bits differently depending on the software used to access them? Suppose an image file viewed in Adobe Photoshop depicts an obscene image, but the same image file viewed via software that employs parental "filters" renders a non-obscene image? Do the bits on their own have any independent status, given that they are meaningless without interpretation by some rendering software? Can the rendering software make them obscene or non obscene?

And how do these scenarios change when the computer is connected via the Internet to millions of other computers? What if other users on the Internet are granted access to a computer and thereby obtain the ability to exercise dominion and control over allegedly obscene bits that reside on that computer? Is everyone with access to the Internet suddenly in "possession"? Does it matter that some users won't have the software necessary to render the obscene images? What exposure is there for users who don't even know about the opportunity? And what about users who know they have access to these bits and know they have dominion and control over these bits, but choose not to render them? Are they in "possession"? Does it matter that they never asked for access? Complicated questions.

And while we're on the topic of complicated questions, how does one define "knowing possession" in the context of computer data? Classic principles of good user interface design dictate that users should be shielded from having too much knowledge of what's going on under the hood, and software is often designed to hide intermediate operations while producing desired end results. Working files are created, saved, moved, and deleted without any visibility to the end user. And because we all want our computers to be faster, software developers often create additional by-products in an effort to enhance performance. Some of these unseen by-products may be responsible for file activities that are completely invisible (and potentially unknown) to a user. Statutes that require

“knowing possession” of computer files are difficult to enforce in an environment where files are being created, moved, and stored without a user’s actual knowledge or explicit command.

Another challenge unique to Internet pornography cases is the struggle to define “obscenity” in the context of a global community. Classic pornography legislation targets materials deemed “obscene”. Obscenity, in turn, is defined in terms of local community standards. This makes some sense when the issue is whether a product in local circulation (e.g., a movie) offends the sensibilities of those within the sphere of circulation. But how do you apply “local” community standards to restrict content that necessarily exists in every community across the globe? What standards do you apply to Internet data? National standards? World standards? Applying “local community standards” to restrict content on the Internet effectively grants every local community veto power over the First Amendment rights of everyone else in every other community.

All of these challenges combine to make the prosecution of standard Internet pornography problematic and subject to attack on constitutional grounds. In truth, I rarely see prosecutions for Internet pornography of the classic, adult variety. What I *do* see every day at both the state and federal level, is the vigorous and relentless prosecution of child pornography cases. When it comes to the prosecution of Internet pornography, child pornography is where the action is.

Child pornography is easy to despise and easy to prosecute. It’s hard to imagine anything more reprehensible than crimes against children, and most of us will agree that the exploitation of children for sexual gratification deserves harsh punishment. And herein lies one of the greatest challenges facing defense counsel in a child pornography case: the emotional response.

Child sexual abuse is astonishingly common. Whenever I am in trial on any kind of child-sex case, I routinely ask jurors how many of them have been exposed to child sexual abuse in their lives, either directly or through someone they know. The number of raised hands at this point is simply astonishing. Everyone, it seems, has had some contact with child sexual abuse. And most are perfectly willing to tell you how they feel about it. Every reference at trial to child pornography is likely to conjure up painful memories for some, if not most, jurors. It’s not uncommon to see jurors silently crying during testimony.

How you traverse the emotional minefields that these cases bring with them will depend on the type of case you’re defending. If you’re lucky enough to have a client who is able to deny any involvement with the alleged child pornography, you can join the jurors in taking the moral high ground against this offensive material and focus on the facts that distance your client from the material. If, on the other hand, you’re defending a distribution or manufacturing case where the evidence of possession is undeniable, then you must confront the reality that jurors are going to be highly offended by the subject matter and you must take this into account during voir dire. Your challenge then is to

inoculate your jurors in advance so that their sensibilities are prepared for what they're going to see in court.

How do you prepare jurors for the shock ahead? You can't, completely. Prosecutors know this and they savor the moment that they put on display the very images they decry as a continuing victimization. All you really can do is attempt to isolate the revulsion of the jury from their attitudes toward your client. Obviously your client can't do this, you have to do it for him, and this is where your representation first begins to affect the outcome. You must lead the way for jurors and show them how to perform this miraculous separation. I favor the Gerry Spence technique, which he characterizes as "I'll show you mine, if you show me yours." Demonstrate to the jury how you have managed this same feat in approaching your case. When you can show jurors that you have the same revulsion, the same offended sensibilities, and that you have had to struggle with the idea of defending a case involving this material, and yet have managed to rise above your own prejudices and biases and reminded yourself that you were here to do a job and uphold our system of justice, you lead by example and provide jurors with the inspiration to do the same. Moreover, by discussing these topics candidly during voir dire, you make it possible for jurors to speak candidly about their own prejudices and biases. And you gain information and insight into individual jurors in the process, allowing you to identify the trouble spots in the panel that might not otherwise have surfaced. It's of course better to find out during voir dire if you have problem jurors on the panel, than to learn about it as the verdict is being rendered.

I've found that most jurors will accept this challenge. It's a matter of psychology. If you ignore the issue and simply hope or expect jurors will do their job, then they will do what they are naturally inclined to do. Biases and prejudices are there whether we identify them or not, and if left unidentified they remain latent and lethal. But if you challenge jurors to confront their feelings, to recognize them, and to realize that the law doesn't expect them to be free of such feelings, the law only asks them to separate these feelings from their consideration of the case, I believe that most jurors will accept this challenge and try to prove to you that they can do it. Some will get by you and retain their hidden agenda, but most are going to want to do the right thing, and the beauty of the jury trial system is that the peer pressures of a small group of well-motivated individuals can overcome that one-off that got by you. And even if they don't, the burden on the state to produce a unanimous verdict works in your favor here.

Nuts & Bolts of Forensic Computing

An important defense tactic in child pornography cases is to teach the jury how many of the end results they see on computers are the result of hidden activities going on behind the scenes as a result of the efforts of software engineers to make things easier for users. The key here is that software is often designed to make many things happen without the explicit knowledge of the end user. Some of these hidden activities facilitate actions which may appear to be criminal but in fact are not. A classic example is the web cache.

A “cache” is simply a temporary storage location on the computer’s hard drive that is used to store data that has been found as the result of a search request. The idea is that many of our searches produce identical data sets, and rather than have to go find the same data over and over again by repeating time-consuming searches, software developers store recently found data into the cache. The next time a search is requested, the search program first checks the cache to see if the data being requested is already there. If it’s there, bingo, no new search required, and the results are simply delivered to the user. If the data requested is not in the cache (i.e., it has not been recently found and placed into the cache), then the usual search routine is executed and the data retrieved from its original source. This type of efficiency results in huge time savings and is one of the reasons that Google searches are so fast, for example. The next time you do a Google search, look at the abstracts listed on the page and notice that one of the first things that appears after each abstract is a link to the “Cached” version of the data. You will notice that virtually every item returned as a result of your search request has been previously cached by Google. This is one reason their searches are so blindingly fast.

Web browsers are one of the biggest beneficiaries of caching technology. This is because any search that has to go out onto the Internet and search across cyberspace is necessarily going to be time consuming and slow, relative to a search of your computer’s hard drive. One thing you may not realize is that every time you point your browser to a web location, you are actually performing a search request. Your browser is told to go to the web page that exists at the address you type in, download whatever is there on to your computer, and then assemble and display it on your screen. What actually exists at the web site is data in the form of text, images, video, and so on. A typical web site may have hundreds, or even thousands, of images. Every little graphic image on the page is probably a separate image file that was created on some computer using graphic tools like Adobe Photoshop, and has to be downloaded to your computer so that your browser can display it on your screen. It’s a mistake to think of your computer as a window onto the web, displaying in real time layouts that are out there. It’s more accurate to think of your computer as more of a television that can be tuned into a channel and used to capture a broadcast over the air (or cable) and then reassemble the image in your living room and display it. When you go to www.cnn.com you are actually opening up a data connection to the web page that exists at www.cnn.com and instructing your computer to download every data file that exists on that page, and then assemble and display this data on your screen. Thus the very act of visiting a web site is a search request that results in the downloading of data to your computer.

The developers of web browsers realize that you will probably be going to www.cnn.com more than once and, rather than requiring you to download every single image on that page each time you visit, they actually save all the images downloaded from the site and store them on your computer. The storage area for this process is commonly referred to as the “web cache”. If you’re using Microsoft’s Internet Explorer as your web browser, this storage area is located deep within your Windows system folder and may be named something like “Temporary Internet Files”. Of course, the images appearing on a site like www.cnn.com are going to change daily and so not every file cached is going to be used, but so much of the content is the same on a day to day basis that it pays to have

everything saved into the cache just in case, so that when you next visit the site, your browser can search the cache first and use the files there to display on your screen rather than download them all over again. This is the essence of caching.

Notice what is happening here. You visit a web site and, without your express permission or even knowledge, graphic images residing on the site are being downloaded and saved on your computer. Sound dangerous? You bet it is, and you should always be prepared to challenge any assertion that images located in the web cache are “knowingly possessed”. When I get discovery in these cases, one of the first things I want to know is: where were the images located? Most law enforcement agencies use dedicated software tools like Encase by Guidance Software (<http://www.guidancesoftware.com>) or Forensic Toolkit from AccessData (<http://www.accessdata.com/>). These products are designed to retrieve and document data found on seized computers, and these software programs will often detail exactly where the images were found. Look for telltale indicators like file addresses that begin with “C:\Windows\System32 ...” and end up with something that looks like “\Temporary Internet Files”. This is an indication that the files were located in the web cache. This should be a big red flag that the files were never explicitly saved or stored by the user, but were stored without the user’s knowledge by the web browser.

Consider the following scenario: a user goes to a “marginal” web site that has ad banners for Viagra and adult pornography. The user **accidentally** clicks on a banner and unleashes a wave of unwanted pop-ups displaying all manner of pornographic content. Horrified, he shuts down Windows and goes and takes a cold shower without doing anything further on his computer. One of the sites that came up in a pop-up window displayed an image of a child engaged in an explicit sex act. Without any knowledge or intent, this user has downloaded child pornography onto his computer.

Suppose the above user is sophisticated enough to know about the web cache and he decides to delete these images by clearing his cache from the web browser’s Options menu. File deletions present additional issues. Most users aren’t aware of what happens to a file that’s been deleted. Computer files are managed by the computer’s Operating System and, although they may look to the user like logically whole units that exist in one specific location, the way the computer actually stores them on your hard disk is not at all intuitive or simple, and may involve many different pieces of data scattered all across your hard drive in distinct locations. When you tell your computer to open a file, it makes a request to the Operating System, which then goes out to all those different locations on the hard drive and pieces together the data and presents it to you as a whole. The Operating System maintains a kind of “table of contents” that knows where all these pieces are, the user is never required to know anything more than the fact that the file exists as a whole. That’s how computers are meant to work. You just want the file, you don’t care about how the Operating System manages the pieces.

When you tell your computer to “delete” a file, it doesn’t bother to go out and find all the pieces again because it knows that you’re no longer interested in all the pieces. So the first thing it does is simply remove all the pieces from the “table of contents”. Nothing is actually physically deleted at that point, and many users would be surprised to learn that

ALL of the data in the file they just deleted still exists on the hard drive at that point, and is readily available for inspection by anyone who knows how to use any of a number of widely available disk snooping tools. But your Operating System dutifully reports that the file no longer exists. Lies!

Hard drives store data in physical regions of the disk known as “sectors” and the Operating System keeps track of which sectors have been allocated to store data, and which sectors have not been allocated and are therefore available to store new data. When all of the sectors are allocated, your disk is full and cannot save any additional files. When you tell your computer to “delete” a file, in addition to removing the file pieces from the “table of contents”, the computer also informs the Operating System that the hard drive sectors previously allocated to store these individual pieces are now available for new storage. This means that some of the pieces of the deleted file could now be overwritten by new data if the Operating System were to save a new file by storing some of the new file’s pieces on sectors that had previously been allocated to the “deleted” file. In this manner, as new files are saved to the hard drive, old, “deleted” files are incrementally destroyed as the sectors holding their individual pieces are overwritten with the pieces of the newly stored files. This is one of the only ways to actually physically delete a file, by overwriting it with new file data. There are software programs that will actually go out and locate all of the pieces of a “deleted” file and overwrite them with zeroes and other meaningless data, and in this manner actually perform physical deletions of the file beyond the point of recovery. But such tools are found typically only in high security environments where physical file deletion is required along with paper “shredding”.

What this means is that the defense lawyer should be on the lookout for indications that the image files found on the client’s computer had been previously deleted, indicating an intent NOT to possess. The way this shows up is that the forensic software tools used by the government indicate that the files were found in “unallocated space”. If the government’s discovery does not reveal this fact, you should explicitly ask whether the files were found in allocated or unallocated space. If found in unallocated space, this means that the files had been deleted. An indication that files were deleted could be good or bad for your case, depending on the facts, but it’s something you should certainly know.

You’ll find that police agencies typically use either Encase or Forensic Toolkit to do their forensic evaluation of your client’s hard drives. Be sure to determine which products were used by law enforcement and request in discovery the exact version number of the product used. Depending on the issues that arise in your case, you may need to subpoena bug database records from the software vendors and it will be important to know exactly which version of the software was being used. You would be surprised to see how many bugs are known to exist and are well documented in shipping software. It is absolutely axiomatic that no software is free from bugs. The only question is: how bad are the bugs that shipped with the product and what are their consequences?

Another important technology to be aware of is the rapidly growing world of peer-to-peer computing. In computer parlance, “peer” computers are other computers in a network that are at the same level in a hierarchy. The workstations in an office are typically all “peers” of each other. Personal computers on the Internet are considered “peers” of each other. One of the great revolutions of the computing age is the idea that personal computers can work together in teams (i.e., peer-to-peer) to share large computer processing jobs that would bring any of the machines to its knees if done alone. This notion of peer-to-peer computing has revolutionized the way we approach tasks that were once thought to require huge mainframes with exorbitant processing power. A good example of this technology at work is the Seti@Home project (<http://setiathome.ssl.berkeley.edu/>). Through this effort, thousands of personal computer users have voluntarily tied their computers together to harness their combined processing power to join in the search for intelligent life elsewhere in the universe.

Perhaps the most widespread application of peer-to-peer computing is Internet based file sharing. Internet users have been swapping music and movie files since such files first became digitally available, and the battle between file sharers and copyright holders has been raging for years. Popular shareware programs like Gnutella or Kazaa make it easy for Internet users to share the files on their hard drives with other Internet users, and in turn get access to the files of others on the Internet. What’s of interest to the defense lawyer is that the software programs used for peer-to-peer file sharing are not cognizant of the content that is actually in the files being shared. Suppose Dad sees a directory on another user’s computer that lists “Snow White and the Seven Dwarves”. He decides he’d like to download this for his kids to watch and he starts the download. What he doesn’t know is that the guy who made “Snow White” available for download actually took a video called “Five Year Old Facials” and renamed it to “Snow White” before making it available. The file sharing software has no way of knowing the difference and the download proceeds. Dad and the kids are in for a surprise.

Even more dangerous is that these software programs automate so much of the process that many downloads proceed without any human intervention at all and Dad may wind up with a surprising set of files all over his computer, files which he hasn’t even yet reviewed. Law enforcement relentlessly tracks the locations where child pornography is offered. But they also track the IP addresses of the users who download these files. I have represented more than one client who got a knock on the door and found police armed with a search warrant, with no idea how they wound up the subject of an investigation for child pornography.

The defense lawyer sorting through the facts of his or her case must have all of this technological context in mind. When the client claims no knowledge of how a file got on his computer, it’s your responsibility to figure out how those images got there. This investigation cannot be completed without a thorough understanding of the technologies that can lead to the acquisition of illegal materials on a personal computer.

How do you keep up with all this technology? The most obvious choice is to employ the use of a computer forensics expert. This is of course expensive and somewhat unwieldy,

but it's the best approach because, well, experts are expert, and they will catch things that you won't, no matter how technically savvy you are.

You can try to keep up by reading the various technical publications and literature, but I find that the best supplement to your efforts is to be a user of technology. If a program like Kazaa is implicated in your case, there simply is no substitute for becoming familiar with the application and understanding how typical usage patterns can innocently contribute to compromising situations. If it's alleged that your client said something incriminating during an Instant Messaging (IM) session, it helps to be aware that your client's IM program automatically saves chat logs on his computer. This is something you might never know and might never occur to you unless you used the program and understood how it works and the features that it offers.

My advice to defense attorneys always is to know the technology. Learn how IP addresses are used to identify individual computers on the Internet, how files are saved on computers, how images can be manipulated in Photoshop. If you are not able to learn the technology, consider referring the case to an attorney who is known for his or her technical prowess. Knowledge of computer forensics is more critical in these cases than in any other kind of criminal case. With sufficient technical knowledge you can spot issues that can be directed to the attention of a hired expert. After all, the expert is only going to be directed to the issues which you've spotted, and if you're not able to identify an issue in the first place, it may never be raised or even considered by the expert.

Do not ever assume that the government is telling you the full story. Most police and prosecutors that I've dealt with know very little about technology. Consider the issue of computer file time stamps. A time stamp is supposed to tell you when the file was created. But of course that file stamp is only valid if the computer knows what time it really is. A computer that has its clock set to 1955 is going to cause every file created on it to have a 1955 time stamp. In one of my child pornography cases, time stamps on the images were in question and became a critical element in the prosecution's case. A police officer tried to establish the accuracy of the time stamps by attempting to establish that the computer's clock was correctly set. He stated in his police reports that the computer clock was correct because he found on that same computer web pages that had been saved containing time-specific data that was consistent with the time stamps. It sounded like a plausible argument until I pointed out that it was based on a flawed assumption. The police officer didn't understand the difference between static and dynamic data and, in the end, his saved files with their time-specific content were the equivalent of a picture of someone holding up a newspaper. Assuming that the picture wasn't edited in Photoshop (and that's a large assumption these days), all the picture does is prove that the picture had to be taken AFTER the date in the newspaper. But you can't prove that it was taken the day appearing on the newspaper. Similarly, the officer's saved file did nothing to prove when the file was actually saved, other than the fact that it was saved after a particular date.

In the end, the government was not able to prove the validity of the time stamps in my case and abandoned the issue altogether, throwing out the alleged illegal images in

question. The only reason we prevailed on this point was because I knew the officer was incorrect in his assumption. If you don't know the technology, you're going to miss such opportunities. The point is that you must challenge every assumption the prosecution makes. Do not assume that they know the technology because, more often than not, they won't.

How do these cases arise?

Most arrests for child pornography involve computers, even those cases involving books and movies. Of course, people don't usually carry around their computers displaying images to the public, so most prosecutions are going to arise as a result of some government agency looking through your client's computer. In many cases this will be a result of the execution of a search warrant authorizing the police to search your client's computer. Since computers are the record keeping medium of choice throughout the business world, search warrants relating to just about any crime will often include an authorization to search "computers, hard drives" and "other computer related media" as targets of the search. Under general search and seizure law principles, if police find contraband in a location where they are authorized to be, then that contraband may be seized as well. There are exceptions, but generally speaking, if police are authorized to search for image files on a computer, they will be authorized to seize child pornography files they locate on the computer. Issues to examine are whether a warrant specifically authorized a search for "image files" and if a warrant specifically contemplated that file names might be changed to disguise their content, thus authorizing individual files to be opened irrespective of their names. If a warrant provides a general authorization to search for "records of ownership, business and customers lists", that sort of thing, and a police officer then opens up a folder entitled "family photos" and finds child pornography there, there's an issue as to whether the warrant (which must describe, "with particularity the places to be searched") actually authorized a search of that location, and this should be raised via a motion to suppress.

Community groups like the National Center for Missing and Exploited Children (NCMEC) are often the originators of a child pornography prosecution. These groups maintain information for law enforcement identifying popular photographic "series" that make the rounds on the Internet. In many cases they will even identify the actual minor victims in the pornography and provide that information to prosecutors, who are then able to defeat the claim that there were no actual minor victims involved. Defense counsel should make a discovery request to find out if there have been any interactions with NCMEC on the case.

Many Internet Service Providers (ISPs) work cooperatively with NCMEC to initiate law enforcement action when child pornography is discovered on their servers or making its way through their systems. Companies like Yahoo and MSN have very well defined protocols for reporting suspected child pornography to NCMEC, who then evaluate the material and forward on to appropriate law enforcement authorities.

If, for example, NCMEC identifies an image in a Yahoo user group as belonging to a series known to have an actual minor victim, they will report this information to Yahoo and Yahoo will deliver back to them a detailed report containing information relating to the image. The amount of information relayed depends on what information NCMEC reports to them in the first place. Typically, NCMEC only knows that the image was found in a particular user “group”. Yahoo determines which of its users created the group, and will then return a long and detailed report to NCMEC that includes fields for IP address of the user uploading the image, date of the upload, contact information for the user registered as the creator of the group, contact information for the user who owns the account, and so on. This report should be demanded during discovery. Don’t assume that the prosecution has it, ask for it explicitly and remind the government of its Brady obligations; if they don’t have it, demand that they get it. Neither Yahoo nor NCMEC is going to give it to you.

One of the first tasks for the defense lawyer is to carefully examine this report. The ISP will typically provide a formatted report with enough data to make your eyes glaze over. It’s critical that you examine every item in the report and make sure that you understand exactly what each reference means. In one of my cases, a Yahoo report contained many references to an image file found in one of their user groups, and the report included a field titled “access date”. That field was interpreted by police as the date on which my client first accessed the photo and this became an issue in the case. A careful reading of the report, however, revealed that Yahoo used that field as the date that they first **archived** the photo. “Access date” was just their terminology (illogical as it seems). I would never have known that had I not read carefully the legend and the entire report.

Handling the Defense

In my experience, the typical lifespan of a prosecution for child pornography is 6-12 months from the time the accused is first confronted with the accusation. Discovery can be very time-consuming, especially if you require experts. Law enforcement forensic evaluations can take months on their own, and the delays are multiplied if you engage experts to do their own independent forensic examination. An important point: defense counsel absolutely has to get mirror image copies of the hard drives seized. Don’t rely on the government’s “offer” to allow you to come in and “inspect” the images. Insist on your right to get your own mirror image copies for your own defense purposes. This of course presents problems. The knowing possession or distribution of child pornography is a felony, so prosecutors have been known to argue that they cannot take possession of this material themselves (even less so you) and they certainly will not knowingly ship it to defense counsel.

Courts have struggled with this issue and reached a number of creative solutions. Typically, prosecutors will argue that defense experts are free to come to state facilities and “inspect” the data using their own software tools and procedures, and that this is sufficient to meet discovery obligations. Courts have allowed this type of limited access and granted substantial amounts of time for defense experts to perform their “inspections”. But most experts will tell you that they cannot adequately perform their

work outside of their rigorously controlled test environments back in their offices, and that attempts to force them to go “inspect” data at government offices is wholly insufficient.

In the end, you will have to rely on the law of your jurisdiction for guidance. Don’t look to the US Supreme Court for any help here. In Washington State, where I practice, the Washington State Supreme Court has ruled in *State v. Boyd*, 160 Wn.2d 424, 158 P.3d 54 (2007), that a defendant has a right to a mirror image copy of the hard drives seized in such cases, so that his defense expert can conduct his defense in the context of his own test environment. If you are lucky enough to have this kind of law on your side, use it to your advantage and move for the production of mirror images copies of the data. Don’t rely on offers of “inspection”.

Interviewing your client is a critical first step in any criminal case, but these cases require that you cover additional topics. How sophisticated is your client with technology? If your defense is unwitting possession, the degree to which your client understands issues like browser caching, or peer-to-peer file sharing, will be critical. Many of my clients are software engineers and they are invariably held to a higher standard of knowledge.

It’s important to find out every possible way in which your client may have come into contact with the illegal content. In one case, I represented an employee of a large Northwestern ISP after he was arrested and charged with possession of child pornography following a NCMEC tip that sent police to his house with search warrants. It turned out that he had been employed by the ISP to download child pornography and package it up for delivery to law enforcement, and he was authorized to work from home using his personal computers to handle the huge workload. This is an example of just how absurd these arrests and prosecutions can occasionally be: police arrested one of the very people they were relying upon to prosecute these cases!

Prosecutors are often unwilling to negotiate resolutions in these cases simply because they don’t have the technical knowledge to understand the arguments you are making, and they sense that you’re trying to snow them with techno mumbo jumbo. In these situations it’s best to hire a computer forensic expert with stellar credentials and have them prepare a report that makes the case in terms that a juror could understand. You’re going to need something like this for trial anyway, so you might as well get it produced early enough in the case to support your negotiating efforts.

It’s my opinion that defense lawyers don’t take enough cases to trial. This is particularly true in child pornography cases where there seems to be a consensus that once the jury sees the evidence, your client is toast. While it’s undoubtedly true that these cases present huge emotional challenges for jurors, I continue to believe that most jurors will try to do the right thing. I don’t believe that these cases should be evaluated for their trial-worthiness based on the single fact that the evidence is ugly. Every case has issues and if you’ve done your job getting the jury to understand its proper role in the process, you shouldn’t be any more afraid of the jury’s reaction to the evidence than you would of a breath test in a DUI case or autopsy photos in a homicide.

What if your client doesn't want to go to trial and wants a deal? It's also my opinion that the best way to negotiate a resolution is to prepare for trial. Prosecutors know what you're doing and what you're not doing to prepare for trial and if you're doing nothing, they know that you're probably expecting to settle. Doing a full forensic work up after discovery demands for a mirror image copy of the seized hard drives is a good way to signal loud and clear that you're not just sitting around waiting for a deal. When you consider what a prosecutor will have to go through in order to comply with discovery demands in this type of case, and the fact that he has no victim he has to check with before a deal is made, few cases offer as much nuisance value to coerce a settlement.

A final point to consider: keep in mind that sex offender registration is not considered "punishment" by most courts. Accordingly, efforts to retroactively make certain offenses registrable are usually immune to Ex Post Facto challenges. This means that an offense that your client pleads to today, may make him a registered sex offender tomorrow. Beware of sex-crazed legislatures falling all over themselves in an effort to be "tough on sex offenders"; the list of registrable offenses grows each year. Always seek a non-sex deal if possible.

Conclusions

Child pornography cases are tough and there's always so much at stake. Your clients deserve not only the full attention that you give all your most serious cases, but also the special needs of the forensic expertise that can make all the difference.

In closing, here's a suggested Checklist of things to do in your child pornography cases. These actions are, of course, in addition to all the other things that you would ordinarily do in any criminal case:

- Client interview
 - Determine in detail client's computer sophistication
 - Determine how the images could have got there

- Discovery
 - Demand a mirror image of computer hard drives seized
 - Ask about NCMEC Interactions
 - Ask for version numbers of law enforcement forensic software
 - Ask for all ISP Reports on the matter
 - Ask for ALL communications between ISP/NCMEC/Law enforcement
 - Consider asking forensic software vendor for bug database info
 - Check warrants for specificity
 - Remind prosecutor of Brady obligations to get all of the above

- Investigations
 - Hire a computer forensics expert
 - Have expert prepare a report for a LAY person's understanding

- Determine whether files were found in Web cache
 - Determine whether files were found in unallocated space
 - Challenge police assumptions (trust that they are newbies too)
 - Know the Application (Gnutella, Web browser, IM)
 - Make sure you understand every field in the ISP report
- In Voir Dire
 - Pre-Inoculate jurors to the ugliness
 - Gerry Spence's "I'll show you mine if you'll show me yours"
 - Lead by example, provide the inspiration to accept the challenge
- Negotiations and Settlement
 - Present your lay expert report to prosecutor
 - Prepare for trial to set expectations
 - Require a non-sex charge for resolution