Chapter VI

Digital Discovery for Prosecutors

by Johnette Jauron

This chapter addresses some of the digital discovery issues prosecutors face today. It is by no means an exhaustive discussion, and because both the law and technology involved are ever changing, a diligent prosecutor must stay as educated as possible with current trends in high tech crimes. This means actually using the computer technology involved or at the very least understanding how others it.

At its most basic, evidence of crime can frequently be found on computers. Unless it is properly preserved, analyzed, and disclosed, it will not be admissible at trial. While some of the issues surrounding digital evidence may be somewhat more mystifying than the traditional documentary and testimonial evidence used in criminal prosecutions, digital evidence is subject to the same basic rules of discovery. It differs, however, in the methods of acquisition, preservation, storage, analysis, and disclosure.

I. The Basic Discovery Rules: Statutory Obligations and Due Process of Law

On June 5, 1990, the Crime Victims Justice Reform Act, or Proposition 115, was enacted by the people of the State of California to effect comprehensive reforms in criminal procedure. This act, which made both constitutional and statutory amendments, among other things, narrowed the scope of discovery in criminal proceedings. Thus, Chapter 10 of title 6 of the California Penal Code was enacted to govern the discovery process in criminal proceedings.[1]

Penal Code section 1054.1 requires the prosecutor to disclose to the defendant all of the following materials and information, if in the prosecution's possession or if the prosecution knows the material and information is in the possession of the investigating agencies:

> (a) The names and addresses of persons the prosecutor intends to call as witnesses at trial.
> (b) Statements of all defendants.
> (c) All relevant real evidence seized or obtained as a part of the investigation of the offenses charged.
> (d) The existence of a felony conviction of any material witness whose credibility is likely to be critical to the outcome of the trial.
> (e) Any exculpatory evidence.
> (f) Relevant written or recorded statements of witnesses or reports of the statements of witnesses whom the prosecutor intends to call at the trial, including any reports or statements of experts made in conjunction with the case, including the results of physical or mental examinations, scientific tests, experiments, or comparisons which the prosecutor intends to offer in evidence at the trial.

Prosecutors must be familiar with the statutory rules that apply to all criminal discovery in California, keeping in mind the purpose of criminal discovery:

> (a) To promote the ascertainment of truth in trials by requiring timely pretrial discovery.
> (b) To save court time by requiring that discovery be conducted informally between and among the parties before judicial enforcement is requested.
> (c) To save court time in trial and avoid the necessity for frequent interruptions and postponements.
> (d) To protect victims and witnesses from danger, harassment, and undue delay of the proceedings.
> (e) To provide that no discovery shall occur in criminal cases except as provided by this chapter, other express statutory provisions, or as mandated by the Constitution of the United States.[2]

Prosecutors are always responsible for disclosing material exculpatory evidence to the defendant in a criminal case in accordance with the rule articulated by the United States Supreme Court in *Brady v. Maryland*.[3] This is a prosecutor's role exclusively,[4] and it is one that includes an affirmative duty to evaluate the evidence for exculpatory information.[5] Determining whether evidence is exculpatory or not involves a legal evaluation, therefore, prosecutors may not rely on investigators to satisfy this obligation.[6]

In addition, prosecutors have an ethical duty to support the constitutional requirements of due process and do the right thing to promote justice in every case. As the California Supreme Court has said in *Izazaga v. Superior Court*:

> The prosecutor's duties of disclosure under the due process clause are wholly independent of any statutory scheme of reciprocal discovery. The due process requirements are self-executing and need no statutory support to be effective. Such obligations exist whether or not the state has adopted a reciprocal discovery statute. Furthermore, if a statutory discovery scheme exists, these due process requirements operate outside such a scheme. The prosecutor is obligated to disclose such evidence voluntarily, whether or not the defendant makes a request for discovery. [¶] No statute can limit the foregoing due process rights of criminal defendants, and the new discovery chapter does not attempt to do so.[7]

Given a prosecutor's legal and ethical duty to review, evaluate, and disclose any material exculpatory evidence in his or her possession, what is a prosecutor to do with digital evidence that may contain terabytes[8] of information? What if that information has not been completely examined by investigators? Do prosecutors have a legal or ethical obligation to review all existing digital evidence for exculpatory evidence? If so, how far does that obligation extend? Does this mean that prosecutors, or more realistically forensic examiners, must review the entire contents of all digital media seized in every case for potentially exculpatory evidence?

It certainly is not reasonable to expect a prosecutor to review all digital evidence seized in a case, particularly if an investigator has not analyzed that evidence. Nor is it reasonable for criminal investigators to expend valuable resources in doing the defense's investigation. At the same time,

investigators analyzing the evidence for inculpatory information may not find or even recognize exculpatory information.

The logical solution—making a copy of all the digital evidence for the defense—is not without problems. Primarily, storage capacity for copied media must be considered. A hard drive from a personal computer purchased in 2007 can typically hold 500 gigabytes of data. Terabyte hard drives exist and personal computers can contain multiple hard drives. If all of that data is to be provided to the defense, the media upon which to put it must be provided to forensic examiners. This means the defense must supply a hard drive or other digital storage device. Copying the media takes time and resources as well, so prosecutors should plan accordingly.

Secondarily, releasing such vast amounts of personal data may put many other individuals at risk. This is particularly true when the evidence itself is contraband such as stolen personal identifying information or when it contains infected files. Images of child sexual exploitation create a tremendous burden on prosecutors to ensure that defense attorneys are allowed an opportunity to sufficiently inspect the evidence, all the while keeping the young victims from the perpetual exploitation of having those images duplicated and passed on. If there is a concern that seized but unanalyzed evidence may contain contraband, no copies should be made until the analysis is complete. That may require the defense to provide encryption keys or passwords if there are areas of data inaccessible to examiners.

Additionally, the format of the copy differs depending on how it will be used. A forensically viable image of the evidence is protected from alteration and is scientifically authenticated as a genuine duplicate, but it can only be viewed with specialized forensic software. A cloned copy, however, is a copy vulnerable to irrevocable changes in the system files, deleted files cannot be viewed without using specialized software, and the data on a cloned copy cannot be forensically verified for analysis.

II. Defining Digital Evidence

Although California has a statutory definition of "high tech crime," there is no statutory definition of "high tech evidence."[9] "Writing" is defined in Evidence Code section 250 as:

> handwriting, typewriting, printing, photostating, photographing, photocopying, transmitting by electronic mail or facsimile, and every other means of recording upon any tangible thing, any form of communication or representation, including letters, words, pictures, sounds, or symbols, or combinations thereof, and any record thereby created, regardless of the manner in which the record has been stored.

Further, a "printed representation of computer information or a computer program is presumed to be an accurate representation of the computer information or computer program that it purports to represent,"[10] as are printed representations of images stored on a video or digital medium.[11]

The few civil cases that discuss discovery of digital evidence are largely focused on spoliation and cost issues. For criminal discovery purposes, digital evidence can essentially be considered any information obtained from a computer or other electronic device that can be stored digitally on magnetic media (e.g., a floppy disk) or on photo-optical media (e.g., a CD-ROM).

All computer data, at its most fundamental, is simply binary code: ones and zeroes in a particular order representing letters and digits. Data is stored in a computer in either volatile or non-volatile memory. Volatile memory requires some power source to maintain it or else it disappears when the power is interrupted. Non-volatile memory retains data in long-term storage until it is overwritten with other data. Some data, such as video or audio files, can take up an enormous amount of storage space on the media compared to text or data files. Even text files can account for voluminous amounts of information that may not be readily distributable in printed format.

Digital evidence can include volatile data and often includes data that is not part of a visible saved file, but rather is "hidden" data created by the computer itself (e.g., erased versions of a file, portions of a partially overwritten file [slack space] as well as "metadata"). "Metadata" may identify file creation or access dates, the author of a document or an author's comments, the type of camera that took a digital picture, or other potentially valuable data. As such, digital evidence can contain an enormous amount of valuable information. It must be properly seized, properly preserved, and properly analyzed, but it can yield a wealth of information that must somehow be disclosed to the defense in a criminal case. Often, however, this means sorting through gigabytes or even terabytes of data.

Ideally, all original evidence—including data—should be kept in a law enforcement facility with the proper chain of custody preserved. Forensic examiners tasked with analyzing the digital evidence, first make an acquisition or forensic image of the media by copying it in its entirety bit by bit (as opposed to file by file) with a commercial imaging tool, which preserves both the physical and logical data and makes no changes on the original. Once that image is authenticated with forensic software, the investigator can begin an analysis of the image without compromising or even touching the original evidence. This allows for analysis of system settings, metadata, and data from unallocated and slack space.

As of July 2007, one of the most commonly used forensic software applications by law enforcement is "EnCase" by Guidance Software.[12] There are many other forensic software applications on the market including Forensic Toolkit (FTK)[13] or Ilook,[14] and some are free to law enforcement such as Prodiscover[15] or Spada.[16]

EnCase is based on law enforcement specifications and requirements. It reads all DOS, Windows, Macintosh, and Linux hard disks and removable media, and allows a forensic investigator to save an exact image of a disk to an evidence file. Every byte of the evidence file is verified using the Message Digest 5 (MD5) algorithm that was adopted by the federal government as an encryption standard many years ago. The MD5 algorithm compares two very large unique numbers to one another and verifies with certainty that the evidence file created exactly matches the files captured from the original media. In this way, the forensic examiner can ensure that the original media and the acquired copy are identical and have not been altered in any way.

Once a forensic image is authenticated it is analyzed. In the analysis, the investigator "bookmarks" items of evidentiary value to include in a report, and typically creates a narrative analysis of the relevant evidence. Most forensic analysis reports organize data in subfolders and some even put data into a graphical user interface that allows viewing and sorting evidence, as well as text-string searches.

Most forensic analysis reports can be provided to the defense in electronic format on a CD. The report can be viewed electronically by anyone with a computer, or portions of it can be printed out on paper like a traditional police report. Portions of a report such as file structures, scanned images, e-mails, or other lists can be printed out, but most reports in their entirety are too large to do so. Printing all the data, or even all the documents, found by a forensic examiner during a typical analysis is usually not an appropriate method of discovery because the data can be so voluminous. For example, all text documents on a typical 10-gigabyte hard drive printed out on standard 8.5 x 11-inch paper would yield a stack of paper some 900 feet tall. (Think the Eiffel Tower, three Statues of Liberty, or a 90-story building.)

Digital information can be so much more voluminous than traditional paper evidence that standards should be developed and maintained by each office in order to efficiently exchange information with defense counsel. If the evidence is not already in digital form, a prosecutor should consider the costs and benefits of putting it into a digital format. If it is in a digital format, a prosecutor must consider whether it will be turned over to defense counsel or to an expert hired by the defense. Counsel for the defense will likely request digital evidence in the form of a cloned copy, since the data can be viewed from most desktop computer operating systems. A forensic image file cannot be viewed without particularized software.

If requested, prosecutors should be prepared to provide the digital evidence to a defense expert. A reasonable approach to such a request for discovery is to give the defense expert the contents of an acquired drive as a forensic image and let the defense conduct its own analysis. This ensures that the evidence is not tampered with and that all exculpatory evidence is disclosed. If all the evidence has not been thoroughly analyzed by investigators, it is a good idea to draft an agreement for filing with the court that there are restrictions on the use of the evidence image. For example, by accepting the forensic image, the defense should agree not to restore or modify any actual evidence file images, not to copy any files, and agree to return the image to the forensic examiner at the conclusion of the case. Additionally, if any contraband or confidential material is found, observation should cease and it should be reported to the court immediately.

A. Practice Points for Sample Types of Digital Discovery

Any information that may be of evidentiary value in a criminal prosecution can exist in electronic format. Certainly digital evidence will be crucial in most computer intrusion, fraud, counterfeiting, or child sexual exploitation cases, but increasingly, digital evidence is turning up in traditional crimes like robberies, burglaries, and even domestic violence. The following are only samples as the complexity of digital evidence is ever expanding. Every prosecutor would do well to stay current on the technological issues relating to crime and the different types of evidence needed to prove it.

Some common examples of digital evidence in 2007 include e-mails, Internet Service Provider (ISP) logs, forensic evidence acquisitions, digital audio or video segments, file organization structure, a suspect's Internet history, and the types of programs a suspect has been using.

1. E-mail

An e-mail is most often connected to a particular suspect through an analysis of the message header. The header information is typically a detailed description of the text of a communication trail from creation and transmission through receipt. It is generated by the e-mail program and is documented at the beginning of a given message by the mail server. Headers can be forged, however, and they require an analysis by someone trained to parse e-mail headers. The text of an e-mail properly authenticated through a forensic examiner or ISP custodian of records as well as any attached documents or files, may be admissible at trial.

Spoofing, or the falsification of an e-mail account name or sender information, can be established relatively easily by a clear explanation of headers by the forensic examiner. Again, this information would only be obvious to a forensic examiner, and not readily apparent to anyone who simply reads the e-mail.

E-mails can be provided to the defense in paper printout form, which may or may not include a paper report printed by the forensic examiner. If asked to do so, an examiner's report can include a narrative explaining the header and what it means. An e-mail can also be provided in electronic form by itself or as part of a forensic report such as those done in E-mail Detective,[17] FTK, or EnCase.

2. Images, audio files, video files, and voice mail

Digital images can be compelling evidence at trial and they are often found during a forensic examination of a suspect's computer. Images can be stored in various formats and are often duplicated onto storage media. Image files can be "hidden" by placing them inside other files, among operating system files, or by assigning altered file name extensions to them, thus preventing them from being found in a traditional search for pictures. Because images can be of various resolutions and sizes, they can sometimes give a forensic examiner a good idea of what a user was doing with the image. For example, a "thumbnail" image is a reduced-size version of a picture that is often found on Web sites in order to speed download time. A Web browser takes time to resize a picture, and if a user is simply viewing various Web sites without downloading or enlarging them, the forensic examiner will only find thumbnail images in the temporary Internet files. Similarly, with pop-ups, once an image is viewed, it remains resident on the computer, thus decreasing the time it takes for the user to see the image. This is very important, for example, when determining whether someone possessed images of child sexual exploitation. If a forensic examiner finds only thumbnail images in a suspect's temporary Internet history, more evidence may be needed to prove actual possession.

Voice mail is often stored on cell phones, PDAs, or other computer systems and care must be taken when confronting unopened voice mail.[18] These and other digital audio files are usually only retrievable by a forensic examiner who has specialized software since most phones, at least, have their own operating system. If a forensic examiner has found voice mail or other recorded messages on seized media, those audio files can be copied as a link in the forensic report, or recorded separately on a CD or DVD for easy transmission to the defense and easy use in court.

Many surveillance videos and audiotaped statements are currently stored on or can be converted to a digital format. Digital audio and video files are easily transferred to CD-ROM or DVD for the defense and the court. Some software programs allow for enhancement or transcription of digital audio files and sometimes even video enhancement, but most programs will save the files in a format accessible to most computers such as AVI, WAV, or M-PEG files.

If a prosecutor does reduce an electronic statement to written format, that transcript must be given to the defense pursuant to an Attorney General Opinion discussing the issue. Where the prosecution has (1) electronically recorded a witness's statement, (2) hired a certified shorthand reporter to report the statement, and (3) furnished to the defense a copy of the electronic recording, the prosecution may … have a duty to order a transcript of the statement from the reporter for inspection by the defense.[19]

3. Internet service provider log files

An Internet service provider (ISP) keep records that are often maintained in the form of logs—logs that can be preserved and retrieved, such as an ISP log of transactions on an e-mail account. Web site log files can contain visitor information such as a date and time of access, and possibly even an Internet Protocol (IP) address. These files are typically obtained from an ISP pursuant to a search warrant or subpoena duces tecum (SDT), or they can be found on a suspect's system if the logging function has been enabled. As a business record, a log can be, and usually is, a data compilation. Business records are generally admissible in stored form as a retrieved image, and in output or printed form, irrespective of the date of retrieval. Keep in mind that logs produced solely for the investigation are not necessarily considered business records and are probably best provided to the defense in printed format.

Additionally, since the investigating officer who requested the log files may not be able to interpret them, you may need either a custodian of records from the ISP or an expert who has experience reading the log files to interpret them. If sent in response to an SDT, log files are typically prepared in a spreadsheet format that is easily provided to defense or put into a trial exhibit.

4. Internet history

A suspect's Internet history or browser information can show a cache of visited sites, bookmarks, or favorite Web sites frequently visited, and even a list of times and dates particular sites were visited. This information is typically listed in a forensic examination report via bookmarks made by the examiner. It may or may not be included within the narrative of the report, and can be printed out or otherwise provided to the defense separately as a list.

5. Cookies

"Cookies" are actually small text files deposited on a hard drive by Web sites to identify visitors to particular Web sites. Typically, they are used to identify interests and provide relevant information by showing an examiner what sites someone has visited.[20] Cookies are

best provided within a forensic examination report because an examiner can provide a list of the cookies found along with important metadata and an explanation of what they mean.

6. Instant messaging (IM)

Instant messages, unless logged or otherwise affirmatively saved by the computer user, will not typically be stored in allocated space on a hard drive. Incriminating fragments or, sometimes complete messages, however, may be found in unallocated or slack space analyzed by an examiner. For this reason, it is important to include any IMs or other text fragments within a forensic analysis report. A good discussion of this issue can be found in *People v. Ulloa*,[21] where a search of a home computer for pictures and videos found evidence introduced at trial in the form of AOL instant messages. There, a motion to suppress for unreasonable search was denied and the criminal conviction of oral copulation with a minor was affirmed.

7. Electronic databases (calendars, address books, or spreadsheets)

Electronic calendars and address books can contain important evidence that is most often bookmarked by a forensic examiner as part of the report. Since it is a relatively graphic piece of evidence typically stored in fairly small-sized files, it is particularly amenable to printing, although it can certainly be provided in electronic format. Other databases or spreadsheets can be included within a forensic report, printed out individually, or provided as an electronic file with or without a viewing program to make it readable in its original state.

8. Flash media

Flash memory is a form of Electrically Erasable Programmable Read-Only Memory (EEPROM). It is a form of rewritable memory chip that, unlike a Random Access Memory (RAM) chip, holds its content without the need of a power supply. Flash memory is commonly used in memory cards, USB flash drives, MP3 players, digital cameras, and mobile phones. From a forensic standpoint, most flash memory devices are acquired and analyzed in the same manner as any hard drive. As such, evidence from flash media can be given as discovery via a forensic analysis report.

9. All-in-one devices

All-in-one devices such as Personal Digital Assistants (PDAs), cell phones, camera phones, and Global Positioning Systems (GPS) are becoming commonplace. Each one, however, has a different file system and different operating system, so generally different methods of forensic analysis are needed to search them. These devices can pose a special challenge for law enforcement due to the volatility of data and wide variety of interface methods (e.g., different cables to connect to a computer) as well as a lack of comprehensive forensic analysis software. The data recovered from these devices, such as the call history on a cell phone, is often very useful. But since most call history data is not acquired as a forensic image, the data will typically be copied into a spreadsheet by the examiner. The forensic examiner's report is, therefore, the most important piece of discovery when dealing with all-in-one devices.

B. Additional Methods of Providing Digital Discovery

1. Cloning

One way to capture the data on a hard drive is to clone it. This method of copying a hard drive or other digital storage device evidence is usually not the preferred choice of forensic examiners because of its inherent instability, and a cloned copy does not allow for automatic verification of the data. Further, deleted files, system files, and other metadata cannot be readily viewed on it. The cloning process makes an exact duplicate of the hard drive, but because it remains bootable, it is subject to alteration in the same way as the original. Additionally, a cloned copy will contain any virus or other Internet-transmitted program found on the original. Typically, clones are made as backup copies by users who may wish to restore data.

A restored hard drive, because it is a complete bootable clone of the original seized drive, allows anyone, even a layperson, to view and analyze the electronic evidence. Because a layperson can view files from Windows in a cloned drive, a defense attorney may request this. In some cases, a clone will be the only available method of obtaining or copying the original evidence. In those cases, a cloned copy of the evidence is the most accurate copy available in current technology and should be treated as the best evidence.

2. PDF files

One way in which reports and other originally printed documents can be maintained without concerns of being modified from their original state is via PDF files. Portable Document Format (PDF) is a file format developed by Adobe Systems for representing two-dimensional documents in a device-independent and resolution-independent format. Each PDF file encapsulates a complete description of a two-dimensional document that includes the text, fonts, images, and two-dimensional vector graphics that compose the document. Importantly, PDF files do not encode information that is specific to the application software, hardware, or operating system used to create or view the document. This feature ensures that a valid PDF will render exactly the same regardless of its origin or destination. PDF is also an open standard in the sense that anyone may create applications that read and write PDF files without having to pay royalties to Adobe Systems.

Documents can be scanned into PDF format via a scanner or copy machine, saved onto CD-ROM, e-mailed to others, or selectively printed by whoever views them. Of concern in large cases is that Bates stamping is not always a part of a PDF file. Many programs such as "IntelliPDF Bates"[22] actually place a Bates stamp on electronic PDF files. Additionally, some photocopy machines have Bates modules available for lease that simply attach to the copier. This is an advisable method, particularly for large "paper" cases like identity thefts, credit card frauds, or other economic cases.

In many identity theft cases, each victim has a report from their local police agency that is associated with the case. Often these are initial car burglary reports or "counter" reports wherein the victim documents the initial loss of personal identifying information. A good way to keep track of victim reports is to scan them into PDF format, and provide them to

the defense digitally. Remember, however, that unless the original scanned document was redacted, these reports contain sensitive information that the defense attorney should be prohibited from distributing to his or her client.

3. Password protected viewers

Some software programs, FTK for example, allow a viewer to access some or all files protected via a password installed by the forensic examiner. In this way, a prosecutor can access all the files in the report, a defense attorney can access all the files except for the contraband or otherwise encrypted ones, and anyone who happens to pick up the CD cannot access the report at all. This may become one of the best ways to provide digital discovery in the near future. Not all forensic examiners are familiar with this process, and not all cases warrant this level of protection for the data. In certain cases such as child sexual exploitation crimes, however, this may be a realistic and satisfactory way to proceed with discovery.

4. Printouts

As nice as it is to carry one CD into court when providing discovery instead of bankers' boxes full of paper, it is not always feasible. Some prosecutors may still insist on having one complete paper copy of all the evidence in a given case. Some defense attorneys may insist on obtaining paper copies of everything no matter how voluminous. When so requested, bear in mind that printing out hundreds or thousands of pages of material will take time and incur some printing costs. In many cases, those costs will have to be borne by the prosecutor's office or the courts.

III. Maintaining Security of Sensitive Digital Evidence

A. Technical Security Requirements

It can be technically challenging to keep digital images secure because random remnants of a particular file can be stored in a computer's internal files. All digital images viewed on an individual computer, including images viewed on Web sites or within e-mails, may remain on the hard drive for a long time, and therefore remain accessible to anyone who uses that computer. Nearly everything viewed on a computer screen is captured in "temporary" files and saved on the hard drive. Additionally, images viewed on a computer screen are saved in unallocated space. All of this data can remain on a hard drive even after an Fdisk,[23] format, or delete command. Similarly, if images are saved on a floppy disk and later deleted, those images remain in unallocated space for anyone to find.

For example, if a defense attorney receives a digital image as discovery in a criminal case, then views that image on a stand-alone computer or on a networked computer, that image may be retrievable even though the attorney never copied or saved the file. If a recipient of digital images views those images on a computer linked to other computers via a local area network or the Internet, the digital images in the cache memory, swap files, or unallocated cluster space may be retrievable from anywhere on that network. These complexities, coupled with the ability of sophisticated users to retrieve data that has ostensibly been removed or deleted from the computer, make it a challenge to craft an effective and all-encompassing protective order and to

provide sufficient safeguards to ensure that harmful images or sensitive victim information is not subsequently recovered and disseminated as discovery despite the best efforts of all involved.

The best practice when dealing with the discovery of any sensitive digital evidence is to bring the issue to the trial court's attention in the form of a proposed protective order. A protective order can and should identify what specific evidence is being provided to the defense and should make clear that further disclosure of the evidence to anyone not involved in the preparation of the criminal defense should be prohibited absent further order of the court. It should limit the physical location in which the evidence is maintained, the security measures used to protect the evidence from further dissemination, and it should ensure the return of the evidence at the conclusion of the case. A sample protective order is included as an exemplar in Appendix A.

B. Identity Theft Victim Information

Increasingly, personal identifying information is located in digital format in counterfeiting, fraud, or other computer-theft-related cases. Not only is this stolen property, it often represents very personal information about individuals who may never be located or informed of their loss of security. Penal Code section 530.5 in 2007 defines personal identifying information as anyone's name, address, telephone number, health insurance identification number, taxpayer identification number, school identification number, state or federal driver's license or identification number, social security number, place of employment, employee identification number, mother's maiden name, demand deposit account number, checking account number, savings account number, personal identification numbers or password, passport number, date of birth, unique biometric data, other unique physical representation, unique electronic data, telecommunication identifying information or access device, information from a birth or death certificate, and credit card numbers.[24]

Penal Code section 964 further requires all "confidential personal information" be kept confidential by courts and district attorneys. How then does one redact electronic copies of evidence given to the defense? Particularly where there is a well-organized police report that lists the name, address, phone number, driver's license info, and perhaps even a social security number and credit card number of each and every victim—nicely collated for easy access?

With paper copies, it is easy enough to go through each page with a marking pen and physically mark out personal confidential information of victims and witnesses. With electronic copies, some software programs, such as FTK, allow password-protected areas of a report in which sensitive information can be stored. In some cases, sensitive information can be acknowledged and protected in the form of a court order. In other cases, having a defense attorney acknowledge receipt of confidential material, in whatever format, should be enough to satisfy the courts. In all cases, digital copies of evidence should be destroyed at the conclusion of a case.

C. Sexual Assault Victim Evidence

In many sexual assault cases, a victim's computer may contain evidence corroborating her statement or documenting a defendant's statements. Nonetheless, the entire contents of a victim's computer are not appropriately a subject of defense discovery. A reasonable procedure is to search a victim's computer under a limited consent signed by the victim. That consent can be limited by

file type, dates of relevance, or even specifically named files. In this manner, only those files or dates (or however the consent is delimited) may be examined and only those files examined may be given to the defense.

If the defense wants to obtain copies of the victim's entire computer for some other purpose like fishing for exculpatory evidence, let defense counsel present good cause to the trial court in the form of a subpoena. If any dispute develops surrounding what digital evidence is appropriately subject to criminal discovery, take the issue to the trial court for an in camera review.

D. Child Sexual Exploitation Evidence

Images of child sexual exploitation are a form of child abuse that are often found on a computer or other digital media. These images are digital contraband and represent one of the most controversial areas of digital-discovery law and practice. There are some very important considerations to be balanced by any prosecutor faced with a trial judge who does not understand why a prosecutor should not make a copy of the images for the defense.

Penal Code section 1054.1(c), requires the prosecution to "**disclose** to the [defense]… [a]ll relevant real evidence seized or obtained as part of the investigation of the offenses charged."[25] Disclosure is not defined within the statute, nor is there any case law defining "disclosure" within this context. Nowhere does disclosure require duplication. No one would dispute that the defense must have access to all evidence. Access, however, does not always mean duplication of evidence, particularly when that evidence is clearly contraband.

The purpose of the discovery chapter is explicit in Penal Code section 1054: "To promote the ascertainment of truth in trials by requiring timely pretrial discovery;"[26] **and** "To protect victims and witnesses from danger, harassment, and undue delay of the proceedings."[27] Similarly, the California Supreme Court has articulated the purpose of modern discovery statutes as to "further the quest for truth."[28]

In 2003, the California Legislature enacted Senate Bill 877, an urgency statute amending Penal Code section 1054.10 to read:

> (a) Except as provided in subdivision (b), no attorney may disclose or permit to be disclosed to a defendant, members of the defendant's family, or anyone else copies of child pornography evidence, unless specifically permitted to do so by the court after a hearing and a showing of good cause.
>
> (b) Notwithstanding subdivision (a), an attorney may disclose or permit to be disclosed copies of child pornography evidence to persons employed by the attorney or to persons appointed by the court to assist in the preparation of a defendant's case if that disclosure is required for that preparation. Persons provided this material by an attorney shall be informed by the attorney that further dissemination of the material, except as provided by this section, is prohibited.

Note that nothing in this section requires a defense attorney to be provided with copies of images of child sexual exploitation. Rather, it requires that if copies are made, those copies must be

treated very differently than traditional documentary evidence. Further, there is express statutory authority here for judicial oversight of this material in the form of a "good cause hearing."[29]

What is a good cause hearing in this context? At a minimum, a defendant should be required to establish some logical reason why possession of this contraband would further his defense of the criminal charges. Additionally, it should be established that during the course of this good cause hearing, the defendant does not get unsupervised or exclusive access to the contraband material.

Certainly due process requires that criminal defendants have an opportunity to examine and, in appropriate cases, have forensic tests performed on evidence to be offered against them.[30] Due process does not require that the right of discovery in criminal cases is absolute. "The court retains wide discretion to protect against the disclosure of information that might unduly hamper the prosecution or violate some other legitimate governmental interest."[31] Moreover, a defense attorney bears some responsibility for making an effort to examine evidence. "It is the duty of the defendant's trial counsel to go to the office of the district attorney and inspect the [materials] available to him there."[32]

Legally incapable of consent, children who are sexually exploited once by being exhibited in child pornography are perpetually exploited: first by the original performance of the acts, then by the creation of a permanent record of the conduct, then again each time that record is reproduced, and again when that photograph, film, or videotape is viewed or passed on to another.[33] **Preventing continued sexual exploitation and abuse of children**—even if sanctioned through a court order mandating duplication of the child pornography images for defense discovery purposes—**constitutes a compelling governmental objective of surpassing importance**.[34]

Unlike the provisions of Penal Code sections 311 et seq., in which the possession and distribution of images of child sexual exploitation do not apply to the activities of law enforcement and prosecuting agencies in the investigation and prosecution of criminal offenses,[35] there is no statutory immunization for the possession of child pornography for the purpose of preparing a criminal defense or pursuant to criminal discovery. Moreover, it is settled law that there is a compelling state interest in protecting children from sexual exploitation, and that this policy lies behind the California Legislature's decision to create a comprehensive statutory scheme prohibiting the possession, duplication, and distribution of child pornography.[36]

"The prevention of sexual exploitation and abuse of children constitutes a government objective of surpassing importance."[37] The United States Supreme Court has found that "the use of children as subjects of pornographic materials is harmful to the physiological, emotional, and mental health of the child."[38] Further, the child suffers "psychological harm,"[39] and an invasion of the child's "vulnerability"[40] from the pornographic depiction. "These harms collectively are the consequential damages that flow from the trespass against the dignity of the child."[41] Thus, there is no question that images of child sexual exploitation represent a permanent record of the sexual exploitation of a child, which is only exacerbated by its duplication and distribution.[42]

As of 2007, *People v. Westerfield*[43] is the only published case on the issue of discovery of images of child sexual exploitation in California. There, the Court of Appeal in the Fourth District focused primarily on the narrow question of whether the statutory scheme governing lawful possession of child pornography barred the distribution of such materials to the defense, and

whether such distribution would subject the prosecution to liability. The *Westerfield* court rejected the prosecution's interpretation of the statutory scheme and concluded that distribution of child pornographic materials to the defense was not expressly barred by sections 311 et seq.[44] The court then, in a very cursory analysis, went on to conclude that the prosecution was therefore affirmatively obligated to reproduce and distribute the documents to the defense under the rules of discovery, without any consideration or discussion of the countervailing considerations set out above. Indeed, the *Westerfield* court relied exclusively on the unique facts of that case as justifying the order to compel discovery, namely the sheer number of photographs at issue and the fact that the defendant had asserted his right to a speedy trial. The court justified its ruling by noting simply: "Finally, requiring the defense to view—and apparently commit to memory—the 'thousands' of images at the computer crimes office obviously impacts Westerfield's right to effective assistance of counsel and his right to a speedy trial."[45]

The *Westerfield* court made quite a leap from its finding that distribution was not statutorily **prohibited** by Penal Code sections 311 et seq., to its conclusion that reproduction and distribution was constitutionally **compelled**, a notion that has been soundly rejected by the federal courts considering this same issue in the federal criminal discovery context. In *United States v. Kimbrough*,[46] the United States Attorney's office refused to duplicate the charged item of child pornography, offering instead to allow the defense and their expert access to it. The defendant moved to dismiss based on a violation of discovery and the trial court denied the motion. The Fifth Circuit Court of Appeal affirmed the trial court's ruling, finding that the government's actions were reasonable and permissible under the Federal Rules of Criminal Procedure 16(a)(1)(C).[47] Implicit in this ruling is the finding that the government's actions were also reasonable and permissible under the United States Constitution. The court held "[w]e find that any prejudice or technical violation of Rule 16 is insufficient to comprise a deprivation of Kimbrough's constitutional rights."[48]

Similarly, in the case of *United States v. Horn*,[49] the trial court properly denied the defendant's motion to obtain copies of the videotapes that were going to be used against him at his trial on child pornography charges. The court found it sufficient for the defendant's expert to view the original tapes, especially since the tapes were themselves **prima facie contraband**.

Both of these federal cases were premised on the fact that compelling interests in protecting the children depicted in the pornographic images outweighed any countervailing interest by the defense in obtaining physical copies of those images, and that the defendant's constitutional rights were fully satisfied by simply having sufficient **access** to the materials. In this regard, the federal courts recognized that such images are properly viewed as contraband, like narcotics, stolen property, or weapons, rather than traditional documentary evidence. As contraband, it need only be made available to the defense and to defense expert for testing and analysis, but need not be reproduced and freely distributed to the defense. This logic is all the more compelling in the child pornography context given the harms associated with each additional reproduction and distribution as described by the United States Supreme Court in *New York v. Ferber* (1982) 458 U.S. 747.

Additionally, the analysis in *Westerfield* wholly fails to address the countervailing considerations outlined in *Ferber, Kimbrough*, and *Horn*. The discovery statute does not create any statutory obligation to **reproduce or distribute** evidence. Rather, as with the comparable federal rules,

section 1054.1(c), simply requires **disclosure**. Moreover, section 1054(d), expressly recognizes the need to protect victims as an element of the discovery process. Accordingly, even assuming the result in *Westerfield* was correct in light of the facts of that case, it should properly be viewed as representing the extreme situation in which duplication and distribution was compelled simply because the alternative was unworkable.

Penal Code section 1054 nowhere mandates that real evidence, particularly contraband evidence, be created anew merely for the convenience of the defense attorney. It requires only disclosure of that evidence. Thus, as long as the prosecutor has given the defense an opportunity **to examine and review** the materials in evidence, the requirements of Penal Code section 1054.1 should be satisfied. There should be no obligation on the part of the prosecution to reproduce physical evidence for the defense as discovery. If, for example, a stolen painting is the inculpatory evidence, the defense attorney would have an obligation to view, examine, and perhaps even have that painting professionally analyzed. The prosecutor, however, has no obligation to make a reproduction of the painting. He or she need only disclose its existence and make it available to the defense.

Most recently, the federal Adam Walsh Child Protection and Safety Act of 2006 was signed into law on July 27, 2006. There, section 3509 of title 18 of the United States Code was amended to add the following language:

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

Thus, in a federal prosecution for child sexual exploitation, this issue has now been resolved by statute. California is still a few steps behind, however, and prosecutors should be aware of the issue and be prepared to educate both the judiciary and the defense bar.

Clearly as technology changes, it will become more and more convenient to reproduce different kinds of material. That will not change the policy considerations which must be weighed in the balance, however. Just because some evidence is **capable** of being reproduced does not mean it

should be reproduced. The goal of criminal discovery is to provide access and promote truth while keeping in mind the rights of the victim and the overarching concerns for public policy.

Note that *Westerfield* focused on the defense's need to have unfettered access to the contraband evidence. There are many ways in which prosecutors and law enforcements officials can satisfy this requirement without duplicating the images themselves. As long as a defense team knows about the contraband evidence, has reasonable access to it, and can have it forensically analyzed to whatever extent they choose, the evidence has been disclosed and the team should be able to adequately prepare for the defense.

The defense should have access to the evidence, even accommodated access, for the sake of convenience. That having been said, the compelling governmental interest in not reproducing child pornography should prevent further reproduction and distribution of the digital images absent a court order finding some good cause for doing so. An example of a Response in Opposition to Defense's Motion to Compel Discovery is included at Appendix B.

An increasingly popular alternative to copying digital images of child sexual exploitation for the defense is to allow a defense attorney to view the images in a laboratory setting. This is common for most tangible forms of evidence and should be considered when dealing with digital images of child sexual exploitation.

Most forensic laboratories, and many law-enforcement evidence rooms, have the capability of setting up a secure room with a stand-alone computer. It is important that the computer have no output devices like a printer, disk, or USB drive, and that the attorney be instructed not to photograph (including via cell phone) or otherwise capture the digital images viewed on the screen. The viewing can be held behind a closed door to accommodate any defense concerns about revealing trial strategy, and it can be made available for as long as an attorney needs to adequately prepare the case. In most cases, this setup will provide the defense with an adequate forum for reviewing the evidence, while still protecting the rights of the abused minors depicted in the images. Additionally, it will keep the evidence secure from alteration, and it should satisfy both court and counsel that the prosecution has made every attempt to accommodate the convenience of the defense as much as possible.

Another alternative method of disclosing images of child sexual exploitation to the defense without making copies is to allow a defense attorney to view the images on a "cold" laptop. By providing a defense attorney with a viewing device only, with no output devices, that he or she can review and then return afterward, a prosecutor can satisfy the concerns of disclosing all the evidence while still protecting the purpose of discovery in protecting abused children from further victimization and greatly accommodating the defense by not requiring them to leave their office. This method requires an acknowledgment by the defense attorney that the laptop must be kept secure from others, must not be duplicated in any manner, and must be returned to the prosecution immediately upon completion (presumably at the end of the day). In some cases, a stipulation and order can be drafted ahead of time to solidify the details of the process.

If a court orders a prosecutor to duplicate images of child sexual exploitation, the prosecutor should draft and submit a protective order for that material. A protective order should contain a stipulation that the defense attorney will not further duplicate the images, any duplication

ordered by the court should be accompanied by copies of the protective order and should be returned at the conclusion of the case, and any access to the materials by the defendant should be in the presence of his or her attorney. See a sample protective order at Appendix A.

Prosecutors should make every effort to be creative in supplying access to inspection rather than making copies for the defense.

IV. Managing Discovery

Of primary importance in all digital evidence cases is ensuring that electronic data is collected, retained, securely maintained, and kept accessible. Particularly with a large volume of data, managing all the evidence can become extremely complicated. In practice, there are three common methods of providing digital storage device discovery to defense. One method is to make a forensically acceptable copy, or a forensic image, for the defense. This will require them to use a forensic expert who has access to specialized software, but so would other scientific or technical evidence. A second method is to make a cloned copy of the evidence along with a very clear description of the restrictions for the user of the clone. A third method is to offer image file access at the prosecutor's local task force or evidence room. This is a practical and reasonable way to disclose contraband or confidential evidence that provides unfettered access to the defense, yet keeps sensitive evidence within the control of law enforcement.

When copies must be made, who should pay the costs associated with duplicating vast amounts of digital data? The media upon which to place the copies can be considerably more expensive than traditional costs of photocopying documents or photographs, and Penal Code section 1054 does not address whether the defendant may be charged with the costs of duplicating discovery.

The Attorney General has opined that furnishing copies to the defense is not statutorily mandated. "Section 1054.1 omits any duty by the prosecution to furnish copies of discoverable materials…. It is sufficient, therefore, that the prosecution affords the defense the opportunity to inspect the materials, allowing the defense to make its own copies if it chooses."[50]

California Code of Civil Procedure section 2031(g)(1) states "If necessary, the responding party at the reasonable expense of the demanding party shall, through detection devices, translate any data compilations included in the demand into reasonably usable form."

Currently, many prosecutors' offices provide photocopies of crime reports or exhibits to the defense without regard to costs involved. When large quantities of paper or other media such as video or audio tapes must be copied, many offices require prosecutors to charge the defense for the costs of duplication. When that duplication involves digital media, however, a forensic examiner must expend considerable resources in copying evidence, assuring the accuracy of the acquired copy, and placing that evidence on properly sized and accessible media.

Reasonableness is again the key to successful discovery. While it may not be reasonable to charge a defendant for an investigator's time in making duplicates of a particular piece of evidence, it is entirely reasonable to expect them to provide a hard drive, CD-ROM, or other media upon which to place the evidence.

While the prosecution and defense may come to any agreement they wish regarding the costs of duplication, a good argument exists that the ultimate responsibility for duplication costs lies with the courts.[51] In *People v. Laff*,[52] the trial court ordered half of the costs associated with a special master be borne by the prosecutor's office. The California Supreme Court overturned the court of appeal's denial of the People's writ and held that the public costs of operating the court system could not be shifted to the parties, and that a lack of funds by the court requires them to seek additional public funds—not require the parties to bear the costs of discharging the courts' judicial duties.[53]

V. Conclusion

High tech evidence is voluminous and constantly changing. It can be found anywhere: networks, servers, PDAs, cell phones, laptops, ATMs, surveillance videos, backup media, thumbdrives, iPods, iPhones, MySpace pages, ISP logs, and even on the surface of the keyboard itself. Additionally, it can be extremely fragile; it is particularly susceptible to destruction or corruption. Given these concerns, and the reality that a great majority of digital evidence is simply not suitable for printing out as traditional documents, electronic exchange of digital discovery in criminal prosecutions must be a topic prosecutors appreciate and understand.

Prosecutors are the ones responsible for the truthful, efficient, and conscientious administration of justice. In the realm of digital discovery, this means educating prosecutors and often times the judges before whom they appear. With a little knowledge and creative thinking, prosecutors may be able to resolve electronic discovery disputes before they arise and, hopefully, keep court costs down while elevating the professionalism of all involved in the process.

ENDNOTES

1. For a complete discussion on Prop. 115, see California Criminal Discovery, Pipes & Gagen, pp. 187–88.
2. Penal Code § 1054.
3. *Brady v. Maryland* (1963) 373 U.S. 83, 87.
4. *In re Brown* (1998) 17 Cal.4th 873, 881.
5. *Jamison v. Collins* (2002) 291 F.3d 380, 387.
6. *Id*. at 387.
7. *Izazaga v. Superior Court* (1991) 54 Cal.3d 356, 378.
8. A terabyte is one trillion bytes or 1,000 gigabytes.
9. Penal Code § 13848(a). High Tech Crime is defined as "those crimes in which technology is used as an instrument in committing, or assisting in the commission of, a crime, or which technology is the target of a criminal act."
10. Evid. Code § 1552.
11. Evid. Code § 1553.
12. *www.guidancesoftware.com.*
13. *http://www.accessdata.com/catalog/partdetail.aspx?partno=11000.*
14. *http://www.ilook-forensics.org/.*
15. *http://www.techpathways.com/DesktopDefault.aspx?tabindex=3&tabid=12.*
16. *http://www.spada-cd.info/.*
17. E-mail Detective, *http://www.hotpepperinc.com/emd.html.*
18. For more information on the Electronic Communications Privacy Act, see Chapter IV of this manual, Sections I, et seq. at page IV-1.
19. 85 Ops.Cal.Atty.Gen. 123 (2002).
20. For description of how "cookies" work, see *In re Doubleclick, Inc. Privacy Litigation* (S.D.N.Y. 2001) 154 F.Supp.2d 497 and *In re Pharmatrak, Inc. Privacy Litigation* (D.Mass. 2002) F.Supp.2d, 2002 WL 1880387.
21. *People v. Ulloa* (2002) 101 Cal.App.4th 1000.
22. *www.intellipdf.com/bates_stamp.htm.*

23. The Fdisk tool is an MS-DOS-based tool that one can use to prepare (partition) a hard disk. The Fdisk tool can be used to create, change, delete, or display current partitions on the hard disk. Each allocated space on the hard disk (primary partition, extended partition, or logical drive) is then assigned a drive letter (*http://support.microsoft.com/kb/255867*).
24. Penal Code § 530.5(b).
25. Penal Code § 1054.1(c) (emphasis added).
26. Penal Code § 1054(a).
27. Penal Code § 1054(d).
28. *In re Littlefield* (1993) 5 Cal.4th 122, 133.
29. Penal Code § 1054.10(a).
30. *People v. Backus* (1979) 23 Cal.3d 360, 383.
31. *People v. Superior Court (Barrett)* (2000) 80 Cal.App.4th 1305, 1316.
32. *People v. Garner* (1961) 57 Cal.2d 135, 142.
33. *In re Heather B.* (1992) 9 Cal.App.4th 535, 541.
34. See *In re Duncan* (1987) 189 Cal.App.3d 1348, 1359.
35. See Penal Code §§ 311.1(b), 311.2(e) & 311.10(b).
36. See *People v. Cantrell* (1992) 7 Cal.App.4th 523, 540; *Angie M. v. Superior Court* (1995) 37 Cal.App.4th 1217, 1225; *In re Duncan*, *supra*, 189 Cal.App.3d at 1358.
37. *New York v. Ferber* (1982) 458 U.S. 747, 755.
38. *Id*. at 758.
39. *Id*. at 775 (O'Conner, J., concurring).
40. *Id*. at 776 (Brennan, J., concurring).
41. *United States v. Weigand* (9th Cir. 1987) 812 F.2d 1239, 1244.
42. *Ferber, supra*, 458 U.S. at 759.
43. *People v. Westerfield* (2002) 99 Cal.App.4th 994.
44. *Id.* at 997–998.
45. *Id.* at 998.
46. *United States v. Kimbrough* (5th Cir. 1995) 69 F.3d 723.
47. Fed. R. Crim. P. 16(a)(1)(C) provides in relevant part, "upon request from the defendant that the government shall permit the defendant to inspect, and copy or photograph, books, papers … which are material to the preparation of the defendant's defense or are intended for use by the government as evidence in chief at trial or were obtained from or belonging to the defendant."
48. *Kimbrough*, *supra*, 69 F.3d at 731.
49. *United States v. Horn* (5th Cir. 1999) 187 F.3d 781.
50. 85 Ops.Atty.Gen. 123, 127 (2002).
51. For a good discussion and analysis, see Pipes & Gagen § 5:12.5.
52. *People v. Laff* (2001) 25 Cal.4th 703.
53. *Id*. at 740–741.

Johnette Jauron is a deputy district attorney in Solano County.

This page intentionally left blank.

Appendix A

Sample Protective Order

DAVID W. PAULSON
District Attorney
Solano County
JOHNETTE JAURON State Bar No. 183714
Deputy District Attorney
675 Texas Street, Suite 4500
Fairfield, CA 94533
tel. (707) 784-6800

Attorney for the People

SUPERIOR COURT OF THE STATE OF CALIFORNIA

IN AND FOR THE COUNTY OF SOLANO

PEOPLE OF THE STATE OF CALIFORNIA, Plaintiff, vs. JOHN DOE, Defendant.	NO. PROPOSED STIPULATION AND PROTECTIVE ORDER Date: September 21, 2007 Time: 8:30 a.m. Dept: 4

STIPULATION AND PROTECTIVE ORDER

In this case, the defendant is charged with Possession of Child Pornography, in violation of Penal Code § 311.11(a). The defendant has requested and the Court has ordered the People to disclose:

_____

_____

_____

to an expert for the defendant in this case. Defense Counsel has identified _____ as that expert, specializing in

_____. Said expert's business address is _____ and his/her telephone number is _____. The Court has reviewed said expert's curriculum vitae (CV) and has tentatively determined said individual's experience and background qualify him/her to testify as an expert in the above-listed area of specialization. Pursuant to People v. Westerfield, (2002) 99 Cal.App.4th 994, and noting the provisions of Penal Code section 1054.10, the parties jointly request that disclosure of these materials be subject to the following restrictions:

1. The cost of making any duplicates of this material for the defense shall be borne by the defendant, unless otherwise ordered by the Court.

2. The above-described materials or their contents shall not be disclosed to anyone except the defendant, his counsel of record and any defense investigators or experts working on the case, absent further order of the Court. These materials shall be used only in preparation of the defense in this proceeding. Any person to whom these materials or their contents are disclosed must be provided with a copy of this Stipulation and Order and must execute the Agreement in the form attached hereto as Exhibit A, which shall be served on the Court within ten days of disclosure. While the defendant may review the materials in the presence of counsel, for purposes of assisting counsel in preparing and presenting the defense in this proceeding, under no circumstances shall the defendant be given copies of any part of these materials to keep, nor shall the defendant be left alone with these materials.

3. In no event shall any graphic image containing actual or alleged child pornography be copied, duplicated, or replicated, in whole or in part, including, but not limited to duplication onto any external media. In the event said copying is necessary for preparation of the defense in this proceeding, defense counsel shall separately apply to this Court for leave from this Order. Only upon a showing of a compelling need shall the defense be permitted to make said copy or copies. In the

event a copy of any portion of the materials is ultimately made pursuant to said Order, said copy or copies shall be accompanied at all times by a copy of this Stipulation and Order and any Order specifically authorizing said copy.

4. The above-described materials shall not leave the State of California, the County of Solano, and they shall not be put on the Internet for any reason.

5. Any computer into which the above-stated materials may be inserted into for access and operation shall not be connected to any network while a copy of the materials is accessible on said computer.

6. Any computer into which the above-stated materials may be inserted for access and operation shall not be connected to any printer while a copy of the materials is accessible on said computer unless:

a. the printer utilized is a local printer;

b. the printer is connected only when and as necessary to print non-graphic image files; and

c. the before-named defense expert is him/herself personally present at all times when a printer is connected.

7. The above-described materials must be maintained in a locked safe within the business office of the defense expert and shall remain in said locked safe when not actively being used in the preparation of a defense to the charges in this case. The defense expert will securely clean any computer system or media used to access these materials including the cache memory, swap files, unallocated cluster space, and any other volatile or non-volatile memory at the conclusion of this case.

8. The materials provided to _____ pursuant to this order, and any copies thereof, shall be returned to the Court for destruction within thirty (30) days of the conclusion

of this case for destruction consistent with Penal Code section 312. At said time, the defense expert and counsel for the defendant shall file a brief report to the Court, specifying that the terms of this Order have been complied with. This Order is ongoing and contraband images must be returned to the Court whenever they are found and are no longer necessary for the defense of this case.

9. Failure to abide by any aspect of this order shall result in sanctions by this Court, including contempt, and may be punishable by state or federal criminal charges for possession or dissemination of child pornography.

_____ _____
Date

_____ _____
Johnette Jauron, Attorney for the People Date

ORDER

In light of the stipulation and agreement of the parties to this action, and good cause appearing therefore, it is HEREBY ORDERED that disclosure of the above-described discovery materials shall be restricted as set forth in Paragraphs 1 through 9 above.

_____ _____
Judge of the Superior Court Date

EXHIBIT "A"
AGREEMENT TO BE BOUND BY PROTECTIVE ORDER

I, the undersigned , _____ (print name), hereby acknowledge that I have received a copy of the Protective Order entered on _____, 2007, in the matter entitled People v. , Solano County Case No. , have read and understand the Protective Order and agree to be bound by all the provisions thereof. My business/residence address is as follows:

_____

_____

_____

_____

I consent to personal jurisdiction over me by the Solano County Superior Court for purposes of enforcing the Protective Order.

I declare under penalty of perjury under the laws of the State of California that the forgoing is true and correct.

Executed on this _____ day of _____, 2007, in the County of _____, California.

_____ _____
Date

This page intentionally left blank.

Appendix B

Response in Opposition to Defense Motion to Compel Discovery

DAVID W. PAULSON
District Attorney
Solano County
JOHNETTE JAURON State Bar No. 183714
Deputy District Attorney
675 Texas Street, Suite 4500
Fairfield, CA 94533
tel. (707) 784-6800

Attorney for the People

SUPERIOR COURT OF THE STATE OF CALIFORNIA

IN AND FOR THE COUNTY OF SOLANO

PEOPLE OF THE STATE OF CALIFORNIA,	)	NO.
	)	
Plaintiff,	)	RESPONSE IN OPPOSITION TO
	)	DEFENDANT'S AMENDED MOTION TO
vs.	)	COMPEL DISCOVERY
	)	
JOHN DOE,	)	Date: September 21, 2007
	)	Time: 8:30 a.m.
Defendant.	)	Dept: 4

TO THE DEFENDANT AND HIS ATTORNEY OF RECORD:

The People of the State of California submit the following Response in Opposition to defendant's Amended Motion to Compel Discovery. This Response is based upon the included Memorandum of Points and Authorities, the records on file with the Court, and any evidence to be presented at the hearing on the Motion.

I. STATEMENT OF FACTS

Solano Sheriff's Deputy D. Snedeker submitted report number CR07-1611, which states that on March 7, 2007, after confirming the defendant was on probation and subject to a search and seizure order, he and two other deputies went to the defendant's residence to conduct a probation search. During the search, deputies found 26 hypodermic needles, a mirror with powdery residue (which later tested positive for methamphetamine), a spoon with powdery residue, and 12 baggies containing powdery residue. As deputies entered a bedroom, they saw an EMachine laptop computer that was logged onto the internet. Deputy Bradford opened a file on that laptop and saw several images of what appeared to him to be young males engaged in sexual activity. Deputies seized the laptop along with a hard drive, nine disks, and two additional laptop computers. All digital evidence was sent to the Northern California Computer Crime Task Force (NC3TF) for forensic analysis.

NC3TF Senior Inspector W. Bennet submitted report number HT07-108, which states that on March 27, 2007, he conducted a forensic examination of the evidence using specialized software that allows him to view an exact duplicate of the drive's contents without changing any of the files it contains or the time stamps associated with those files. As he reviewed the files on the Emachine's hard drive, he bookmarked the details of the relevant files and sent those details to an FTK report which he copied onto a CD. That CD, capable of being viewed from any web-based browser, was then placed into evidence. Senior Inspector Bennet found on the hard drive of the Emachine 17 photographs of juvenile males engaged in sexual intercourse and sexually suggestive poses. He estimated the age of the juveniles to be between 11 and 16 years old. He also found numerous pictures of what appear to be teenagers "a little bit older" engaged in various sexual activity. He found the same pictures of juvenile males on the additional hard drive that was seized along with the Emachine.

On May 14, 2007, the People filed an Amended Felony Complaint alleging one count of a

violation of Penal Code section 311.1, exhibiting a minor in pornography, a felony, in addition to the already-filed charges of possession of a controlled substance, possession of a hypodermic needle, and one count of maintaining a place for selling or using controlled substances. On or about August 15, 2007, the Solano County Sheriff's Department made the evidence available for inspection, and counsel for the defendant viewed the report in private and for as long he wanted. The People continue to make the evidence available for unfettered access by defense counsel and any qualified forensic examiner he may hire.

For purposes of clarification, the People believe there are only two pieces of evidence in dispute: 1) an exact duplicate of the 80 gigabyte Emachine hard drive, acquired to preserve the integrity of the original in an unaltered state via a proprietary software program called EnCase, which is viewable by any competent forensic expert (the E01 file); 2) a report of the analysis of that hard drive written by Sr. Inspector Bennett and stored on a CD in evidence (the FTK report).

II. POINTS AND AUTHORITIES

A. There Is A Compelling State Interest in Protecting Victims of Child Abuse

"The prevention of sexual exploitation and abuse of children constitutes a government objective of surpassing importance." (*New York v. Ferber* (1982) 458 U.S. 747, 755.) The United States Supreme Court has found that "the use of children as subjects of pornographic materials is harmful to the physiological, emotional, and mental health of the child." (*Id*. at p. 758.) This conclusion "easily passes muster under the First Amendment." (*Ibid*.) Further, the child suffers "psychological harm," (*id*. at p. 775 [O'Conner, J., concurring]), and an invasion of the child's "vulnerability" (*id*. at p. 776 [Brennan, J., concurring]), from the pornographic depiction. "These harms collectively are the consequential damages that flow from the trespass against the dignity of the child." (*United States v. Weigand* (9th Cir. 1987) 812 F.2d 1239, 1244.) **There is no question that child pornography**

represents a permanent record of the sexual exploitation of a child, which is only exacerbated by its duplication and distribution. (*New York v. Ferber, supra*, 458 U.S. at p. 759.)

More recently, the Supreme Court observed that "as a permanent record of a child's abuse, the continued circulation [of child pornography] itself would harm the child who had participated. Like a defamatory statement, each new publication … would cause new injury to the child's reputation and emotional well-being." *Ashcroft v. Free Speech Coalition* (2002) 535 U.S. 234, 249.

Similarly, the compelling state interest in protecting children from sexual exploitation lies behind the California Legislature's decision to create a comprehensive statutory scheme prohibiting the possession, duplication and distribution of images of child sexual exploitation. (See *People v. Cantrell* (1992) 7 Cal.App.4th 523, 540; *Angie M. v. Superior Court* (1995) 37 Cal.App.4th 1217, 1225; *In re Duncan* (1987) 189 Cal.App.3d 1348, 1358.)

Child pornography is so pernicious that every abused child so depicted is further victimized by each subsequent duplication and distribution of the contraband image, even within the context of criminal discovery. Particularly where as here, the People have made every effort to provide unfettered access to that evidence and the defense has made absolutely no showing of good cause as to why possessing physical copies of the images would assist in the preparation of his defense, the People contend that the Court has no basis upon which to grant the defense request to order that the People duplicate and distribute the digital images of child sexual exploitation in this case.

B. Relevant Law Governing Criminal Discovery Does Not Mandate Duplication and Distribution of Images of Child Sexual Exploitation

Penal Code section 1054.1, subdivision (c), requires that prosecution "*disclose* to the [defense] all relevant real evidence seized or obtained as part of the investigation of the offenses charged." (Emphasis added.) Disclosure is not defined within the statute, nor is there any case law

defining "disclosure" within this context. Disclosure is not the same thing as duplication.

The purpose of the discovery chapter is explicit in Penal Code section 1054: "(a) To promote the ascertainment of truth in trials by requiring timely pretrial discovery;" *and* "(d) To protect victims and witnesses from danger, harassment, and undue delay of the proceedings." Similarly, our Supreme Court has articulated the purpose of modern discovery statutes as to "further the quest for truth." (*In re Littlefield* (1993) 5 Cal.4th 122, 133.)

In 2003, the California Legislature enacted S.B. 877, an urgency statute amending Penal Code section 1054.10 to read:

> (a) Except as provided in subdivision (b), no attorney may disclose or permit to be disclosed to a defendant, members of the defendant's family, or anyone else copies of child pornography evidence, **unless specifically permitted to do so by the court after a hearing and a showing of good cause**. (Emphasis added.)
> (b) Notwithstanding subdivision (a), an attorney may disclose or permit to be disclosed copies of child pornography evidence to persons employed by the attorney or to persons appointed by the court to assist in the preparation of a defendant's case if that disclosure is required for that preparation. Persons provided this material by an attorney shall be informed by the attorney that further dissemination of the material, except as provided by this section, is prohibited.

Nothing in this section requires a defense attorney to be provided with copies of images of child sexual exploitation. Rather, it requires that if copies are made, those copies must be treated very differently than other documentary evidence. Further, there is express statutory authority here for judicial oversight of this material in the form of a "good cause hearing."

July 27, 2006, the Adam Walsh Child Protection and Safety Act was enacted that, among other things, amended the Federal statute dealing with child exploitation evidence **to specifically prohibit reproducing copies of child pornography for the defense in a criminal case**. Section 3509 of title 18 of the United States Code was added as follows:

> **(m) Prohibition on reproduction of child pornography.—**
>
> **(1)** In any criminal proceeding, any property or material that constitutes child pornography (as defined by section 2256 of this title) shall remain in the care, custody, and control of either

the Government or the court.

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

Certainly due process requires that criminal defendants have an opportunity to examine and in appropriate cases have forensic tests performed on, evidence to be offered against them. (*People v. Backus* (1979) 23 Cal.3d 360, 383.) However, the right of discovery in criminal cases is by no means absolute. "The court retains wide discretion to protect against the disclosure of information that might unduly hamper the prosecution or violate some other legitimate governmental interest." (*People v. Superior Court (Barrett)* (2000) 80 Cal.App.4th 1305, 1316.)

Moreover, a defense attorney bears some responsibility for making an effort to examine evidence. "It is the duty of the defendant's trial counsel to go to the office of the district attorney and inspect the [materials] available to him there." (*People v. Garner* (1961) 57 Cal.2d 135, 142.)

C. Westerfield's Analysis Was Wholly Inadequate and Its Conclusion Was Overbroad and Therefore Incorrect

The defense cites the decision by the Fourth District Court of Appeal in *People v. Westerfield* (2002) 99 Cal.App.4th 994, 998, as mandating that all images of children engaged in sexual conduct must be duplicated and distributed to the defense in order to comply with a prosecutor's duty to "disclose" that information. However, *Westerfield's* **very cursory** analysis is properly viewed as describing an extreme case that is limited to the unique facts presented there. Moreover it was decided before the Legislature amended PC §1054.10 to explicitly require an express showing of

good cause in order to reproduce contraband child pornography evidence in a criminal prosecution. To the extent the *Westerfield* case can be read as setting out a broad rule mandating duplication of all images of children in all child sexual exploitation cases, it is wrongly decided. This Court absolutely retains the discretion to sustain the People's objection to the reproduction and distribution of images of children engaged in sexual conduct and in this case, the exercise of that discretion is both proper and necessary.

In *Westerfield,* the defendant was accused of kidnapping a seven year-old girl, murder with special circumstances, and misdemeanor possession of images of child sexual exploitation in a no-time-waived, special circumstances jury trial. (*Westerfield, supra,* at pp. 996-997.) Police and FBI agents seized thousands of images of child sexual exploitation in several different formats from the defendant's computer, photographic, and video collection, storing it at an FBI laboratory. The prosecutor allowed the defense attorney access to view the material only at the FBI office and only as monitored by law enforcement. (*Ibid.*)

The defense moved to compel the prosecution to duplicate and distribute to the defense copies of all of the digital and video images of children engaged in sexual conduct. The prosecution objected, contending that the statutory scheme governing the lawful possession and distribution of images of child sexual exploitation for law enforcement purposes did not allow for providing such materials to the defense in a criminal case. (*Id.* at p. 997.)

The Court of Appeal in *Westerfield* **focused primarily on this narrow question** of whether the statutory scheme governing lawful possession of child sexual exploitation images barred the distribution of such materials to the defense, and whether such distribution would subject the prosecution to liability. The *Westerfield* court rejected the prosecution's interpretation of the statutory scheme and concluded that distribution of images of child sexual exploitation to the defense was not expressly barred by section 311 et seq. (*Id.* at pp. 997-998.) However, the court then went

on to summarily conclude, in a very cursory analysis, that the prosecution was therefore affirmatively obligated to reproduce and distribute all images to the defense under the rules of discovery, without any consideration or discussion of the countervailing considerations set out above.

Indeed, the *Westerfield* court relied exclusively on the unique facts of that case as justifying the order to compel discovery, namely the sheer number of images at issue, the various media involved, the unwillingness of the FBI agents to allow the defense to view the images without their presence, and the fact that the defendant had asserted his right to a speedy trial in a capital case. The court justified its ruling by noting simply: "Finally, requiring the defense to view -- and apparently commit to memory -- the "thousands" of images at the computer crimes office obviously impacts Westerfield's right to effective assistance of counsel and his right to a speedy trial." (*Id.* at p. 998.) Consequently, the ruling in *Westerfield* is properly viewed as woefully incomplete in failing to weigh all of the considerations inherent in the distribution of child sexual exploitation images and as limited to the unique facts of that case in which the limitations imposed on the defense by the prosecution were unduly burdensome given overly restrictive access and the incredible volume of images.

First, *Westerfield*'s unwarranted leap from its finding that distribution was not statutorily *prohibited* by Penal Code section 311, et. seq., to its conclusion that reproduction and distribution was constitutionally *compelled* has been soundly rejected by the federal courts that have considered this same issue in the federal criminal discovery context.

In *United States v. Kimbrough* (5th Cir. 1995) 69 F.3d 723, the U.S. Attorney's office refused to duplicate the charged item of child sexual exploitation, offering instead to allow the defense and their expert access to it. The defendant moved to dismiss based on a violation of discovery and the trial court denied the motion. The Fifth Circuit Court of Appeals affirmed the trial court's ruling, finding that the government's actions were reasonable and permissible under the Federal Rule of

Criminal Procedure 16(a)(1)(C).[1] Implicit in this ruling is the finding that the government's actions were also reasonable and permissible under the United States Constitution. The court held "[w]e find that any prejudice or technical violation of Rule 16 is insufficient to comprise a deprivation of Kimbrough's constitutional rights." (*Id*. at p. 731.)

Similarly, in the case of *United States v. Horn* (5th Cir. 1999) 187 F.3d 781, the trial court properly denied the defendant's motion to obtain copies of the videotapes that were going to be used against him at his trial on child sexual exploitation charges. The court found it sufficient for the defendant's expert to view the original tapes, especially since the tapes were themselves *prima facie contraband*.

Both of those cases were premised on the fact that the compelling interest in protecting the children depicted in the graphic images outweighed any countervailing interest by the defense in obtaining physical copies of those images, and that the defendant's constitutional rights were fully satisfied by simply having sufficient *access* to the materials. In this regard, the federal courts recognized that such images are properly viewed as contraband, such as narcotics, stolen property, or a weapon, rather than traditional documentary evidence. As contraband, it need only be made available to the defense and to defense expert testing and analysis, but need not be reproduced and freely distributed to the defense. This logic is all the more compelling in the context of child sexual exploitation given the harms associated with each additional reproduction and distribution as described by the U.S. Supreme Court in *Ferber, supra.*

The analysis in *Westerfield* wholly fails to address the countervailing considerations outlined in *Ferber, Kimbrough*, and *Horn*. As explained above, the discovery statutes do not create any

---

[1]. FRCP 16(a)(1)(C) provides in relevant part, "upon request from the defendant that the government shall permit the defendant to inspect, and copy or photograph, books, papers . . . which are material to the preparation of the defendant's defense or are intended for use by the government as evidence in chief at trial or were obtained from or belonging to the defendant."

statutory obligation to *reproduce* or *distribute* evidence. Rather, as with the comparable federal rules, section 1054.1, subdivision (c), simply requires *disclosure.* Moreover, section 1054, subdivision (d), expressly recognizes the need to protect victims as an element of the discovery process. Accordingly, even assuming the result in *Westerfield* was correct in light of the facts of that case, it should properly be viewed as representing the extreme situation in which duplication and distribution was compelled simply because the alternative was unworkable.[2]

The People recognize that the court in *Westerfield* interpreted the statutory prohibitions against possessing images of child sexual exploitation as not applying to the distribution of those images to defense counsel in a criminal case in order for the defense to prepare for trial. However, although *Westerfield* interpreted the statutory scheme as not intending to create any criminal liability for such distribution, *Westerfield* all but ignored the clear legislative intent underlying those provisions to *limit as much as possible* the reproduction and distribution of such images of child sexual exploitation. By expressly identifying who could possess and distribute such materials and identifying the specific purposes and circumstances under which those people could lawfully possess

---

[2]. As an aside, the *Westerfield* court's statement linking the defendant's right to effective assistance of counsel to his assertion of his right to a speedy trial in light of the high number of pornographic images is logically flawed. First, while a defendant has a statutory right to a speedy trial within 60 days, the constitutional right to a speedy trial is based on reasonableness, rather than a fixed time frame, and that reasonable period is necessarily dependent upon the complexity of the issues and the volume of the evidence. The requirement that defense counsel examine and analyze 1000 digital pornographic images, rather than be provided with hard copies, is no different from the situation of a defendant charged with possessing 1000 different packages of controlled substances, each of which must be submitted to laboratory testing. The delay involved in such testing is unavoidable and does not implicate a defendant's constitutional right to a speedy trial.

Moreover, a defendant may not play off one constitutional right against another to create his own claim of error and then raise that complaint on appeal. Thus, if a diligent trial attorney simply cannot adequately prepare for a large case (such as a capital case like in *Westerfield*), the defendant cannot assert his right to a speedy trial in order to create error by forcing defense counsel to proceed while insufficiently prepared and then claim ineffective assistance. Accordingly, the *Westerfield* court's cursory analysis as to why duplication and distribution should be *compelled* is premised on false choices and overstated constitutional concerns.

and distribute such material, the Legislature evinced an unmistakable intent to *narrow* the class of people who possessed this type of contraband and to *curtail* the circumstances justifying reproduction and distribution of such harmful materials. Thus, even when reading logical exceptions into the statutory scheme, as was done by the court in *Westerfield*, the courts must be ever mindful that such exceptions should be narrow and limited to *compelling* circumstances based on the facts of each case, rather than setting out wholesale blanket exceptions without regard to actual need. Critically, such compelling circumstances simply are not present in the instant case.

III. CONCLUSION

Ordering the People to duplicate and distribute digital images of child sexual exploitation to defense counsel as part of a criminal discovery order is tantamount to ordering the creation of new illicit material. There is no statutory exemption for distributing child pornography to criminal defense attorneys or criminal defense experts; only for law enforcement and prosecution agencies. It is contrary to the legislative intent behind Penal Code section 1054 and Proposition 115, it is contrary to federal law on the same issue, and it bears no reasonable relationship to the protection of the defendant's constitutional rights or any other sense of fundamental fairness. Furthermore, it continues a cycle of victimization that harms abused children. There is hardly a more compelling state interest than preventing the further abuse of children. The People remain willing to work with this Court and counsel to craft alternative accommodations to allow for reasonable access to the contraband evidence which protect the rights of the defendant and which protects the abused children from unnecessary further victimization.

The People respectfully requests this Court deny the defendant's Motion to Compel requiring the People to duplicate and distribute the digital image of child sexual exploitation here.

//

Dated: November 6, 2007

Respectfully submitted,

_____
JOHNETTE V. JAURON
Deputy District Attorney