Legal Solutions
Embracing Technology

The Law Firm of Donald Wochna LLC
www.wochnalawfirm.com
dwochna@wochnalawfirm.com
330.815.2891

ELECTRONIC DEVICES AS WITNESSES

Donald Wochna
Attorney
Certified Computer Forensic Examiner (CCFE)
Certified Mobile Forensic Examiner (CMFE)

In order to begin to spot legal issues raised by the use of electronic data extracted from electronic devices, it is essential that attorneys have a way of thinking about the device. In many respects, understanding electronic devices as witnesses is no more difficult than identifying human witnesses; extracting relevant electronic data is no more difficult than interviewing witnesses; and spotting legal issues in the use of the data as evidence is no more difficult than challenging the accuracy, precision, reliability, admissibility and credibility of witnesses and experts.

I. Forensic Science Fundamentals: The Dawning of the Age of Machine as Witness

The scope of expert knowledge in the area of electronic data is rapidly changing. In 1983 when this author began practicing law, attorneys could comfortably ignore technology because client information was shared in paper productions. While clients may have used computers to process data, most communication was done by phone, letter, or facsimile.

By 1999, when this author first began consulting and testifying as a computer forensic analyst, attorneys could remain ignorant of the means and methods by which computers (and other electronic devices) created, stored, processed, and transported data because this knowledge was outside the scope of an ordinary lay person, and consequently was “expert” knowledge. For example, in 1999 it was common for this author to explain “metadata” to an attorney, judge, or jury because they usually had no knowledge of its meaning. Similarly, many people believed “delete” meant that data was removed from a computer.

Like all areas of knowledge, however, the scope of computer information generally known to lay persons expanded over time. Thus, it became common knowledge that “delete” does not remove data from a computer (but the exact steps triggered by the “delete” command remained “expert” knowledge). Additionally, new electronic devices (especially the smart phone) presented their own “expert” knowledge foundation—resulting in the expansion of expert knowledge and certification to mobile devices and networks.

A silent revolution occurred in 2015, however, that promises to dramatically change the practice of law. In 2015, the Ohio Supreme Court approved changes in the comments and interpretation of the Rules of Professional Conduct that struck a balance between the practice of law and technology. By demanding that attorneys obtain knowledge of the advantages and risks of relevant technology, the Court added a technology-knowledge component to the

definition of "Competence" to practice law. This addition is not surprising to those attorneys that recognize that information has migrated from people and paper and has become part of the electronic device environment in which we all practice law. Whether its cell phones, computers, mobile devices, internet of things, or network devices, the electronic device environment creates, processes, transports, and stores data, many times without our knowledge. No attorney can competently represent a client in civil, criminal, domestic, juvenile, or any other area of law without developing both a "way of thinking" about this electronic device environment and a "way of practicing" that leverages knowledge of the electronic devices to focus upon material issues in legal matters, obtain meaningful results, and improve adversarial skills.

This seminar is the first step in your journey leading you to comfortably use knowledge of electronic devices to issue-spot, apply your legal experience to electronic evidence, and to achieve your legal objectives in an efficient manner. You will be led through a "way of thinking" about electronic devices that will serve you in identifying sources of information relevant to your legal objectives. Once those sources are identified, you will learn about the interdependence amongst electronic devices that causes one source to become multiple sources—each with its own advantages and disadvantages for achieving your legal objectives.

Although practicing attorneys need not acquire the knowledge, skill, and certification to conduct forensic examinations, it seems inescapable that these attorneys must, at a minimum, understand the scope and nature of a forensic analysis in order to integrate the forensic analysis with the facts and strategies of any particular case. The author believes that attorneys offering forensic services (either as law-related services or as integrated legal services) will become a common business model similar to that developed in the area of medical malpractice.

Just as knowledge in hundreds of areas of study has been organized in accordance with one or more knowledge paradigms, this white paper and its associated seminar organizes Electronic Forensic Knowledge for Attorneys into the following paradigm:

A. Sources of Data within Electronic Data Systems;
B. Methodology to access Sources without destroying data;
C. Investigative Frameworks to extract available data from Sources;
D. Analysis of artifacts extracted
E. Opinions and Conclusions supported by the Forensic Analysis.

Most of this Knowledge paradigm is comprised of standardized methodologies created by organizations such as NIST, the Scientific Working Group on Digital Evidence, and/or local policing agencies. This paper will present some issues for attorneys to consider as they critically analyze the following in a criminal matter:

- The accuracy and scope of the identification of sources of data within a relevant electronic data system;
- the methodology used to access those sources;
- the investigative framework followed to extract available data
- the scope of analysis conducted upon artifacts available;

- the accuracy of opinions and conclusions (as well as the efficacy of alternate explanations) of artifacts to be used as evidence in a criminal matter.

I. Sources of Data within an Electronic Data System: the accurate and complete identification by law enforcement or by an investigative attorney of sources of relevant data within an electronic environment requires a way of thinking about the environment.

Critically analyzing law enforcement's identification of relevant electronic devices demands that criminal defense attorneys understand the facts and explore the devices related to a matter in a fashion similar to that used by in-house counsel to investigate internal fraud. This author suggests criminal defense attorneys view electronic devices a "electronic witnesses" in a case.

1. Treating Electronic Devices as if they were Witnesses.

Electronic devices are everywhere. They come in all sizes and colors, and the trend seems to be that they get smaller and more powerful each year. They include computers, cell phones, medical devices, pda's, thumb drives, and a host of devices many of which remain invisible to us. A computer manages the operational functions of our vehicles, including, monitoring RPM, throttle position, shift lever position, vacuum, oxygen, and the amount of weight placed on the passenger seat. Computers fly our airplanes, control temperature in our freezers, monitor our property when we are gone, and, of course, allow us to communicate across the internet. In some situations, we may not even be aware that we are interacting with some form of electronic device. For example, a recent news report focused on employees in a hospital who were surprised to learn that their employee identification tags included a small Radio Frequency Identification Device (RFID) that was communicating with a computer to monitor employee hand washing and location on the hospital premises.[i]

When something occurs in our lives that requires investigation of our actions or the actions of others with whom we interact, the electronic devices used by each of us may be our best witness. Treating electronic devices as witnesses is merely recognizing the special capabilities of these devices: they contain electronic memory and processing capabilities. Their memory allows them to store information, like a file cabinet: the information created by the key player using the device, such as the documents, memos, email etc. The processing capability of each electronic device allows each device to also record the manner in which the device was used.

As described in greater detail below, electronic devices automatically store information about the manner in which they are being used at any time. This information is created—not by the key player using the device—but rather by the file system, operating system and applications installed on the device. Event information created by the device can be processed and the manner in which the device was used can be "recreated. This is, basically, the purview of device forensic analysis.

Wochna Law Firm
dwochna@wochnalawfirm.com

2. A Two Step Process of Identifying the Electronic Witnesses that are the Sources of Discoverable Information

The power of the Computer as Witness (and Storage Container) paradigm is that it allows us to begin to accommodate electronically stored information in any case by relying on a skill set that is well developed in practice: identifying key players/witnesses in a case. In order to accurately include as witnesses those electronic devices on which may reside relevant data, we ought to consider the following three step process:

a. Step One. Focus on the Electronic Device, not the individual electronic records or documents. Generally, identifying relevant electronic devices as sources of electronic evidence is no more difficult than identifying key players. The identification of relevant electronic devices focuses upon the "device"—not upon the data resident on the device. This is similar to initially focusing upon identifying the witnesses and leaving to another day the act of interviewing each witness to identify relevant testimony. At the commencement of a matter, when we have duties to preserve relevant electronically stored information, we ought to focus on preserving the "device" rather than the individual documents on the device. Preserving the device will automatically preserve the data on the device. The advantage of preserving the device includes the fact that preservation of the device does not require that we search the device. There is no need to expend time and money early in the case addressing the volume of documents resident on each electronic device that might be potentially relevant to the matter. There is no need to become concerned and overwhelmed by the volume of data that might exist in a particular case. Furthermore, preserving the device, instead of individual documents, preserves all the evidence, is accomplished in minutes (faster than the device can be searched); insulates us from the litigation response process, and is affordable.

b. Step Two: Identifying the devices used by key players. Sometimes we can get overwhelmed by the number of computers and electronic devices used by key players and related to an event or investigation. A hospital, for example, may have thousands of devices, including Radio Frequency Identification Devices embedded in everything from sponges to equipment and name tags. In such a situation, the "Computer as Witness" paradigm proves useful because it analogizes electronic devices to human witnesses.

For example, a school district may have hundreds or thousands of employees; but not every employee is a witness in a matter. Each of us could probably identify those employees that are related to a particular matter; and we would not be overwhelmed by the total number of employees. Similarly, we ought not to be overwhelmed because there are hundreds or thousands of computers and electronic devices in the workplace. Not all electronic devices will be witnesses. We need only identify those devices that are witnesses.

Wochna Law Firm
dwochna@wochnalawfirm.com

Identifying the devices that are witnesses, however, is a bit more complicated than identifying the key players because some of the electronic devices that we use are never touched by us. For example, our email may be important in a case; and we may send email frequently—but we probably have never seen the email server.

We need a process by which to identify potential electronic witnesses. I suggest that we can become skilled at identifying electronic devices that are potential witnesses by first identifying key players, and then identifying the specific electronic devices used by those key players to create information and/or to interact with others.

(i) Devices used by key players to Create Data. For each key player, we ought to first identify those devices that each key player used directly such as laptop or desktop computer. These devices can be envisioned as devices that each key player possessed and controlled—usually a workstation, laptop, pda, cell phone, home computer. Include in this list those devices used by a third person, such as a secretary, on behalf of the key player. As key players are identified, new devices may also be identified. These devices will be presumed to be sources of discoverable information from which to obtain critical evidence (and which must be preserved[ii]). It is not necessary at the beginning of a matter to determine the exact manner in which each of these devices has been used, nor is it necessary at this point to determine the evidence that may reside on these devices.

(ii) Devices used to interact with others. In addition to identifying those electronic devices directly used by each key player, we ought to identify those electronic devices each key player necessarily used in order to interact with others. For example, a key player might use email to communicate with others. It is probable that the key player has never physically touched the email server (the computer that manages the email system). Nevertheless, the email server will be a "witness" because the email server is integral to the email system and whenever the key player used the email system, his computer was required to interact with the email server. Similarly, whenever the key player uses a home computer to connect to a work computer (a process commonly referred to as a "vpn: virtual private network", the home computer necessarily interacts with one or more computers in the network. Whenever computers interact, they may become witnesses as a result of that interaction. Finally, many servers interact with back-up systems and copy data from the server to the back-up media. Thus, copies of data that are resident on a server when the server is "backed-up" to tape will also reside on the back up tape until the tape is destroyed or reused. The data will remain on the back-up tape regardless whether the data remains on the server.

Depending upon the complexity of the electronic devices used, we may need help in identifying the proper devices that will be witnesses in a matter. The two steps describe above require us to accurately explain the data architecture and data flow of the IT systems with which we interact. This process, itself, can become challenging, as we try to interpret the language and

implications of IT Departments. Based upon my experience, it is not unusual to learn that IT is not certain of all aspects of its data architecture; indeed, in some cases the IT department is completely mistaken about essential features of its data architecture. We must continually probe the descriptions of essential IT data systems until we understand the significant features. Additionally, we ought to be especially wary of IT representations that no evidence will be found on a specific device. It is useful to remember that IT professionals may not always know the manner in which a particular device works; they may not be familiar with the artifacts and data file storage characteristics of the device, the file system, operating system, and/or applications on the device. Fortunately, the exact manner in which the device works, the exact data resident on the device, and the exact manner in which the device was used by a key player need not be identified in order to preserve the device.

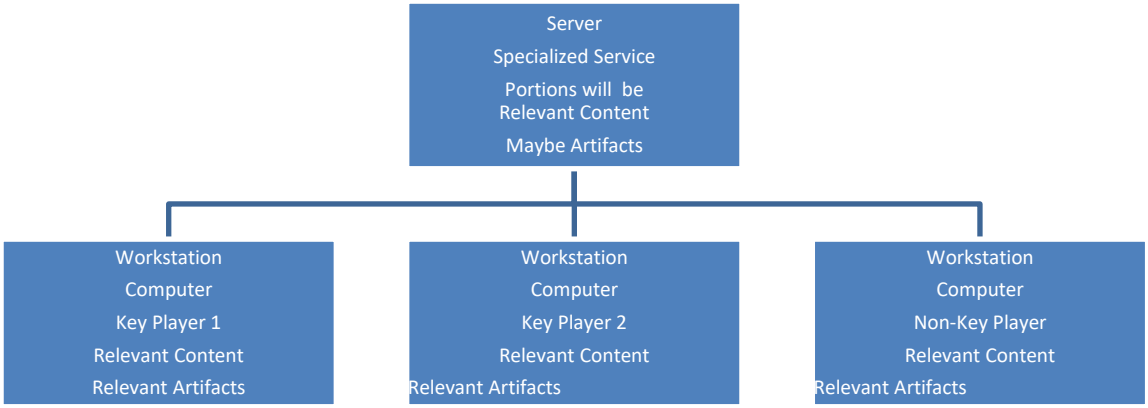
Once the devices used by key players have been preserved, they can be simultaneously searched and analyzed to extract relevant documents, and to determine relevant issues related to the actions of key players and the way in which each device was used.

Counsel can dramatically increase the accuracy of the process of identifying devices in steps 2 and 3 by creating a "matrix" that identifies each key player in a matter and the devices that each key player uses. Creating this matrix may be made easier by including one or more IT personnel who may be able to identify specific devices allocated to each key player. A comprehensive matrix ought to include a discussion of the following topics and an identification of the devices related to each topic.

3. Network Design: Identify the manner in which the network is designed to allow key players to create data and communicate with one another and outside customers, etc. Most networks are based on a "distributed computing" model, in which the processing power of computers is placed at every workstation used by key players. Each workstation computer contains a hard drive and processor connected to other computers over a network. Some of the other computers to which the workstation is networked will include computers that perform specialized functions, named servers. Servers include those computers dedicated to email, storage of files, storage and processing of database information, and storage of applications for use by end users. Data created on a workstation computer flows to servers for processing (email, database, and financial transactions), storage, sharing, etc.

In a distributed computing network, every workstation computer used by a key player may contain relevant electronic evidence, even if the network is configured to require data be saved onto file server computers. This is because computers with hard drives and processors generally operate by automatically recording information to their internal hard drive. This automatic function is used by the computer to recover data from operating system crashes, improve speed and efficiency of workstation computers, and permit multi-tasking at the workstation. As a

result of the normal operation of the computer, file system, and the applications used by key players, relevant data ordinarily will be resident upon key player workstation computers.



It is common for IT personnel to assume that because a workstation computer is configured to save data to a file server computer, there is no relevant data resident on the workstation computer used by a key player. This assumption is almost always inaccurate, and Counsel may need to probe answers and explanations provided by IT personnel to test the accuracy of such representations. Generally, Counsel can consider it a rule of electronic devices that "If it's on the screen, it's on the machine"—at least until the data is overwritten.

The specialized computers on which are performed specialized functions (such as storage on a file server, or email on an email server) usually will contain relevant electronic evidence along with a large amount of data from non-key players. On servers, it is common to preserve only the electronic evidence related to key players, and to continue the routine, good faith processing of data from non-key players.

Not all networks use a distributed computing model. Some networks are built so that workstation "computers" do not have any hard drive or processing capability. Instead, this type of network uses "dumb terminals" at workstations through which key players operate centralized computers or servers to perform functions. Because the dumb terminal does not contain storage or processing capabilities, the terminal device used by the key player may not contain any electronic evidence that needs to be preserved.

4. Remotely Accessing Network. Counsel should inquire and determine whether the network configuration permits devices other than key player workstations to access the server computers remotely. Many networks permit remote computers (such as home computers or laptops operated remotely) to connect to the network and operate as if the remote device were a workstation computer. These types of connections are usually referred to as Virtual Private Networks (VPN), and their existence will frequently lead counsel to devices used by key players remotely that may also need to be preserved.

5. Virtual Machines. Counsel should inquire whether the network configuration includes "virtual machines". "Virtualization" is the result of special software installed upon workstation or server computers. This special software permits a key player to use a workstation computer or server to create one or more "virtual computers"—computers that appear to exist and operate independently of the workstation computer; but which are actually created by the workstation computer. Virtualization is similar in concept to cloning, in which specialized software allows a key player to use a single workstation computer to create several virtual computers, each running independent of one another and performing independent functions. Once the functions are completed, the key player can collapse the virtual machine electing to save the results of its operation.

Virtual machines permit key players to significantly leverage the programs and software installed on their workstation computers. This capability also has been misused by key players who have created virtual machines and then used them for improper purposes. Many people erroneously believer that the manner in which a virtual machine has been used cannot be determined from artifacts on the workstation computer. Although analysis of these artifacts requires substantial knowledge and expertise in virtual machine technology, Counsel ought to treat virtual machines as simply "special" types of devices used by key player.

6. Database Issues. Counsel should be aware that databases as "sources of discoverable information" present unique preservation (and production) challenges. Databases are designed as hundreds or thousands of discrete "file cabinets", each containing very specific information. For example, a simple database that is used to track orders could be comprised of many individual file cabinets containing the following information:

a. the last names of all customers; b. the street names for all customer addresses; c. the names of all products; d. the prices of all products; e. purchase order numbers of all purchases; f. customer id numbers, etc. If you looked into the database "file cabinet" containing customer last names, all that you would see is a list of names. No data exists in this file cabinet to connect the last names to any address or any purchases. Similarly, the file cabinet containing product

pricing will have only a list of prices; no data will exist that connects a particular price to a particular product.

The power of databases lies in (a) the design feature that breaks down complicated relationships into hundreds or thousands of "file cabinets" (each called a field. The information in each field is called a "value"); and (b) the ability of a database program to answer a question (termed a query) by extracting from each file cabinet only that data that responds to the query. Thus, if counsel requests to know all the products sold to a particular customer during a particular time period, the database software extracts from the several file cabinets the proper information and displays the result on a screen or in a report.

The initial challenge of preserving a database relates to changes in the data in the file cabinets. As clients use a database, the information changes from minute to minute. New customers are added; new orders processed, new products added; old products eliminated; old prices deleted, etc. When a client reasonably anticipates litigation, he therefore, has a duty to preserve a database related to the matter; however, in just a few minutes, the database may have changed.

Additionally, it is generally the case that litigants are more interested in the results of a query and the process by which those results were obtained, than in preserving the exact content of each "file cabinet" data field. Moreover, the client must anticipate that the results of queries from a specific database will be requested in litigation. Indeed, where a very comprehensive database was created for specific litigation, and subsequently transferred to backup tapes and the active database destroyed, a litigant did not need to restore the database from inaccessible backup tapes where the litigant was not under a reasonable appreciation that the database would be requested in subsequent litigation with another party.[iii]

7. Access Control to Data. In determining relevant sources of discoverable information, counsel may gain valuable insight by discussing the means by which the client manages and controls access by key players to relevant data. For example, if a matter includes sensitive financial data generated by a client, Counsel will want to understand how access to that data is limited through the use of network access controls or other means. This understanding will help Counsel to identify those key players that had access to sensitive data and for whom preservation may be particularly important and necessary to accomplish quickly

8. Document Retention Policy. It is critical that counsel understand the document retention policies related to the electronic devices in order to identify those processes that threaten to destroy the electronically stored information that must be preserved. For example, a client may be about to begin a "computer refresh" during which workstation computers of key players may be updated by installing a new operating system and standard set of applications. This process could potentially destroy relevant ESI that ought to have been preserved.

Wochna Law Firm
dwochna@wochnalawfirm.com

9. Devices and Characteristics of Devices about which Key Players may not be aware. Key players may not be aware of every electronic device with which they interact; consequently, key players may not be aware of the existence of one or more electronic witnesses. Identifying the electronic witness (i.e. identifying the sources of discoverable information within the client's data network and architecture) is the single most important skill set for counsel to either acquire or bring to the initial client interview. Identifying the electronic witness can be a very difficult process. Not all electronic devices are computers. Indeed, not all electronic devices are even visible—and yet once their identity is discovered, the devices can easily become the most important, single feature in a case.

a. Seeing the Common Computer as Witness: Spotting the Electronic Device(s) that can serve as witnesses in a particular case is challenging to many attorneys; but it gets easier if counsel continues to treat the devices as if they were individual witnesses. For example, consider a hypothetical case in which an employee of your client used his work computer to connect over the client's company network to the company's server, and unlawfully copied from the server onto a thumb drive a copy of your client-company's customer list. Thereafter, he secretly took the thumb drive with him when he left your client-company and obtained new employment with a competitor. On his first day of work at competitor-in violation of competitor's corporate policy—he connected the thumb drive to his new company work computer and downloaded from the thumb drive onto new company's work computer a copy of your client company's customer list. This scenario is, unfortunately, very common[iv]

In this scenario there may not be any human witnesses to the actions taken by the former employee. The former employee, however, used a company computer and interacted with the Company's network. The computers the former employee used and those with which he interacted are witnesses. Some of these witnesses will be within your client-company's control:

Your client-Company's Work Computer used by Former Employee

Your client-Company's Server[v] on which resides Customer List

Other devices that are witnesses will be within the exclusive control of the former employee, including:

Former employee's thumb drive

Former employee's home computer (to which he connected the thumb drive)

Finally, there are devices that are witnesses that are within the control of Former Employee as he works for New Employer/Competitor:

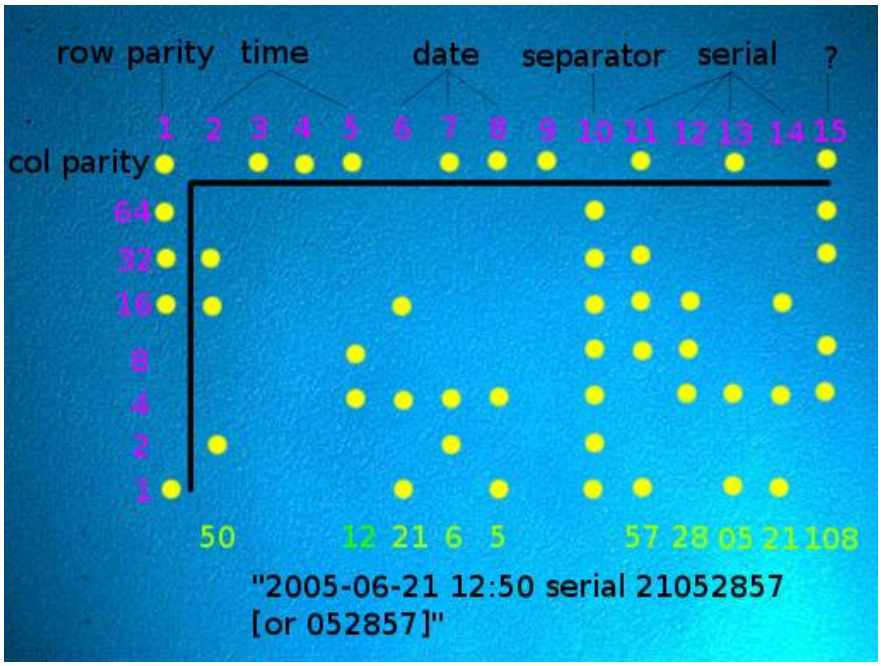
New Employer Work Computer

There may be other devices that are involved with this hypothetical matter; but the devices described above are the ones that are reasonably identifiable at the beginning of this type of case. Once the devices are identified, counsel ought to be wary of making conclusions regarding the electronic evidence that may reside on each device. For example, if counsel simply treated all these electronic devices as "storage containers" or "file cabinets", she might conclude that there is little chance that the former employee created any letter, email, note, or other "document" that would evidence his theft of the customer list. Additionally, counsel might conclude that these devices only need to be searched for a copy of the customer list. If no copy of the list exists on any of the devices, counsel might conclude that there occurred no theft (or that these devices contain no evidence of such a theft).

If counsel reacts this way to this hypothetical case, she has fallen into the trap of trying to identify the "documents" in a case in which electronic devices were used. In this case, for example, there are no "documents" created by the former employee. Nor is there any copy of the customer list on any of these devices (except for the copy on the server where it is stored). However, these devices will contain electronic evidence of the manner in which they were used. Electronic "event" evidence will include information that identifies the thumb drive and that identifies the act of copying the customer list to the thumb drive. This event evidence was created by the operating system and file system when the former employee connected the thumb drive to his work computer and then connected the work computer to the server. By preserving the client-company's workstation computer and server, counsel will have preserved the electronic Event evidence—without ever needing to know or understand the technical nature of that evidence, which can be extracted and analyzed later in the case.

b. Seeing the Uncommon Device as Witness: Not every electronic witness will be a computer. Even the simple color copier can become a powerful witness. Color copiers have become "event witnesses" in certain cases because color copiers secretly embed onto each color copy certain anti-counterfeiting data that identifies the make, model, and serial number of the color copier, as well as the date and time when the copy was made [vi]. In one such case, certain criminals used a color copier to created counterfeit rail tickets. The counterfeit tickets were circulated and ultimately attracted the attention of the Dutch police. The police, however, knew that many color copiers can become event witnesses by analyzing the anti-counterfeiting dots.

Wochna Law Firm
dwochna@wochnalawfirm.com



Above is Example of Anti-Counterfeiting Dots Embedded in Copied Page

By examining the counterfeit ticket, locating the embedded anti-counterfeiting dots, and interpreting those dots, the Dutch police quickly obtained the copier's make, model, and serial number. It was relatively simple, thereafter, to locate the purchaser of the copier and subsequently arrest the people responsible for the counterfeit tickets.

This example highlights the usefulness of treating an electronic device as a witness, even when the exact manner in which the device operates is not known. Treating all electronic devices as if they were potential witnesses in a case is very similar to treating people at the scene of an accident as witnesses

c. Seeing the Uncommon, Invisible Witness: Electronic Devices that are also witnesses will not always be visible or obvious. Radio Frequency Identification Devices, for example, are frequently smaller than a grain of rice and are may be embedded into equipment, tools, and identification tags, etc. Consider a hypothetical case involving a claim that a patient was left lying in a bed, unattended for several hours in a hospital corridor, where he eventually died. Counsel interviewing the hospital client ought to be able to identify the key players, including the on-duty nurse, doctor, and any witnesses that saw the patient in the corridor. Using the three

steps, Computer as Witness Paradigm, counsel ought to expand beyond the identification of key players to include the electronic devices used by each key player. In order to identify the electronic devices, Counsel ought to interview the IT personnel and create a matrix as described above. During this interview, counsel ought to constantly probe IT personnel's characterizations and representations to be certain that counsel understands the data architecture used in the hospital. In this hypothetical, the attorney ought to identify security cameras that record electronically the corridor in question and any RFID (radio frequency identification device) embedded in the patient bracelet. When used to track patients, RFIDs in the patient bracelet communicate with an "interrogator" device to log the location of the bracelet. These tracking logs area stored on special servers and can be provided to counsel. By reviewing these logs, counsel will be able to track the patient's movements throughout the day; and will be able to prove that the patient was never in the corridor unattended for several hours.

In addition to tracking patients by bracelets, RFID technology is being used to track doctors and nurses. RFIDs embedded in employee identification cards permit employee tracking logs to be created and maintained for all employees—including those key players that claim to have seen the patient in the corridor. Their testimony can be corroborated by proving that the RFID logs locate the key player at the precise place and time as their oral testimony[vii].

Counsel need not completely understand how the RFID device works, nor does counsel need to know the exact electronic evidence resident on the device (or on the computers to which the device communicates). Rather, Counsel can get technical help where needed to preserve the device and search it to recover evidence at a later date.

10. Synching: Perhaps one of the most challenging issues for attorneys is recognizing the manner in which devices "synch" with one another to backup data and create additional forensic artifacts that may be relevant to a matter.

II. Digital Forensics: Smartphones, Emails, and The Investigative Framework: criminal and corporate forensic investigations are not conducted in a vacuum.

Forensic examiners do not "make up" the protocols that they want to follow; but rather the operational processes that comprise an investigation have been defined. For example, NIST SP 800-101 rev1, "Guidelines on Mobile Device Forensics" defines the four processes of a forensic examination: Preservation, Acquisition, Examination and Analysis, and Reporting. Each of these processes, in turn, is further defined: for example, the Scientific Working Group on Digital Evidence has developed the Mobile Forensic Pyramid of levels of extraction and analysis.

Criminal Defense attorneys that do not possess much knowledge regarding the manner in which cell phones work, for example, would benefit greatly by reading the NIST SP 800-101, revision 1. For example, the factual underpinnings of the Carpenter v United States case, discussed in the

privacy section below, become much more meaningful when the nature of a cell phone system is understood.

A. Scope of Analysis and Artifacts

For many criminal defense attorneys (especially those who do no in-house investigations) the tools and methodologies associated with the Preservation and Acquisition processes may not be useful except to critically analyze whether law enforcement changed or destroyed data. In most cases, law enforcement identifies the devices that law enforcement determines are relevant to a matter and preserves those devices as part of its initial collection of evidence.

Acquiring access to the data on devices, however, has become a process that ought to interest criminal defense attorneys. At the time of the writing of this white paper, the Apple manufacturer of iPhone and the several manufacturers of Android phones (using an operating system based upon Linux and developed by Google) have two opposing theories of privacy that impact the accessibility of data on their respective phones.

Apple has undertaken several steps to restrict access to data on their iPhone. The method by which access to data is limited begins by limiting the functionality of the "access port" associated with the iPhone.

> Apple quietly introduced a significant privacy safeguard as part of the new iOS 11.4.1 update that was released on July 9th. USB Restricted Mode prevents USB accessories that plug into the Lightning port from making data connections with an iPhone, iPad, or iPod Touch if your iOS device has been locked for over an hour. This seemingly small change goes a long way in blocking tools used by law enforcement to crack passcodes and circumvent Apple's encryption and built-in measures designed to shield sensitive user data.

Almost all forensic analysis of an iPhone requires connecting a USB forensic device to the iPhone through the Lightning port. Once connected, the USB forensic device must execute software commands that permit the software to copy the available SQLite databases to an external storage device for analysis. Some commercial forensic tools include tools that automatically parse the SQLite databases and provide data organized by type in a template report. One of the most common tools is Cellebrite's UFED Physical Analyzer. This tool creates a UFED Logical report and a UFED Data Dump that can be obtained by criminal defense attorneys for analysis.

Android phone manufacturers have adopted an "open source" approach to security and continue to provide significant functionality for USB devices connected to Android phones through the data/charging cable port while in Android Debugging mode (the Android Debug Bridge). The ADB bridge permits investigators to obtain a Physical image of Android phone, while the iPhone Lightning Port limits investigators to a Logical Image.

Wochna Law Firm
dwochna@wochnalawfirm.com

B. Physical versus Logical Image. A physical image of a computer or a cell phone is an exact, byte for byte image of the hard drive, internal storage, sim card, etc. A physical image contains all data resident on the device, including data that is in a "deleted" state as well as data in a "corrupt or incomplete" state. For many years, a physical image was stated to be the "gold standard" of forensics.

> A physical image is a complete image of all the contents of a storage device, a so called bitstream copy. A Bitstream copy involves the copy of all areas of a storage device. Because a bit stream copy is a bit-by-bit copy of the original storage device it will also include the unallocated areas of a storage device. This means you will be able to perform data recovery on this copy, something that is not possible with a normal copy or clone made by "normal" disk cloning software (e.g. Norton Ghost, Acronis Trueimage).
>
> Another great "feature" of a physical image is the possibility to write the image back to a disk. Since a physical image is a bitstream copy of a storage device you will be able to write this image back to the other storage device and create an identical copy of the original. This can be extremely useful if you want to boot up the original system (e.g. for live examination of the system). The system will perform exactly as if the original drive has been inserted.

https://www.raedts.biz/forensics/forensics-101-forensic-image/

A logical image is not as good as a physical image from a forensic perspective. A logical image:

> A logical image is a file system level image. These images are usually created when you are unable to create a physical image (e.g. device limitations) or when you just want to image a certain folder (e.g. a user's mailbox, or a user directory on a server). Creating a logical image is the best way to only capture the data in a folder, a nothing more.
>
> One major drawback of a logical image is that you do not capture any unallocated data. If the suspect has deleted important files prior to the creation of the logical image, there is no way to recover them with a logical image. You should always try to create a physical image when it is suspected that the user might have deleted important data.

Id.

It is impossible to create a Physical Image of an iPhone. Only a Logical Image can be made because of security constraints placed on the accessibility of forensic software to the data on the iPhone through the lightning port. As forensic software manufacturers learned that Physical Imaging was not possible on iPhone, Additionally, the use of the lightning and/or ADB ports to gain access to the device required the forensic software to write some data to the device. Writing data to the target device was always s considered taboo. However, the current standard appears to have changed the marketing and instructional courses to eliminate the claim that Physical Images were the gold standard of forensics and that no data can be written

to the target. The current standard is one embedded within the NIST 800-101 rev 1 standard, that all steps ought to be well documented so that changes in the data state of the targeted evidence can be documented and transparently proven to have not caused any change to relevant evidence.

C. Access via fingerprint or face recognition.

Controlling access to the data within a device is a dual edge sword: for the customer, controlling access is a means of enforcing a subjective expectation of privacy (without regard to the 4th amendment); for law enforcement (and in-house attorney investigations) controlling access invites "jailbreaking" or "hacking" around the manufacturer's installed access control.

For example, based upon the unique nature of fingerprints, many manufacturers installed fingerprint recognition functionality in their computers and/or cell phones. This functionality, however, can easily be defeated:

> It becomes clear that even with little effort a fingerprint scanner can be fooled. Therefore, most scanners today don't come even close to meet the safety requirements of an average corporation. Clearly more effort must be put to improve the scanners, before we can say goodbye to passwords

Fooling Fingerprint Scanners Biometric vulnerabilities of the Precise Biometrics 100 SC scanner, Helsinki University of Technology Course Tik-110.452, included with your download materials.

In an effort to be fair to fingerprint scanners, the "Gummy Bear Attack" may not have been successful:

> A group of students from Washington & Jefferson College's Information Technology Leadership program attempted to test the theory. The students made fingerprint casts from a variety of substances, including not only gummy bears but also modeling clay, Play-Doh and Silly Putty and tested the casts against Microsoft's Fingerprint Reader and an APC Biometric Security device. Some of the substances held fingerprints better than the others but the gummy bears were not successful. From the class's report:
>
> *None of us was able to get a gummy bear to hold a fingerprint, either on the flat back surface, or by tearing the gummy bear open and trying to create an impression on the softer interior. It was theorized that perhaps a superior quality of gummy bear, instead of the generic brand purchased, or a gummy candy with a large surface area would work better. But for the remainder of the experiment the gummy bears became simply a form of sustenance.*

GiveMeaFinge.pdf, included in your download materials.

Facial recognition does not appear to fare any better. If a client uses facial recognition to control access to a phone, can law enforcement force him/her to place their face before the phone in order to unlock it?

Wochna Law Firm
dwochna@wochnalawfirm.com

> A child abuse investigation unearthed by *Forbes* includes the first known case in which law enforcement used Apple Face ID facial recognition technology to open a suspect's iPhone. That's by any police agency anywhere in the world, not just in America.
>
> It happened on August 10, 2018 when the FBI searched the house of 28-year-old Grant Michalski, a Columbus, Ohio, resident who would later that month be charged with receiving and possessing child pornography. With a search warrant in hand, a federal investigator told Michalski to put his face in front of the phone, which he duly did. That allowed the agent to pick through the suspect's online chats, photos and whatever else he deemed worthy of investigation.

See Michalski Search Warrant data provided as part of seminar.

The attempt by manufacturers to decrease the access to data by increasing the privacy controls related to the data portals, invites a concomitant attack: jailbreaking the device. Jailbreaking often uses tools that are not recognized by commercial forensic companies to force devices to perform (i.e. admit access to data) that is excluded by the manufacturer. Pangu is one such tool; but if it permits law enforcement to get access to data by circumventing access control features, what implications, if any, are there for the 4th amendment. It is this author's belief that "hacking" skills will become part of the arsenal of highly qualified forensic examiners who go well beyond the capabilities of commercial forensic tools. Indeed, criminal defense attorneys ought to know with a great deal of specificity the limitations placed upon the forensic examiner by the manufacturer and by limitations in the commercially available forensic software.

D. Interpreting Artifacts: iPhone examples

i. **Difference Between JPG and PNG files.** Both JPG and PNG are considered photo file types, but with significant differences. Jpg files are created when a user creates an image using the iPhone camera. Jpg files contain significantly more metadata than do png files. Not all the metadata fields in a jpg are populated with data. For example, geolocation data (usually written into as a latitude and longitude) usually requires the user to activate the geolocation feature on the phone or on an application controlling the camera.

PNG files are used to create screen shots. A png file is a photo file type used by Apple iPhone to create screen shots of a phone's display. Creating a "png" screen shot is relatively easy. An iPhone user simply presses and holds the top or side button of the phone while simultaneously pressing the Home button. See: "How to take a screenshot on your iPhone, iPad, and iPad Touch" available at: https://support.apple.com/en-us/HT200289.

Once a user creates a "png" file screen shot of his/her phone, the phone automatically names the file in a "IMG_****.png" format, in which the **** are sequential numbers generated by the phone's file system. This "Original" png file includes creation, modification, and last access

metadata created by the "Original" phone in accordance with the ***Time Zone in which the Original Phone was located at the time the png file was created.***

Once the "png" screenshot file is created, it can be sent to another phone. The Recipient phone will save the "png" screenshot as an attachment to an SMS message. The "png" file is saved on the recipient's phone in the "attachments" subfolder of the SMS folder. The Recipient's phone's file system will re-name the "png" file in the "IMG_****.png" format, using the sequential number generated by the recipient's phone. This new file would have its own creation, modification, and last access dates—different from those of the Original png file. **The new file on the recipient's phone will have a creation date set to the Time Zone that the recipient's phone was in, at the time it received the file**.

ii. Green and Blue Bubbles. Text displayed in a png screen shot identifies the type of message and device used by displaying text in green or blue bubbles. The different color balloons define the type of message and device used to communicate. Every iPhone and iPod touch since iOS-5 has come pre-loaded with an app called Messages, which includes a feature called iMessages that is different than SMS messages:

- SMS messages are sent through phone company networks. iMessages are sent between iOS devices and Macs through Apple's servers, bypassing the phone company;

- SMS messages are only sent over cellular networks. iMessages can be sent over cellular networks or Wi-Fi;

- SMS messages are not encrypted, while iMessages are protected with end-to-end encryption. This means that they can't be intercepted and read by third parties like phone companies, employers, or law enforcement agencies;

- iMessages can only be sent from and to iOS devices and Macs. They're represented in the Messages app with blue word balloons. SMS sent to and from non-Apple devices, such as Android phones, don't use iMessage and are shown using green word balloons.

iii. **UTC Time**. The forensic software used by law enforcement to extract artifacts generally parses the associated metadata in UTC time. Universal Time Code format ("UTC) is converted to Eastern Daylight Time (EDT) by subtracting four hours from the UTC time; and converted to Eastern Standard Time (EST) by subtracting five hours from the UTC time data.

Care must be taken to remember that the UTC time values reflect the time zone in which the phone was located when the file was created. The dates on which EDT began and ended are available on look-up tables. For example, in 2012, Eastern Daylight Savings Time ("EDT") began at 2 am on March 11 and ended November 4 at 2 am.

Thus, a phone located in a geographic area subject to EDT on 10.14.12, will record time in UTC values and need to be translated. The UTC time data must be converted to Eastern Daylight Savings Time by subtracting 4 hours. This translation requirement can become very complicated

in investigations involving multiple phones located in different time zones, or devices that are travelling through time zones during a critical period of time.

iv. Authentication of text messages. Most of the time, text messages are authenticated by the person who sent or received them.

> [I]in most cases involving electronic print media, i.e., texts, instant messaging, and e-mails, the photographs taken of the print media or the printouts of those conversations are authenticated, introduced, and received into evidence through the testimony of the recipient of the messages.'" Irwin, 2d Dist. Montgomery No. 26224, 2015-Ohio-195 at ¶ 21, quoting Roseberry, 197 Ohio App.3d 256, 2011-Ohio-5921, at ¶ 75, 967 N.E.2d 233. In Roseberry, the Eighth District Court of Appeals noted that the state could have properly admitted text messages from the defendant through the victim's testimony, " because she was the recipient of the text messages, had personal knowledge of the content, and could [identify] the sender of the messages." Roseberry at ¶ 75.

State v. Norris, 2016-Ohio-5729, 76 N.E.3d 405, (App. 2 Dist. 2016)
In some cases, however, neither the recipient nor sender will testify to authenticate a message. At least one Ohio court has addressed the issue of authenticating text messages without testimony of the recipient:

> While the typical means of authenticating text messages, i.e., having the recipient of the text messages testify and identify the sender, was not implemented here, we nevertheless find the text messages were properly authenticated, as the State presented testimony and evidence that sufficiently linked Norris to the iPhone that contained the text messages at issue.

State v. Norris, 2016-Ohio-5729, 76 N.E.3d 405, (App. 2 Dist. 2016)

The “sufficiently linked” test in *Norris* mirrors the low threshold of at least one appellate court. In a 2015 case of first impression, the Lucas County Appellate Court discussed many of the challenges of electronic evidence, including the authentication and admissibility of a screen shot of a Facebook page and of a song from Sound Cloud. See Ohio v Gibson, 2015-Ohio-1679, Ohio App.Ct, Sixth District, Lucas Cty. The Lucas County Appellate Court held, inter alia, that:

> A trial court "need not find that the evidence is necessarily what the proponent claims, but only that there was sufficient evidence that the jury might ultimately do so." Lorraine at 542, quoting United States v. Safavian, 435 F.Supp.2d 36, 38 (D.D.C. 2006). As stated above, once the prima facie threshold is met, "the burden of going forward with respect to authentication shifts to the opponent to rebut the prima facie showing by presenting evidence to the trier of fact which would raise questions as to the genuineness of the document." Hartford Insurance Co. at *7, quoting Zenith, 505 Fed.Supp. at 1219.

Gibson at paragraph 47.

v. ***Although not considered hearsay, computer-generated records must be authenticated by testimony of a person with knowledge of the reliability of the record.***

Computer-generated records are generally NOT considered hearsay because they are not the statement of a human. For example, the Tenth Circuit in *United States v. Hamilton*, 413 F.3d 1138 (10th Cir. 2005). held that "header" information (including the screen name, subject of the posting, the date that the images were posted, and the individual's IP address) was not hearsay because the "header" information was not the statement of a person. *Id*. at 1142-43. See also *United States v. Washington*, 498 F.3d 225, 231 (4th Cir. 2007) (machine-generated data used in a DUI case to determine whether a blood sample contained drugs or alcohol were not statements of the lab technicians and were not hearsay statements because they were not made by persons but rather by machines analyzing the sample; no Confrontation Clause issues), cert. denied, 129 S.Ct. 2856 (2009); *United States v. Khorozian*, 333 F.3d 498, 506 (3d Cir. 2003) (information automatically generated by fax machine is not hearsay because "nothing 'said' by a machine . . . is hearsay").

Computer-generated records, however, must be authenticated to be admitted. Authentication requires some testimony that the devices and software used to generate the computer records were functioning properly. (See 2 McCormick on Evidence, § 294 at 286 (John William Strong, et al., 4th ed. 1992); Saltzburg at p. 370). Among the factors courts may apply in determining whether a proper foundation for admission of computer-generated evidence has been laid include whether the computer was standard and in good working order, whether the operators of the equipment were qualified, whether proper procedures were followed, whether reliable software was used, whether the program operated properly, and the exhibit derived from the computer. See *State v. Swinton*, 847 A.2d 921, 942-43 (Conn. 2004).

vi. The accuracy of iPhone Read Receipt metadata appears to have been analyzed or tested in only two experiments. The results of those experiments suggest that the accuracy of time value metadata related to iMessage communication exchanges is related to the accuracy of the iPhone System Clock.

Whether time and date metadata associated with iMessages are accurate to the minute and/or second is a complicated issue involving the accuracy of the iPhone System Clock compared to the Apple servers' clock. As summarized by the authors of the only forensic analysis of this issue to date:

> It has been established that the accuracy of iMessage time stamps depends upon whether the time stamping function is carried out globally by Apple servers or the internal system clock of the device. ***When the internal system clock is used to time stamp, the temporal data is as accurate as the system clock. In contrast, Apple server time stamps appear to be only accurate to 128 seconds***, ***which is further complicated by appearing to only update every approximate 137 seconds, in addition to the uncertainty as to which process executes the time stamp function at any given time***. Seeking to discover the triggers for which process is used to time stamp iMessages, this

> research has shown that the accuracy of the receiving device's internal system clock influences whether messages are time stamped locally using the internal system clock, or globally using Apple servers. When the internal system clock is ahead of Apple server's definition of time, Apple servers are used exclusively to time stamp iMessages. When the internal system clock is behind Apple server's definition of time, the system clock is used exclusively to time stamp. Consequently, due to the way in which Apple server times are incremented, a device with an accurate system clock will have iMessages time stamped with both Apple servers and the system clock at varying intervals.

See: "Temporal Analysis Anomalies with iOS iMessage Communication Exchange", Michelle Govan and Kenneth Ovens, School of Engineering & Built Environment, Glasgow Caledonian University, Scotland *Proceedings of Cyberforensics 2014*, University of Strathclyde, Glasgow (hereinafter the "Govan/Ovens" research).

The Govan/Ovens experiment and conclusions were based upon an analysis of:

- 1,800 text messages sent from one Apple ID to another at two second intervals; and
- Metadata time stamps generated when the device clock time was set manually, either in advance or behind time, ensuring that it would always be ahead or conversely behind Apple's server definition of time.

It ought to be noted, however, that it may be impossible to obtain the Apple server's time definition due to the passage of time, or because it is resident only upon the Apple server.[1]

vii. Location and GPS metadata. Several forensic software tools will extract GPS longitude and latitude information from jpg or other picture file formats and automatically plot the location on google maps. Many defense counsel simply accept the plotted locations. It is significant to note that the Device Locations information is extracted from applications that integrate GPS information with their services:

> "Locations" data is extracted from various areas on the mobile device in various GPS serviced apps as shown. It is important to note that this data does not necessarily reflect actual locations the device has visited. Several apps store GPS coordinates as metadata – some of which did not originate on the mobile device being analyzed. So, it's important to note the source and/or the individual application populating the location data to determine its meaning and purpose.

[1] The exact definition and location of Apple server time definition is not public information. It may be necessary to assume that the Apple server time definition is that displayed on an iPhone unless manually changed to be ahead or behind that value.

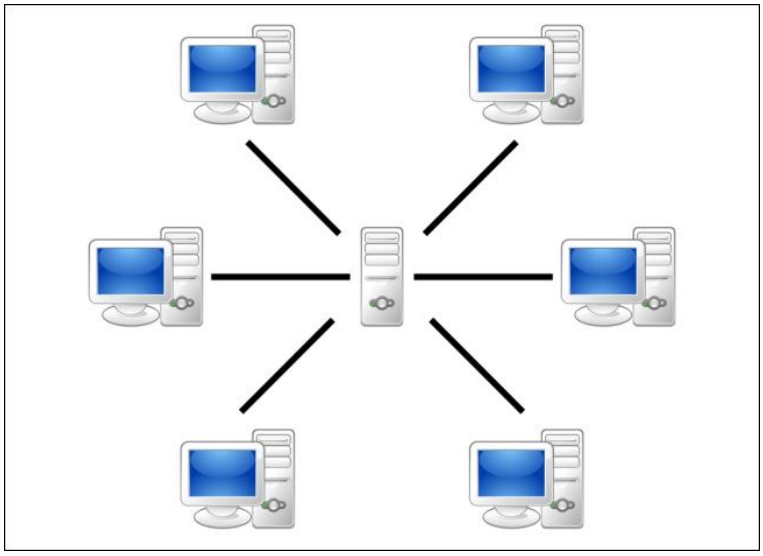
> If Geolocation Services are turned on and the application utilizes the services, these entries will be created in the "Locations" tab according to the application that was being used. Individual application entry metadata will vary from app to app and depending on the iOS and app version.

Cellebrite Extraction Reports: Frequently Asked Questions
https://www.iltanet.org/blogs/russcapps/2017/10/17/cellebrite-extraction-reports-frequently-asked-questions?ssopc=1

\

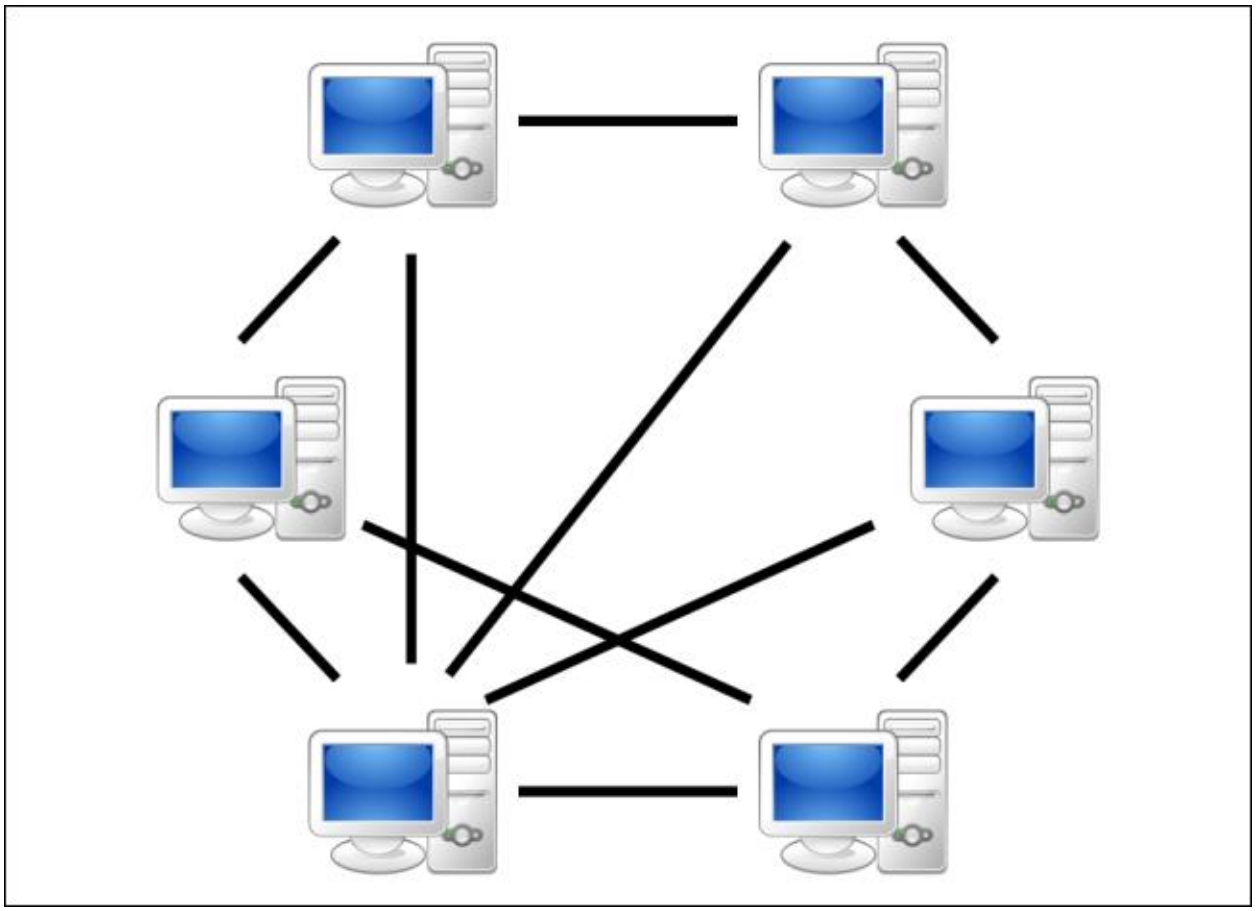
E. An Example of a Bit Torrent environment.

A bit torrent case is one involving the bit torrent large file downloading software. When you download a web page, your computer connects to the web server and downloads the data directly from that server. Each computer that downloads the data downloads it from the web page's central server. This is how much of the traffic on the web works.



But we know as each computer downloads a portion of the desired file stored on the central server, other computers are waiting for their turn to connect to the server and begin the download. Suppose, however, that other-later in time computers-could begin to download the desired file by downloading the file (or a part of the file) from one or more of the computers currently connected to the central server. Suppose, additionally, that the file on the central server were broken into hundreds of parts (called "seeds"), which were being both downloaded and shared at the same time. Under those conditions, downloading would look like this:

Wochna Law Firm
dwochna@wochnalawfirm.com



This is a bit-torrent download environment. The computers in the BitTorent environment are simultaneously downloading parts of the desire file and "serving" to other computers in the BitTorrent environment copies of the parts of the desired file that have already been downloaded. The group of computers in the environment is called a swarm, and each computer in the swarm is a "seed" because it downloads from other computers in the swarm while simultaneously "serving" seeds to other members of the swarm. BitTorrent is a peer-to-peer protocol, which means that the computers in a BitTorrent "swarm" (a group of computers downloading and uploading the same torrent) transfer data between each other without the need for a central server. This environment significantly increases download speed.

When the desired file was originally posted on the central server, downloading to a few members of the swarm took some time; but as each swarm member received part of the desired file, and shared that part with anyone else in swarm, the speed of download to all members of the swarm dramatically increased.

F. Special issues with child pornography. Some criminal defense attorneys may take possession of a client's cell phone or computer for various reasons. Great care should be taken, however, to avoid violation of federal child pornography statutes. Ohio Revised Code Sections 2907.321, 2907.322, and 2907.322 punish, inter alia, possession of child pornography. Each of these Code

Wochna Law Firm
dwochna@wochnalawfirm.com

Sections also contain an exemption to the application of these statutes if, inter alia, the offending materials are possessed for a bona fide judicial purpose. Many attorneys assume that the possession by a law firm of child pornography images resident on cell phones or computers owned by clients as part of a judicial process is exempt from prosecution under Ohio law. While this may be true, Ohio law does not preempt federal prohibitions related to the possession of child pornography contained in 18 USC Sections 2252 and 2252(A). Federal law does not contain any exemption whatsoever for the possession of child pornography. While possession of child pornography by a law firm may be exempt from prosecution under Ohio statutes, such possession constitutes a violation of federal law. Not only does possession of child pornography by a law firm risk federal prosecution; but such possession risks a civil suit brought by "persons aggrieved" to recover statutory damages of $150,000 per image possessed. See OUTLINE OF PRESENTATION: WHAT RISKS ARE ASSOCIATED WITH AN OHIO ATTORNEY TAKING POSSESSION OF DEVICES ON WHICH RESIDE IMAGES OF MINORS THAT VIOLATE OHIO REVISED CODE SECTION 2907?

ETHICS: WHAT RISKS ARE ASSOCIATED WITH AN OHIO ATTORNEY TAKING POSSESSION OF DEVICES ON WHICH RESIDE IMAGES OF MINORS THAT VIOLATE OHIO REVISED CODE SECTION 2907?

Conclusion: Ohio Revised Code Sections 2907.321, 2907.322, and 2907.322 punish, inter alia, possession of child pornography. Each of these Code Sections also contain an exemption to the application of these statutes if, inter alia, the offending materials are possessed for a bona fide judicial purpose. Many attorneys assume that the possession by a law firm of child pornography images resident on cell phones or computers owned by clients as part of a judicial process is exempt from prosecution under Ohio law. While this may be true, Ohio law does not preempt federal prohibitions related to the possession of child pornography contained in 18 USC Sections 2252 and 2252(A). Federal law does not contain any exemption whatsoever for the possession of child pornography. While possession of child pornography by a law firm may be exempt from prosecution under Ohio statutes, such possession constitutes a violation of federal law. Not only does possession of child pornography by a law firm risk federal prosecution; but such possession risks a civil suit brought by "persons aggrieved" to recover statutory damages of $150,000 per image possessed.

❖ Relevant Ohio Statutes ❖ Ohio Revised Code Sections 2907.321: Create, reproduce, publish, promote, advertise for sale, sell, deliver, disseminate, display, exhibit, present, rent, provide, offer or agree to sell, deliver, disseminate, display, exhibit, present, rent, or provide, buy, procure, possess, control obscene material with minor as participant

❖ ORC 2907.322: Create, record, photograph, film, develop, reproduce, publish, advertise for sale, dissemination, sell, distribute, transport, disseminate, Exhibit, or display, create direct, advertised for presentation, present, or participate in presenting, knowingly solicit, receive,

purchase, exchange, possess, or control any material that shows a minor participating or engaging in sexual activity, masturbation, or bestiality.

❖ ORC 2907.323: Photograph, direct, create, produce, transfer, possess, or view any material or performance that shows a minor who is not the person's child in a state of nudity

❖ Ohio Exclusion: Each Ohio statutory provision contains the following: ▪ [the statutory prohibitions do not apply if the] material or performance is sold, disseminated, displayed, possessed, controlled, brought or caused to be brought into this state, or presented for a bona fide artistic, medical, scientific, educational, religious, governmental, judicial, or other proper purpose, by or to a physician, psychologist, sociologist, scientist, teacher, person pursuing bona fide studies or research, librarian, member of the clergy, prosecutor, judge, or other person having a proper interest in the material or performance. ▪ Note: Proper Persons do not include by name, defense attorneys and defense experts, nor prosecutors and judges

❖ Ohio Exclusion Pragmatic Issues: ▪ Can a Prosecutor and/or Judge take CP evidence home? ▪ Can they review CP evidence in Chambers? ▪ Can Assistant Prosecutor possess CP images in his/her office? ▪ Can Defense attorney take possession of copies of the CP evidence? ▪ Transport the evidence in the car? ▪ Take it to the office/home ▪ View it ▪ Do we ask the Prosecution to mail us a copy of the evidence? ▪ Does the Prosecution print the CP images onto paper and give to defendant? ▪ Can defense counsel and defense expert share the CP contraband images? ▪ Can defense expert challenge prosecution by using demonstrative exhibits?

❖ Ohio CP Case: Ohio v Brady 2008 ▪ After passage of 18 USC 2256 ▪ Dean Boland attorney ▪ Dean Boland and Brady ▪ Boland argues: Brady cannot get fair trial because computer forensic expert cannot do his/her job without violating federal law ❖ Cannot research websites involved in case ❖ Cannot access with intent to view the contraband electronic evidence ❖ Cannot possess the evidence in preparation for trial ▪ Ohio Supreme Court did NOT discount expert's fears ▪ Did NOT hold that expert was insulated from federal law due to Ohio's exemptions ▪ Ohio Supreme Court held that defense expert could use protocols that complied with federal law (including federal criminal procedure that prohibits defense from having copy of contraband) ▪ Because it is possible for Brady's expert to examine and analyze the state's evidence at the prosecutor's office or another government facility, the trial court abused its discretion in determining, prior to trial, that the lack of an exception for expert witnesses in the federal child pornography laws deprived Brady of the assistance of an expert and further deprived him of the ability to receive a fair trial. Brady at paragraph 48.

▪ Ohio Supreme Court made it clear no violation of federal law is permitted when conducting a trial ▪ Brady's argument that he would like his expert to create exhibits for use at trial is also not well taken. It is axiomatic that an expert's conduct must conform to the law. If in preparing for trial, [Brady's expert] were to create images of real children engaging in sexually explicit conduct, or modify images of identifiable children to appear that they are engaging in sexually explicit conduct, his conduct would violate federal law ▪ This is no different from the practice of prohibiting experts in drug cases from manufacturing controlled substances or prohibiting

experts in counterfeiting cases from printing counterfeit money... ▪ While an expert may view and analyze the state's evidence and offer an opinion as to its content (i.e. whether it is what the state purports it to be), see Evid.R. 703, an expert may not violate the law when providing expert assistance to aid in the defense of a case.

❖ Brady and Safe Harbor: Is there anything left of Ohio's safe harbor? ▪ What about research, congressional hearings, presentations that show real CP for legislative reasons?

▪ Brady and Risk Management ❖ All forensic examinations of contraband must be performed using protocols that comply with federal law. ❖ Forensic examination of computer vs. image issues ❖ Computer Forensic examination is NOT image analysis ❖ Computer Forensic examination does NOT require viewing the images ❖ Forensic examination does NOT require possession of the contraband ❖ Therefore, forensic examination does not require a computer forensic expert to access an electronic file containing CP contraband for purposes of viewing the file

❖ Authentication of Image: Does an expert need to access a CP file to view its contents in order to authenticate the file? ❖ How do you authenticate the contents of a CP file? ❖ despite advances in technology, "`[j]uries are still capable of distinguishing between real and virtual images.'" Tooley, 114 Ohio St.3d 366, 2007-Ohio-3698, 872 N.E.2d 894, at ¶ 50, quoting United States v. Kimler (C.A.10, 2003), 335 F.3d 1132, 1142. ❖ new photographic and computer imaging technologies make it possible to produce by electronic, mechanical, or other means, visual depictions of what appear to be children engaging in sexually explicit conduct that are virtually indistinguishable to the unsuspecting viewer from untouched photographic images of actual children engaging in sexually explicit conduct.18 U.S.C. § 2251 (2000), Cong. Finding 5. ❖ R.C. 2907.322(B)(3), which states, "In a prosecution under this section, the trier of fact may infer that a person in the material or performance involved is a minor if the material or performance, through its title, text, visual representation, or otherwise, represents or depicts the person as a minor," is not overbroad but merely allows the state to prove its case with circumstantial evidence. Tooley at ¶ 2,

❖ The inference permits, but does not require, a fact-finder to infer the age of the person depicted in an image. Tooley at ¶ 35. Thus, it is still the state's burden to prove beyond a reasonable doubt that the images depict real children. Tooley at ¶ 35.

❖ Federal Law: 18 USC 2252 and 2252(A) prohibit knowing possession or knowingly accessing with intent to view ❖ Computer Forensic Exam does not require viewing ▪ were the image files ever opened ▪ are the images resident on the computer in an area from which they cannot be accessed or accessed only with specialized tools and knowledge (unallocated areas of drive) ▪ are the images in Internet Temp files? ▪ have the images been moved to personal folders

❖ State of Washington Case law related to copies of evidence ▪ The Washington state Supreme Court held that under the Washington State Superior Court criminal rules the state had a duty to provide the defense with copies of child pornography evidence that it intended to use at trial. ▪

Wochna Law Firm
dwochna@wochnalawfirm.com

State v. Grenning, 169 Wash.2d 47 (2010) ▪ State v. Boyd, 160 Wash.2d 424 (2007) ▪ State of Washinton ▪ The Washington state legislature enacted substitute House Bill 2177 effective July 2012. ▪ Patterned after the Adam Walsh act, the Washington statute requires child pornography evidence to remain in possession and control of the court or relevant law enforcement agency ▪ State of Washington ▪ The evidence must be made reasonably available for either party's examination. Where copies are necessary for a party's case, the burden shifts to the requesting party to make a "substantial showing" to the court ▪ State vs Federal ▪ It appears that state laws and case law are restricting the rights of criminal defendants, criminal defense experts to child photography evidence. ▪ What are the restrictions in federal law that are applicable to criminal defense experts and criminal defense attorneys?

❖ Federal Case Law ▪ It all started with the: Child Pornography Prevention Act of 1996. This Act prohibited any visual depiction including any photograph, film, video, picture, or computer or computer-generated image or picture that is or appears to be of a minor engaging in sexually explicit conduct.

▪ Also prohibited: Any sexually explicit image (even of adults?) advertised, promoted, presented, described, or distributed in such a manner that conveys the impression that the image is of a minor engaging in sexually explicit conduct

❖ CPPA was challenged by Adult Entertainment Trade Association: Free Speech Coalition ▪ Young-looking adults, Boxes, Titles of Films, description of films, "biographies of actors". Legal, adult portrayed by Title and description as if actor was 17?

❖ District Court, Northern District of California: CPPA is enforceable ❖ Ninth District Appellate Court: CPPA unconstitutional ▪ Appellate Court Analysis: ▪ Scope of Regulation of Images, Text, Film discussed by US Supreme Court in ❖ Miller v California ❖ New York v Ferber ▪ Miller v California ❖ Defines the limit of the First Amendment ❖ Text, film, video, etc.—Speech that affronts community standards can be made unlawful as obscenity ▪ New York v Ferber ❖ First Amendment Speech—even if not obscene under Miller—can nevertheless be made unlawful if the Speech is the result of the exploitation/harm to real children ▪ Appellate court reasoned that the CPPA unconstitutional because ❖ Does not require the "appears to be" or "conveys the impression" Speech to be obscene under Miller ❖ Does not require the Speech be created by harming real children ▪ Thus, where Speech contains images, text, film, video of non-people (i.e. virtual people), who "appear to be" or "convey the impression" that they are minors engaging in sexual activity, such speech is protected First Amendment Speech ▪ Government argued that ❖ Real and virtual images difficult—and in some cases impossible—for average person to differentiate ❖ [Computers/Technology gotten so good you can't believe your own eyes] ❖ [Remember this when we visit Ohio's case law] ▪ Due to the difficulty of differentiating real from virtual images ❖ Defendants will simply always claim the image is virtual ❖ Prosecution will always need to prove the image is "real" ❖ Victims may be required to appear and authenticate images of their abuse ❖ Constantly re-victimizing victims ▪ To avoid this result, the CPPA permitted a Defendant to raise a limited affirmative defense ❖ Show materials were produced using only adults ❖ Materials were not distributed as if material was CP ❖ Defense limited to

non-possession offenses under the CPPA ❖ Possession of these materials would not be given this affirmative defense

❖ Defense also not available if defendant avoided using people completely. If defendant simply generated computer image—no affirmative defense ❖ US Supreme Court held that the "appears to be" and "Conveys the impression" provisions of the CPPA were unconstitutional ▪ Reaction to opinion ▪ Reaction to Free Speech Coalition ❖ The National Center for Missing & Exploited Children ❖ Congressionally created nonprofit, private company ❖ Created by Children's Assistance Act of 1984 ❖ Decision will result in proliferation of child pornography ❖ Free Speech Coalition Court's analysis permitted the prohibition of virtual CP only where the CP Speech violated miller as obscene. ❖ Non-obscene, virtual CP Speech would be protected Speech ❖ Thus, the Obscenity standard in Miller became the limit of regulation of virtual CP Speech ❖ But Ferber seemed to be closer to the objective—protecting children ❖ Ferber recognized that the PROCESS by which CP Speech was created involved the victimization of children ❖ "Prevention of sexual exploitation and abuse of children constitutes a government objective of great importance" ❖ The government's interest in preventing sexual exploitation of children "trumped" First Amendment Including non-obscene CP Speech ❖ But real children—not virtual images—had to be exploited in the CP Speech ❖ Thus, Ferber reached all Speech created by sexually exploiting real children ❖ Ferber was not limited to just obscene Speech ❖ Under Ferber distribution of CP Speech (without regard to its obscene or non-obscene nature) can be prohibited ❖ The material depicting the minors leaves a permanent record of the exploitation and harm caused the child—which is exacerbated by distribution ❖ Thus "harm" under Ferber included actions taken by third parties (distributors) to distribute the CP Speech ❖ This will be an important concept when we see how the concept of "harm" has been expanded ❖ After Free Speech Coalition, Government was forced to rely on Miller and obscenity to bring "CP Speech and Virtual CP Speech" within scope of criminal statutes. But Ferber's objective to protect children seemed to present a better path to expand coverage of criminal laws. ❖ In Free Speech, for example, no one challenged the criminalization of "morphing" images of real children. Free Speech Court noted that morphed
images "implicate the interests of real children and are in that sense closer to the images in Ferber" ❖ Modify Federal Law ▪ If CP Speech that "appeared to be" of real children and/or was distributed in a manner to "convey the impression" that real children were involved is constitutional

▪ Can the law prohibit virtual CP Speech that is more closely linked to real children: i.e. indistinguishable? ❖ Congressional Hearings ▪ Technology makes it possible to create "visual depictions of what appear to be children engaging in sexually explicit conduct that are virtually indistinguishable to the unsuspecting viewer from untouched photographic images of actual children engaging in sexually explicit conduct" ▪ Congressional Hearings ▪ "virtually indistinguishable" ▪ versus "appears to be" and "conveys the impression" ▪ Technology successfully defeats your senses vs. descriptions, images that suggest? ❖ 18 USC 2256 ❖ "child pornography" means any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic,

mechanical, or other means, of sexually explicit conduct, where... ❖ 18 USC 2256 ❖ (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (real children) ❖ (B) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; (virtual CP-no child; but harm due to indistinguishable) ❖ (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct (morphing a real child) ❖ 18 USC 2256 ❖ "indistinguishable" means ▪ Virtually indistinguishable, in that the depiction is such that an ordinary person viewing the depiction would conclude that the depiction is of an actual minor engaged in sexually explicit conduct ❖ Expands Ferber's "protecting children from sexual exploitation" by prohibiting the "harm" that results from the viewing, distribution, of CP Speech that admittedly does not use real children—but that technologically cannot be distinguished from CP Speech created using real children ❖ Indistinguishable criteria takes advantage of the Findings of Congress that technology can render "virtual CP" indistinguishable from non-obscene, CP Speech that is unlawful under Ferber because it was created with real children ❖ Expands the Ferber protection rationale to virtual CP Speech ❖ Result of 18 USC 2256 ❖ If defendant uses technology—must do a bad job. If non-obscene virtual CP Speech is not distinguishable from real minors, it is violation of 18 USC 2256 ❖ If defendant uses people (adults)—then defendant has affirmative defense under 2256 ▪ Affirmative Defense ▪ Defendant may show that the alleged CP was ❖ Produced using an actual person ❖ Person was adult when the material was produced ❖ No actual minors used ▪ Ferber Protection Analysis Extended ▪ The Ferber Harm analysis allows criminal law to reach virtual CP (because it is indistinguishable to the viewer, even though no real children were used in its creation) ▪ What about hentai, lolicon, cartoon images, etc. Where the image is distinguishable—but obviously not a real child ▪ Ferber expanded ▪ Does the Ferber "harm" analysis expand criminal law to include distinguishable, non-obscene virtual CP? ▪ Simpson cartoons ▪ Second Life avatar

▪ Protecting Children Rationale ❖ Adam Walsh Child Protection and Safety Act of 2006 ▪ Hearings related to the "harm" visited upon child victims of sexual exploitation, including exploitation using computer technology (i.e. where no real children were used to create virtual CP) ❖ Federal Criminal Rule 16 ▪ In any criminal proceeding, any property or material that constitutes child pornography shall remain in the care, custody, and control of either the Government or the court. ▪ Why? Based upon Findings that the display of CP images—even by defense counsel—constitutes ongoing harm to victim ▪ 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, so long as the Government makes the property or material reasonably available to the defendant ▪ 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.

Wochna Law Firm
dwochna@wochnalawfirm.com

❖ Rule vs. Statute ▪ Criminal Rule 16, as amended, appears to permit defense counsel and experts to view CP evidence in the offices of law enforcement ▪ But accessing CP with intent to view is a direct violation of 18 USC 2252

❖ 18 USC 2252 and 2252(A) ▪ 2252 - Certain activities relating to material involving the sexual exploitation of minors punishes any person who: ❖ (B) knowingly possesses, or knowingly accesses with intent to view, 1 or more books, magazines, periodicals, films, video tapes, or other matter which contain any visual depiction ❖ that has been mailed, or has been shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, or which was produced using materials which have been mailed or so shipped or transported, by any means including by computer, if— ❖ (i) the producing of such visual depiction involves the use of a minor engaging in ❖ sexually explicit conduct; and (ii) such visual depiction is of such conduct;

❖ 18 USC § 2252A - Certain activities relating to material constituting or containing child pornography— punishes any person who, inter alia: ❖ (B)knowingly possesses, or knowingly accesses with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography ❖ that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. ❖ 18 USC Section 2252 and Section 2252(A) ❖ Federal Statutes-Result ❖ Criminal Defense attorneys and experts in federal cases ▪ Must perform all analysis at offices of law enforcement ▪ Must leave all evidence with offices of law enforcement NOTE this section of the Adam Walsh Act (18 USC 3509(m)) changed the Federal Rules of Criminal Procedure ❖ Adam Walsh Act ❖ The Federal Rules of Criminal Procedure cannot create a substantive right that is prohibited or denied by legislation

❖ So, can defense counsel access known CP files with intent to view them? ❖ Ohio CP Case ❖ Can defense expert create an example of virtual CP Speech by creating a computer – generated image that “appears to be” a real child ❖ What if the image is “indistinguishable” ❖ Does this type of exhibit violate federal law? ❖ Ohio CP case ❖ is a trial a proper interest under the Ohio Exemption? ❖ Although the exemption includes prosecutor and judge—does it include defense attorneys and experts? Boland v Eric Holder: Boland attempts to save Ohio’s exemptions by seeking a declaratory judgment from federal court that federal law does NOT preempt Ohio ORC 2907.322 ❖ Ohio District Court, Northern District ▪ [Citing the language of Ohio’s Statutory Exceptions]. In other words, under Ohio law, a lawyer can review and/or create child pornographic materials anywhere, provided it is done strictly in the course of or related to a judicial proceeding ▪ Court contrasts Ohio statutes with federal: ▪ Federal statutes, 18 U.S.C. Section 2252 and 18 U.S.C. Section 2252A, criminalize certain activities relating to material involving the sexual exploitation of minors and certain activities relating to material constituting or containing child pornography, respectively. ▪ [Boland] in this case has not relied, and cannot rely, on the state exception and comply with the federal law, and thus there is a conflict

between these sections of the respective child pornography statutes. ▪ But [Boland's] contention that state law somehow shields him from federal prosecution is contrary to both the Supremacy Clause of Article VI and a long history of Supreme Court case law, noted supra. Unless federal law states otherwise, state law cannot empower a citizen to act contrary to a federal prohibition. ▪ Therefore if [Boland] were to violate 18 USC Section 2252 and/or 18 USC Section 2252A, while participating in a judicial proceeding, he would not be immune from federal prosecution by virtue of Ohio's exemption for activities conducted by lawyers.

❖ Boland Background ▪ Why is Boland leading this fight? ▪ Boland is an attorney and a computer image expert who was retained in several cases in which he created demonstrative exhibits by morphing the images of identifiable minors to make it appear that they were engaged in sexual activity ▪ Boland Background ▪ Boland was investigated for his conduct as a defense attorney/expert and entered into a Deferred Prosecution Agreement

• He admitted that he had violated federal law • Stated he thought Ohio law provided him a safe harbor • Promised not to violate federal law ▪ Boland Background ▪ As part of his duties as attorney/expert Boland • Created exhibits that were either virtually indistinguishable or morphed real children • Possessed those exhibits in his home and office during trial and prep • Displayed those exhibits at trial • Provided copies of those exhibits to trial counsel, court ▪ Boland v Eric Holder ▪ [Boland's] use of prohibited materials in his home and/or office, albeit for a strictly judicial purpose, violates federal law. ▪ Observation: Northern District Court recognized that the language of ORC would permit Boland's conduct—but not federal law. ▪ Risk Management ▪ Treat all protocols in Ohio CP cases ❖ The Real Threat—Private Action ▪ 18 USC 2252 and 2252 (A) contain provisions allowing for a private cause of action ▪ 18 USC 2252(A) • Any person aggrieved by reason of the conduct prohibited under [18 USC section 2252(A)] ... may commence a civil action for the relief set forth in paragraph (2). • (2) Relief. —in any action commenced in accordance with paragraph (1), the court may award appropriate relief, including— ❖ (A) temporary, preliminary, or permanent injunctive relief; ❖ (B) compensatory and punitive damages; and ❖ (C) the costs of the civil action and reasonable fees for attorneys and expert witnesses ▪ 18 USC 2252 and 2252(A) contain the following: ▪ Any person who, while a minor, was a victim of a violation of section 2241 (c), 2242, 2243, 2251, 2251A, 2252, 2252A, 2260, 2421, 2422, or 2423 of this title and who suffers personal injury as a result of such violation, regardless of whether the injury occurred while such person was a minor, may sue in any appropriate United States District Court...and shall recover the actual damages such person sustains and the cost of the suit, including a reasonable attorney's fee....Any person as described in the preceding sentence shall be deemed to have sustained damages of no less than $150,000 in value. Doe v Dean Boland

❖ After Dean created and used the demonstrative exhibits morphing two identifiable children, FBI contacted parents of children, who sued Boland in federal court, Northern District, Ohio ▪ Plaintiffs relied upon Deferred Prosecution Agreement as admission that 18 USC 2252(A) and 2255 had been violated ▪ Boland argued to District Court that these statutes were never intended to apply to expert witnesses; and that Ohio's exemption statute created issues of liability ▪ Also, that the threat of private lawsuit related to manner in which exhibits were prepared and used would affect availability of counsel ▪ Court Granted Boland Summary

Judgment ▪ to read the federal statutes as permitting liability under the instant facts would implicate a criminal defendant's Sixth Amendment right to counsel; was unfair given that Boland was responding to a federal court directive when he created and possessed the morphed images in Oklahoma; and would create serious comity issues since Ohio provided statutory immunity from state child pornography prosecution for expert witnesses.

❖ 6th Circuit, Doe v Boland: Appellate Court Reversed and Remanded: ▪ Congress had no express or implied exceptions for expert witnesses in these circumstances, and that no common-law exemptions apply in this setting ▪ October 20, 2011 ▪ (no witness immunity) ▪ although the statutory private civil causes of action remedies applied to Dean Boland as a testifying expert, the issue remained for remand to the trial court whether the Plaintiff minor children had suffered any damages ▪ Observations on 6th Circuit • Absolutely clear that the Private Causes of Action on behalf of "persons aggrieved" and "victims" of the violation of federal CP laws include defense attorneys and experts in Ohio cases ▪ What about prosecutors and judges if exemption statute offers no insulation?

❖ On Remand back to District Court, Northern District Ohio: ▪ District Court noted that plaintiffs had stipulated they had suffered no damages: neither the minor children nor the parents had ever seen any of the exhibits created by Boland; and the minor children were unaware of the action brought by their parents for damages pursuant to 18 USC 2252(A) and 18 USC 2255 ▪ Plaintiff's counsel argued that under the statute, damages included harm suffered but not yet realized • "Suffers personal injury as a result of such violation, regardless of whether the injury occurred while such person was a minor" ▪ Court Decision

• The Court agrees that the minor Plaintiffs are "aggrieved" and that they have suffered "personal injury." • First there is nothing in either statute [18 USC 2252(A) and 18 USC 2255] that says a victim needs to have seen the offending images, or to have been present when the images were made or shown, in order to be aggrieved or suffer personal injury. • It can be of little consolation to the minors or their parents that these pictures were displayed only to judges, juries, and various court related personnel. • With regard to Section 2255, there is nothing in the statute to suggest that the minors need to know about the images in order to suffer a personal injury. The harm has already occurred….It is probable that Congress provided for the large statutory damages of $150,000 just so that it would not be necessary to have a trial requiring the images be shown and the victims to testify about the psychological trauma they have suffered... • Court awarded summary judgment in favor of Plaintiffs in the amount of $300,000 • $150,000 per image ▪ Observation: Damages are statutory

❖ Sixth Circuit Appellate Decision. Decided November 9, 2012 ❖ Affirmed the District Court's granting of summary judgment to the parents of the children whose images were used by Dean Bolan to create demonstrative exhibits under federal court order in Oklahoma. ▪ Appellate court noted that Dean Bolan entered a pretrial diversion agreement with United States attorney's office for the Northern District of Ohio in which he admitted violating 18 USC section 2252A. ▪ Specifically, Bolan admitted to knowingly possessing a visual depiction that had been created adapted or modified to appear to be an identifiable minor engaged in sexually explicit conduct" in contravention of 18 USC 2256(8)(C) ▪ The FBI located the parents of the children whose

images Boland had used; and in September 2007, the parents filed a civil lawsuit against Bolan pursuant to the private remedies provided in 18 USC sections 2252A and section 2255. ▪ Section 2250 2A provides a civil remedy to “any person aggrieved" by child photography, while section 2255 provides a civil remedy of at least $150,000 in damages to minor victims who suffer a personal injury from various sex crimes ▪ The District Court granted summary judgment to Bowland on the ground that these two civil remedy statutes exempt expert witnesses from liability. We reversed, holding that the laws contained no such exemptions or any other exemption that would cover Boland.

▪ The issue on appeal is: 1) did the plaintiffs meet the requirements for obtaining relief under section 2255; 2) does the definition of morphed images as child photography in section 2256 violate the First Amendment; and 3) does the district court's award violate the sixth amendment's right to counsel ▪ The appellate court noted that Bolan admitted to violating section 2252A when he morphed the plaintiff's images into pornography. The only unresolved issue, therefore, was whether the plaintiff suffered a resulting personal injury that qualified them to the relief afforded by section 2255 • The appellate court held that the plaintiff children suffered personal injuries even though they had stipulated that neither the children nor the parents had seen the offending images; that the children had suffered no financial, emotional, physical, psychological, or other injuries. • The appellate court reasoned that, like a defamatory statement, child pornography injures a child's reputational and emotional well-being. Child pornography violates the individual interest in avoiding disclosure of personal matters. • If the point of Boland's exercise was to demonstrate that the naked eye cannot distinguish morphed images of child pornography from real child pornography, as he claims it was, that goes a long way toward confirming that morphed images may create many of the same reputational, emotional, and privacy injuries as actual pornography • The appellate court carefully parsed section 2255, especially the clause stating that the minor must be both a victim and suffer personal injury • Section 2255 requires that a person be a minor when she is the victim of a sex crime but allows that person to recover when she incurs an injury, regardless of whether the injury occurred while such person was a minor. • But victimhood and injury need not occur simultaneously. A child abused through pornographic video might have one section 2255 claim against the videos create tour as soon as it is produced and another against the distributor or who sells a copy of the video 20 years later. • Cast in this light, the statute separate references to victim and personal-injury show only that minor victims may sue for injuries they incur later in life. • The appellate court held that the statutory structure of section 2255, referring to both victim and suffering personal-injury, was merely two ways of saying the same thing to reinforce its meaning.

• Additionally, the appellate court held that the plaintiff children are real children with legally protected interests in their reputations. By sharing the morphed images with defense counsel and court staff and displaying the images in the courtroom, Boland invaded those interests • And unlike plaintiffs whose only injury is the violation of a statutory right, (citations omitted), Boland's display of the morphed images in court harmed the plaintiff children. ▪ The court next analyzed Bolan's argument that the victim children had sustained no “actual damages" • Most tort plaintiffs, it is true, must show the amount of the damages. But section 2255 is no ordinary cause of action. The statute declares that any victim shall be deemed to have sustained

damages of no less than $150,000 in value. • Bolan argued that the victims ought to be required to prove some amount of damages first in order to qualify under the statute. • In rejecting that argument, the appellate court stated: • The point of a minimum damages requirement is to allow victims of child pornography to recover without having to endure potentially damaging damages hearings • Once a child has shown she was the victim of a sex crime, there is little point in forcing her to prove an amount of damages, only to have the court disregard that figure and award the statutory minimum. The District Court did not err in awarding the plaintiff children the minimum statutory amount without proof of “actual damages". ▪ The appellate court also rejected Boland’s argument that the application of the damage provisions of section 2255 to him, as an expert witness, ran afoul of the First Amendment. • The “evil" of child pornography “so overwhelmingly outweighs the expressive interests, if any, at stake" in this form of communication that it lies categorically beyond constitutional protection, meaning that “no process of case-by-case adjudication is required" to uphold restrictions on it. • In focusing upon the First Amendment argument, the appellate court noted that Boland’s conduct violated provisions of the child pornography statutes that had survived challenge in the Ashcroft case. • Morphed child pornography is indistinguishable from actual pornography, which itself has exceedingly modest, if not de-minimis first amendment value. And unlike pornography that appears to depict children, morphed images are never necessary to achieve an artistic goal.

• Virtual children or actual adults create the same visual effect as a morphed image yet do no harm to the interests of identifiable minors. ▪ Finally, the appellate court addressed the stipulation that the minor children were completely unaware of the existence of the demonstrative exhibits that Bolan had created, only to be used within the four corners of the courthouse.

• Even if the plaintiff children never see the images, the specter of pornographic images will cause them continuing harm by haunting them in years to come. • As a result, it is immaterial Boland never displayed these images outside of a courtroom and never transmitted them electronically. The creation and initial publication of the images itself harmed the plaintiff children, and that is enough to remove Boland’s actions from the protections of the First Amendment.

▪ Finally, the appellate court addressed Boland's intention and alternative means of accomplishing similar results. • This $300,000 reward undoubtedly amounts to tough medicine for Boland. When he created morphed images, he intended to help criminal defendants, not harm innocent children. Yet his actions did harm children, and Congress has shown that it “means business" in addressing this problem by creating sizable damage awards for victims of this conduct.

• Nor was this Boland's only option for trying to help his clients. He could've shown the difficulty of distinguishing real pornography from virtual images by transforming the face of an adult onto another or inserting a child's image into an innocent scene. • If he felt compelled to make his point with pornography, he could've used images of adults or virtual children.

Wochna Law Firm
dwochna@wochnalawfirm.com

❖ Application to attorneys that take possession of devices, such as cell phones and/or computers, known to contain images that violate (or arguably violate) federal child pornography statutes. ▪ In the absence of any federal investigation, possessing these devices sets the stage for the following scenario: • Parents of the minor whose image resides upon a client's cell phone sue the minor and the attorney as "aggrieved parties" pursuant to 18 USC 2255 seeking $150,000 per image. • As part of the civil suit, plaintiff-parents would be required to aver that the defendant client and attorney violated one or more federal child pornography statutes. This would potentially require a "trial within a trial" in federal court; and would undoubtedly result in bringing attention to federal law enforcement.

• Based upon the actions taken in the Boland matter, it appears certain that federal law enforcement would investigate and potentially indict (or defer prosecution) of the attorneys and client. • In any case, once the predicate violation of a federal child pornography statute was established, civil damage award of $150,000 per image appears to be mandatory under the Boland analysis above.

---

[i] "FL Hospital uses RFID to monitor employee hand washing", RFID News, August 3, 2009 available at www.rfidnews.org/2009/08/03/fl-hospital-uses-rfid-to-monitor-employee-hand-washing

[ii] See Preservation in Chapter

[iii] Best Buy Stores, L.P. v. Developers Diversified Realty, Case No.; 05-2310, D. Minn. Nov. 29, 2007

[iv] "Data theft Common by Departing Employees", Brian Krebs, The Washington Post, February 26, 2009.

[v] A server is simply another computer that contains information that is "served" to other computers that are usually termed "clients".

[vi] http://www.pcworld.idg.com.au/index.php/id;1002274598, "Dutch Track Counterfeits via Printer Serial Numbers"

[vii] See, for example, The Ohio State University, "RFID Hospital Patient Tracking" as part of the Patient Tracking Netwiser Project, Fall 2008 available at https://ceti.cse.ohio-state.edu/ceti/showcase/bitwiser