

Module 10: Collection of Electronically Stored Information

Learning Outcomes

Upon completion of Module 10, students will be able to:

- Assess how to collect data generated by email systems, including the databases, attachments and the metadata related to it.
- Identify the challenges with collecting hidden data or data where access is restricted and some of the methods for obtaining this data.
- Evaluate the issues with collecting encrypted data.
- Support whether access to deleted or corrupted data is possible and even desirable.
- Interpret the issues with trying to collect data from proprietary systems and obsolete media.
- Compare and contrast the meaning of the terms privileged, sensitive and not reasonably accessible and recommend what the producing party's lawyer should do to protect this information.
- Prove the ownership, integrity and authenticity of data that has been collected as part of an e-discovery process.
- Defend the importance of time and date information as an essential facet of electronic evidence.
- Examine some of the primary activities in acquiring data in a forensically sound manner.
- Summarize the important points in Module 10 and the reading assignment.

Please read Chapter 5 in *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed.

Please also read the following items, which are included as part of Module 10 in Canvas.

- Google Records Your Voice Texting – and Much More – from *The Indiana Lawyer*
- Emojis Head to a Courthouse Near You – from *ABA Journal*
- Face Time: Facial Recognition Technology Helps Nab Criminals – and Raises Privacy Concerns – from *ABA Journal*
- City Attorney Who Falsified Email Suspended for 180 Days – from *The Indiana Lawyer*. Note that email continues to be a rich repository for potentially relevant evidence and that tampering with it can easily be detected and will have dire consequences, particularly

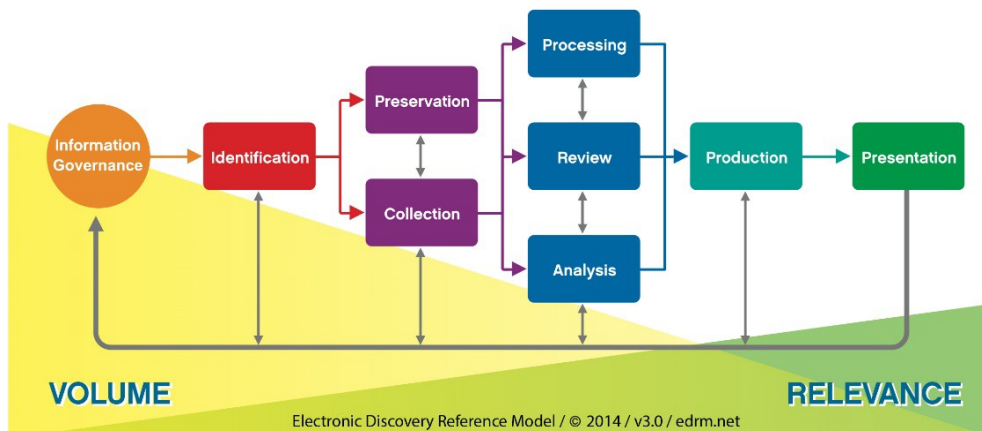
when someone should have known better than to try. According to case law, in Indiana, if a lawyer is suspended or disbarred, he/she is not allowed to work in a law firm in any capacity.

- *Mobile Device Collection – More than Just a Phone* – PowerPoint slides from a webinar from the International Legal Technology Association (ILTA)

Please read the following mini-lecture.

With Module 10, we begin to examine the individual steps in an electronic discovery process. It is helpful to visualize this process using the EDRM, which we were introduced to earlier in the semester. Recall that Module 9 was devoted to information governance/litigation readiness, which should help us prepare for the collection step in an e-discovery process. Note as well that by this step in the e-discovery process, the volume of electronic evidence that we might have to handle has been reduced, but the relevance of that evidence has increased.

Electronic Discovery Reference Model



Our reading assignment, Chapter 5 in *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed., covers the procedures for recovering and acquiring electronic evidence as well as the difficulty in locating some of this evidence. The author discusses how to handle situations where a party claims that data is privileged, sensitive or not reasonably accessible. One important facet of the chapter will be procedures for gathering electronic data in a forensically sound manner to assure the court that no alterations were made to the data and that the integrity of the data has been maintained in its pristine and original state.

The first section of Chapter 5 asks the question: where is our data hiding? Recall that Chapter 3 provided detailed information on various types of electronic data and how it is created and stored. It is important to note that computers and other digital devices can and do lose data sometimes or store it in ways that are inaccessible to normal users. In many cases, data can be stored in ways that can only be accessed, manipulated or recovered using a specific front-end application or interface.

The author devotes several pages of Chapter 5 to how applications function as a vital interface, with email as his first example. This is especially appropriate, since he notes on page 178 that email is the most popular electronic evidence in most court cases. Recall that nearly all email applications that reside on a computer have some kind of database behind them that is

responsible for storing and organizing everything that is received or input, along with its corresponding metadata and any attachments such as images and documents. Any actions taken with the email message, such as opening it, moving it to a folder or saving its attachments, means new attributes will be added to the data in the back-end database. Other activities you might use an email system for, such as contacts information, calendar items and task lists, will be stored in the database. As the author observes on page 180, in many cases, these databases are based on proprietary programming. This means that the organization that created the email application and its back-end database chose to use a database programming language that can only be read by that application – and thus the only way to locate the database and access the information stored in it is to use the email application from which it was created. This becomes problematic because an application can fail, go out of date or be accidentally deleted.

To illustrate this problem, the author shares his own story about why his parents could no longer access anything on their computer, even though everything still existed on the hard drive. Fortunately, there are several solutions if the front-end application for an email system goes awry, which the author describes on pages 182-183, including the availability of PST files in Microsoft Outlook. As he notes on page 182, there are other programs that allow a user to access and open a PST file to search for email, calendar, contacts or task items. Other applications might have a SQL, Oracle or other database system backing them up, especially if this is an Internet-based application. The author assures us that if this is the case, there are many tools and applications available that will allow you to open and query those databases for relevant evidence. Since we may not have the expertise and experience to use these tools most efficiently, the author advises us that we probably will want to consult a digital forensics expert (and probably not the kid across the street). ☺

The next section of Chapter 5 is especially interesting, since it deals with data that is hidden or where access to it is restricted. As the author observes on page 183, “[a]nother place that important information can be stored is in log files or data files that your computer’s operating system might hide from view.” These types of files and folders are called “hidden” or “system” files and most operating systems have special storage space that is inaccessible to users unless they have the correct privileges on the device. For example, there are several different types of files on Windows devices which are hidden from normal view, including files that contain data for the registry. As the author describes on page 183, the registry is a very complex and technical database of connections (hardware, software, applications, etc.) that is the heart and soul of how your computer and its applications interact with the Windows operating system. A long list of data that can be found in the registry is provided on page 184. Other hidden files may contain information about your Internet browsing, including history, cookies and files you access on the Internet or on a network. These will not be files that you can simply find and open on your own and yet they can contain potentially relevant electronic evidence. The Recent folder in the Windows operating system contains data on all of the files you accessed in a given period of time. Other hidden files and folders have information on all of the applications you installed and any error messages or logs that were created by those applications, while others store data on security alerts or systems issues.

The \$MFT (master file table) in Windows computers is a flat database created the first time your computer starts and keeps track of every single file created on your computer as well as modifications, last access times, deletions, archiving or anything else that the operating system needs to track about those files. Note that as a computer forensics expert, the author uses the \$MFT file on a regular basis to understand when a computer was infected with malware and the

type of malware. Another type of hidden file that can be of great value in understanding a computer user's actions is the Restore file, available on some Windows operating systems. If someone was purposely trying to hide his or her actions by deleting applications, Internet browsing activities or the documents that he/she created, the Restore file gives the digital forensics expert a way to go back into the past to see how things looked before. Log files track how applications are being used and any problems with them, usually accessible by knowing the advanced options in the application that allow you to view and manage those files. Other operating systems, such as Linux and Mac, have system files that are not generally available to a regular user. If you want to see some of these files – or at least their folders and file names – you can select “show hidden and system files” in your folder settings on a Windows computer. However, note that they are encoded in such a way as to only be accessible and readable either by an application interface or by the system. As the author advocates on page 188, in understanding where data live, we should not neglect this rich source of information. In many cases, it will contain some of the most important facts and clues to understand what really happened on a computer, when it happened and who might be responsible.

Encrypted data presents another challenge in an e-discovery process, which can make data difficult or even impossible to access (see Figure 5.3). As the author notes on page 188, there are many ways to encrypt data on a computer, from the simple act of assigning a password to a file to the complex process of managing digital certificates that automatically encrypt data in emails, specific folders or entire hard drives. Windows systems may include BitLocker as a tool. As the author observes on page 189, if we need to access data from a device, drive, folder, email or file that is encrypted, the most likely solution is to find out what the authentication mechanism is and learn the passphrase or password. It is best to go through the proper channels to obtain the authentication information. However, there are some readily available tools that allow you to crack or bypass the passwords to files that have been protected through relatively simple encryption. More sophisticated tools may allow an expert to break through more complex encryption schemes, but this is not always possible, which can pose a challenge if we believe that the encrypted information is something that is relevant to a case.

Deleted or corrupted data is covered in the next section of Chapter 5 of *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. Data can be deleted or corrupted for a number of reasons, but the good news is that often a large portion of the data is still intact and available if someone has the skills and tools to find it. The author describes how he is able to accomplish this on page 191. In computer forensics terms, this is called data carving, wherein the tool looks through the lines of data stored on the medium we are searching through and carves out the pieces that make up different file types using a variety of information gleaned from the metadata. As the author observes on page 191, in addition to whether to request deleted, corrupt or lost data as part of an e-discovery process, we want to remember what data might still be there and to do our best to preserve it by not continuing to use a device, which would risk the remaining data to be overwritten or further corrupted.

The author provides some real-life examples of the difficulties when data is stored in a format or on hardware that is no longer available (which to me also argues for a document retention and destruction policy that either moves this data to a current storage method before the format or hardware becomes obsolete or is destroyed in a timely manner when no longer necessary to keep it). The author provides a list of different types of media on pages 192-193. He goes on to illuminate the challenges with floppy disks and certain kinds of drives. An online

search may reveal a vendor who will have the proper hardware or who can provide access to the data. If not, then a reputable and experienced digital forensics expert may be able to assist you. Another way that data can be made inaccessible is if it was created in a proprietary format, such as WordPerfect and Lotus 123. The author describes what the options would be for a 15- year-old document created using an older version of WordPerfect, stored on 5¼-inch floppy disks. A digital forensics expert might be able to gather enough of the raw text in a text-based document, even without the correct software, but photographs, graphics or formulas may be impossible to access. As the author observes on page 196, data stored on obsolete or rare media or stored by an application that uses proprietary code may be considered unreasonably accessible. We need to consider the resources and time that we would need to expend if we attempt to acquire, restore or produce this type of data.

Pages 196-203 are devoted to how to manage privileged, sensitive and inaccessible data. As indicated on page 196, if we want to assert that evidence should not be provided for a case because of privilege, we need to demonstrate this. The author provides the legal definition of privileged information on pages 196-197. Note that this may also be known as attorney-client privilege. Recall that under the 2015 amendments to the Federal Rules of Civil Procedure, objections must be made with “specificity” – in other words, no “boilerplate” objections. There are protections in place for communications between spouses as well as between physician-patient and minister-parishioner. As the author explains on page 197, in order to assert privilege, the lawyer must document all of these types of communications in a privilege log and note in all correspondence that the information contained therein is privileged. (On the other hand, marking 95% of documents as “highly confidential” will not protect them.) Note as well that privilege can be waived if data are inadvertently produced through carelessness in an e-discovery process as well as if a party has communicated with the lawyer using an employer-provided email system.

There is another privilege known as attorney work-product, wherein information that might indicate a lawyer’s strategy for a case can be protected (the rationale being that we want the lawyers for all parties in a case to prepare their own robust strategies), defined on page 214. Note that the attorney work-product doctrine extends to others who are working on the case on behalf of the lawyer, including digital forensics experts. This doctrine only extends to those who are working as an agent of the lawyer. Precautions must be taken to protect the information and to keep it from being inadvertently produced to the opposing party.

As the author indicates on page 200, “[w]hether information is considered confidential, sensitive, or public only matters if someone is maintaining some type of classification of that data.” In addition to information that can be protected as privileged, personally identifiable health and financial information might be considered confidential and private in the U.S. and certainly in Europe. The author advocates that we find out what the privacy laws are in our jurisdiction (and states are allowed to have stricter privacy laws than what federal law says) and manage our confidential information to avoid having it exposed. Certainly, we have this obligation as owners, managers or even employees of companies, non-profit organizations, government agencies, etc. The author asserts that everyone should have practices in place to ensure that health, financial and personal information is held in a safe and secure method and that we are using good security practices, including strong passwords and authentication procedures, encryption, good monitoring and incident response and security-minded development of new applications. Other sensitive information could relate to our nation’s critical infrastructure.

As stated on pages 201-202, “[i]f such information was requested or required for a court case or an audit or other reasons, it would be the responsibility of the producing party to justify its refusal to produce that information by proving the data’s classification is based on real and justifiable concerns.” However, the court might rule that the data have to be produced or perhaps a subset of it as a sample that would show whether there was indeed relevant electronic evidence in the materials overall (recall the *Zubulake* case). The author reminds us that another issue with our request might be a debate over whether the data was not reasonably accessible, with the court able to shift some of the costs of obtaining this data. Of course, a party will not be able to avoid producing data that is rendered not reasonably accessible because of the party’s poor records management practices (yet another reason for all entities to have an information governance/litigation readiness plan that includes a retention and destruction policy). The court may require an accessibility log that documents why certain data is being claimed as inaccessible and can also order cost shifting to reconstitute inaccessible data.

The author devotes a significant number of pages in Chapter 5 to how we prove ownership and integrity of electronic evidence. Questions may be raised because of what is known as plausible deniability. As the author asserts on page 203, “[c]reating and managing data in a way that maintains its integrity, documents its access, and monitors any changes allows a party to ensure nonrepudiation.” On the other hand, it can be relatively easy, either intentionally or by mistake, to corrupt the integrity of a document. Thus, the author discusses the steps that can be taken to ensure the integrity of data, reducing the opportunity for someone to claim plausible deniability and maximizing nonrepudiation. The metadata that is generated when a digital record is created is very important to integrity and ownership as is data that might be collected by an operating system or stored in some type of log or MFT. The author provides an example of how this works in the real world – a plaintiff alleges that a defendant has taken patent information. Note that the defendant company used an invention assignment agreement, but that management agreed to exempt the plaintiff’s invention from this agreement. As the author observes on pages 205-206, the revolution caused by electronic evidence can actually level the playing field in litigation, with both sides having an equally good chance of prevailing if they can prove or disprove the integrity of the evidence (in this example, email and electronic documents). The author relates how careful analysis by the digital forensics team revealed some anomalies from the manager’s normal daily computer use. As the story continues, a deposition of the defendant’s IT manager illuminated some crucial information – management had asked him to set the computer time clock back on the manager’s computer, thereby falsifying the dates on which the emails about the invention assignment agreement were actually sent.

As indicated on page 207, the question of “who” created or accessed a file may be more difficult to prove, especially when more than one person uses a computer or other electronic device. The author notes that the assertion that a virus was responsible can be easily refuted because the computer or device would show actual evidence of a virus. The metadata can also indicate ownership, although this is difficult to prove unless an actual camera showed the person sitting there (which the university has implemented for online exams ☺). Other methods to prove ownership and access include timelines, with an example on page 208, as well as establishing that a piece of electronic evidence was not tampered with. Processes, tools and protocols have to be followed carefully to ensure that the evidence for trial was not changed in any way. One of these tools is known as hashing, described on pages 209-210 (see Figure 5.5). As the author indicates, hash values have a number of uses in an e-discovery process. The author discusses a common practice, which is to copy a set of emails from a computer into a

Word document (although there are reasons why this will probably not be acceptable to the court, nor will it comply with the opposing party's request for files in native format with the metadata intact).

The author concludes this section of Chapter 5 by stating that “[e]stablishing and maintaining the ownership and integrity of electronic evidence can be paramount in any type of case.” The entity should create policies and procedures in order to ensure that it has the means to prove the integrity of its documents, including careful records management and documentation, log management and good practices around the handling of potentially relevant electronic evidence such as litigation holds.

As indicated on page 211, the time and date information included in or about an important piece of electronic data can often be at the heart of establishing what happened, when and to whom (see Figure 5.6). As the author describes on pages 212-213, tracking time is done in different ways by different operating systems. As he notes on page 213, the reason to understand time standards and time zones is because most computers will record creation, access and modification times that occur on them in UTC (Universal Coordinated Time). You may need to translate between UTC and the time zone in which the activity took place, including the location and date. He provides an example of a case where we are asked to identify exactly when a document was created and last saved. (Note that Indiana does observe daylight savings time – and be sure to “fall back” for Sunday, November 5!) As he asserts on page 214, it is imperative that some type of auditing or other means of verification of the accuracy and integrity of the time be established and this can be done by gathering corroborating evidence such as other devices or documentation. (Recall the example of the patent case on pages 204-207, wherein the computer's clock was adjusted to make it look like email had been sent on a different date).

The final section in Chapter 5 of *Electronically Stored Information: The Complete Guide to Management, Understanding, Acquisition, Storage, Search, and Retrieval*, 2nd ed. concerns legal and forensically sound acquisition of electronic evidence. As the author asserts on page 215, “[n]o matter what the reason for gathering that data, doing so in a forensically sound manner is a good practice as it will ensure that the data you produce can be proven to be the same data as you started with and have not been manipulated or changed in any way from the original.” The first priority is to maintain the information in its original state – and be able to prove it. Good records management policies, but most importantly, good practices that you can document that your organization actually follows, are going to be key. The author provides an excellent discussion of records management, which complements what we learned in Module 9 about information governance/litigation readiness.

- A records management policy should include classification of data. This will encompass understanding the types of data that you produce and the legal and archival ramifications for each type of data. For example, there may be laws, regulations, best practices and industry norms that apply to certain types of information, such as contracts, employee matters, taxes, etc.
- Create written policies that are available to all employees that explain any laws or regulatory obligations for maintaining, storing or preserving each type of data. It is advisable to have employees sign a copy of all policies.
- Regularly audit employees to be sure that records retention and destruction policies are being followed according to the procedures put in place. (You might be surprised to

learn that many employees will circumvent these policies, perhaps by saving documents, files and emails on their own systems, in PST files or emailing things to themselves via a personal email account.)

- Note any other data, such as email, intellectual property or log information from the network or a specific application, which should be managed carefully. (Note that the author also advises individuals to do this as well – that we all should make good choices about how our data are preserved, organized and maintained so it will be available when needed.)
- If records management policies and practices need to be developed, gather a group of stakeholders such as top-level management, auditors, legal counsel, IT managers and staff as well as third-party vendors.
- Provide regular and ongoing training about document retention and destruction policies for everyone in the organization who will have access to particular types of data and records.

The author notes on page 217 that “[g]ood records management practices are the most important foundation for ensuring the integrity and availability of records.”

The next step is to acquire the data in a forensically sound manner. The author describes the use of a hash value for the information that will be preserved as well as the creation of an image or snapshot of a set of data. Some operating systems will provide a verified copy, which is usually done from the command line. The author highlights the features in Windows, Linux and UNIX that make this possible. To preserve larger volumes of data, such as entire hard drives, the digital forensics expert will use forensic imaging tools that include a write blocker. A byte-by-byte copy of the hard drive is often called a mirror image, although the author is not entirely satisfied with this term. Because these may be very large files, the forensics imaging application may divide them to be stored on DVDs or CDs or may compress the empty sections of a hard drive. If you prefer using command lines to create your image, the dd command is available in both Windows and UNIX operating systems. As the author indicates on page 220, “[n]o matter what method you choose to create and preserve the forensically sound copies of data, the important thing to understand is the necessity to ensure the integrity of the data so that you can prove the data are the same thing after being copied as they were before.” One possible tool, free from AccessData, is called FTK Imager. <http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk>

In summary, the most important points to consider in collecting electronically stored information are:

- ESI can be difficult to acquire because of corruption, loss, deletion, encryption or loss of the application or device that created it in the first place.
- The most important thing that you and your organization can do is to ensure that your ESI is accessible is to have good records retention policies and good practices that follow these policies.
- Maintaining and documenting the integrity of data will be paramount to make sure that the data is legally admissible as evidence or usable for audits or other recordkeeping functions.

Please also listen to/view a webinar *Mobile Device Collection – More than Just a Phone* from

the International Legal Technology Association (ILTA) on collection from mobile devices – I have uploaded the PowerPoint slides as part of Module 10 in Canvas – http://connect.iltanet.org/viewdocument/02-26-15-webinar-rec?_ga=1.158384826.1469280009.1476121881&ssopc=1

Next Steps

With Module 11, we will consider the preservation step in an electronic discovery process.

Please let me know if you have questions about Module 10 or the reading assignment.



[Home](#)

City attorney who falsified email suspended for 180 days

[IL Staff](#)

October 16, 2017

An Indianapolis city attorney who gave inaccurate information to a news reporter then tried to destroy evidence of his misconduct has been suspended from the practice of law in Indiana for 180 days.

In an order posted Thursday in [In the Matter of: Mark J. Pizur](#), 49S00-1612-DI-631, the Indiana Supreme Court unanimously decided to suspend Mark Pizur for deceitful conduct dating back to November 2015, when he was working for the Indianapolis Office of Corporation Counsel. That month, Indianapolis Animal Care and Control removed dogs from a kennel owned by Paul Upton. One month later, 14 puppies were born from those dogs, and at least five of the puppies died.

When a news reporter sought information from the ACC, Pizur sent an email to the reporter saying Upton had not notified ACC or the city that any of the dogs were pregnant. Pizur was quoted in the reporter's story, but at a subsequent hearing, Upton told the court that statement was inaccurate.

Pizur then falsely told the court that he had been misquoted, so Upton submitted a public records request seeking emails between Pizur and the reporter. Before he provided the requested emails, Pizur deleted the statement that was quoted in the article. However, the news outlet eventually sent Upton a certified copy of the original email, thus showing that Pizur had altered the requested documents.

Pizur eventually acknowledged that he had altered the email and agreed in a Conditional Agreement for Discipline that he had violated multiple Indiana Professional Conduct Rules, including 3.3(a)(1), 4.1(a), 8.4(c) and 8.4(d). He and the Indiana Supreme Court Disciplinary Commission agreed to a 180-day suspension with automatic reinstatement, which the Indiana Supreme Court approved last week.

Pizur's suspension will begin Nov. 22, and he will be reinstated at the end of a 180-day period, provided no other suspensions are in effect. The costs of the proceedings are assessed against him.

Also on Thursday, the justices unanimously suspended an Evansville attorney for pretending to be a deputy prosecutor to get out of a traffic citation. In an order in [In the Matter of: Brian J. Oberst](#), 82S00-1709-DI-605, Oberst was suspended for 60 days after he was convicted of Class A

misdeemeanor impersonation a public servant. The conviction came after Oberst was pulled over for a traffic infraction twice and displayed a badge to the officer who stopped him both times. During the second incident, Oberst also orally indicated he was a Vanderburgh County deputy prosecutor.

Oberst was released without a traffic citation for either stop, though he was neither a deputy prosecutor nor a law enforcement officer at the time of either stop. He was eventually charged and convicted in two separate cases with Class A misdemeanor impersonation of a public servant, but pursuant to a plea agreement, the first of the two cases was dismissed with no conviction upon successful completion of probation. The Indiana Court of Appeals [upheld his conviction](#) in an Oct. 10 opinion.

Both Oberst and the commission agreed he violated Indiana Professional Conduct Rules 8.4(b) and (c), which prohibit committing a criminal act that reflects adversely on a lawyer's honesty and engaging in dishonest or deceitful conduct. The parties agreed to a 60-day suspension with automatic reinstatement, and the justices approved that agreement.

Like Pizur, Oberst's suspension will begin Nov. 22, and the costs of the proceeding were assessed against him.

Finally, the high court converted Sven Marshall's suspension for noncooperation to an indefinite suspension in a disciplinary order issued Thursday in [In the Matter of: Sven E. Marshall](#), 71S00-1703-DI-143. The South Bend attorney was first suspended in May for failing to cooperate with the commission concerning a grievance against him.

The commission has now moved to convert that suspension into an indefinite suspension, and Marshall has not responded to that motion. Finding that more than 90 days have passed since Marshall's suspension, the court agreed and converted his suspension to an indefinite one, effectively immediately. If Marshall wants to be readmitted, he must "cure the causes of all suspensions in effect" and successfully petition the court for reinstatement pursuant to Admission and Discipline Rule 23(18)(b).



EMOJIS HEAD TO A COURTHOUSE NEAR YOU

Use of the pictographs in lawsuits increases

The late July release of *The Emoji Movie* made official what's become obvious to the most casual internet observer: Emojis are a pop culture phenomenon. But fame has a price. The pictographs that have proliferated across online communications are increasingly turning up in court.

The terms *emoji* and *emoticon*—the keyboard-created forerunner of emojis—have cropped up in about 80 U.S. court opinions to date, with about half the case references happening in the last two years, according to a recent paper by Eric Goldman, a professor at Santa Clara University School of Law.

“As emoticons and emojis play an increasingly important role in how we communicate with each other, they will increasingly raise

legal issues,” Goldman says.

The challenge for civil and criminal courts is interpreting emojis without the aid of clear dictionary definitions and interpreting them within the specific contexts in which they appear.

Further obscuring their precise meaning are various cultural and technical factors, especially differences in emoji icons among different technology platforms. The Unicode Consortium sets basic standards for emoji design, but the characters can appear differently across operating systems, devices and software programs.

In one survey, for example, people thought Google’s version of the Unicode-defined “grinning face with smiling eyes” emoji meant “blissfully happy,” but they construed Apple’s version

to mean “ready to fight.”

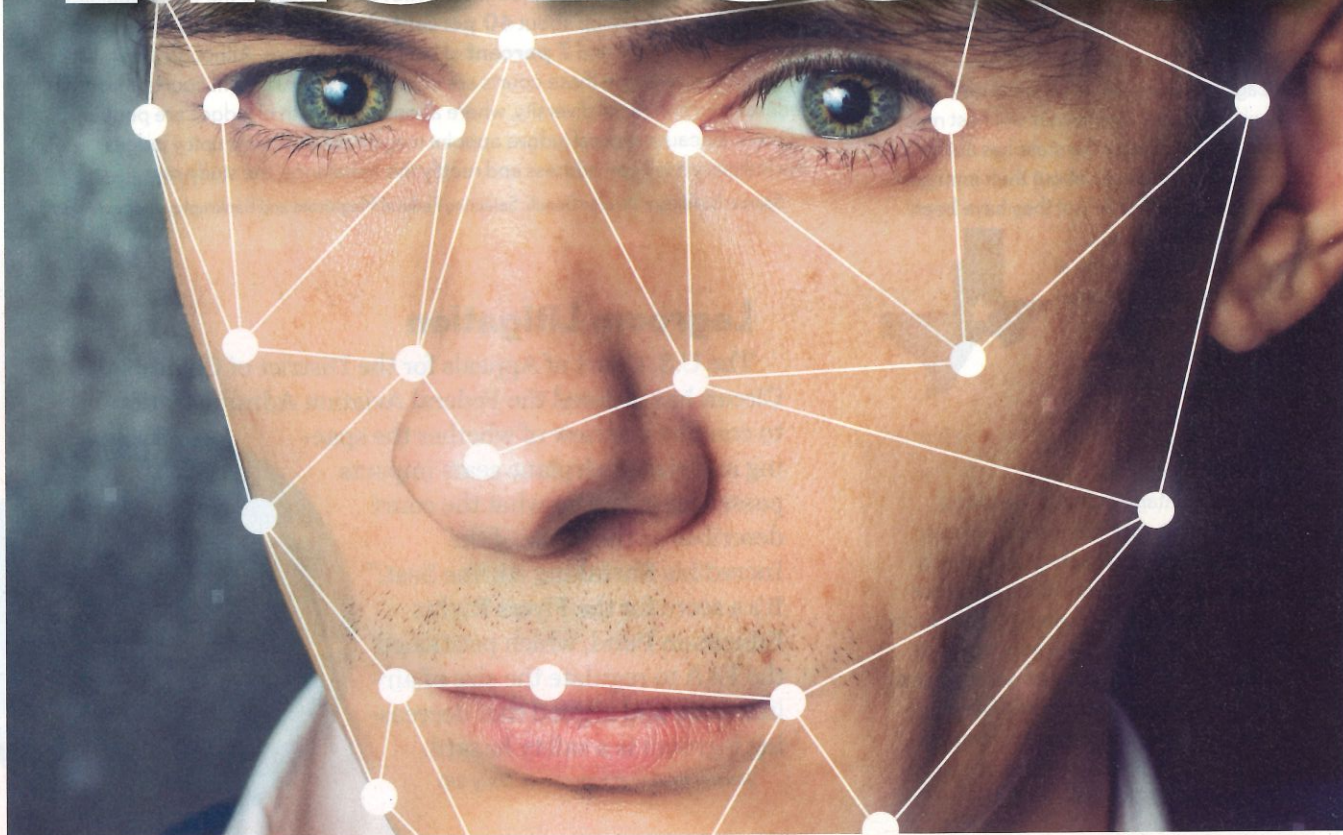
To help clear up such misunderstandings, Goldman suggests some fixes: The consortium should play a more active role in promoting cross-platform compatibility, platforms should warn users of the potential for miscommunication with emojis, and an emoji dictionary should be created.

Goldman warns that the judicial system must prepare for “the coming emoji onslaught.” That means taking steps that include showing emojis in relevant opinions, making emojis and emoticons searchable in legal research engines such as Nexis and Westlaw, and letting juries review them as part of trial evidence.

After all, if they’re appearing in movie theaters, why not the jury room, too?

—Mark Walsh

The Docket



Face Time

Facial recognition technology helps nab criminals—
and raises privacy concerns **By Wendy N. Davis**

National Pulse

When convicted killer James Robert Jones escaped from Fort Leavenworth in Kansas in 1977, he couldn't have imagined the circumstances that would lead to his capture nearly 40 years later.

Jones, a former soldier, had been convicted in 1974 for stabbing to death another soldier, 18-year-old Pvt. Lonnie Eaton. His sentence was 23 years in military prison. After escaping, Jones moved to Florida, where he lived under the name Bruce Walter Keith.

Federal marshals located Jones, then 59, in 2014, after they used facial recognition technology to compare Jones' old military photo to photos from a database of Florida driver's licenses—including one issued to him as Keith in 1981. After they made a positive match, the authorities arrested Jones at the air conditioning repair shop in Pompano Beach where he had been working.

The sophisticated technology that helped nab Jones enables people to be identified based on photos of them—including pictures taken by state agencies, such as departments of motor vehicles, as well as surveillance footage captured by street cameras.

In general, the software relies on algorithms to compare different photos and determine whether they depict the same person. Although the field is still in its infancy, its popularity is growing. Law enforcement officials are using it to help solve crimes and find fugitives. The private sector is drawing on facial recognition for confirming airport

SHUTTERSTOCK

check-ins, helping people identify their friends on social networking sites and more.

PRIVACY MATTERS

But even as the technology is proving useful on a variety of fronts, its growing deployment is raising alarms among civil libertarians, who worry that the capability to identify people based solely on their appearance will erode privacy.

Cameras are ubiquitous on the streets already. If the technology comes into wider use, people could be identified as they go about their daily business, says Adam Schwartz, a civil rights lawyer at the Electronic Frontier Foundation in San Francisco.

"We take it as a given in a free society that we can go out in public and be a face in the crowd without anyone knowing where we're going and coming," Schwartz says.

More than 117 million U.S. adults are already in databases that can be accessed at will by law enforcement officials seeking to deploy facial recognition software, according to a 2016 report by the Center on Privacy & Technology at Georgetown University Law Center.

For example, the FBI has arrangements with officials in 18 states to access driver's license photos to investigate crimes by comparing them to photos of suspects.

Law enforcement officials say they need all the tools at their disposal to fight crime.

But others think the authorities might be overstepping with these initiatives. "Innocent people should not be on this database," said Rep. Stephen Lynch, D-Mass., during a recent congressional hearing on the subject. "This is corrosive of our very liberty."

Delta Air Lines recently started testing a facial recognition system in Minneapolis that allows passengers who have passports to check their bags at a kiosk and then verify their identity via a facial scan.

In June, JetBlue Airways began to test a boarding procedure that relies on scans of passengers' faces in lieu of physical boarding passes.

And internet companies such as Facebook use the technology to enable people to automatically tag their friends in photos.

Developers in Russia created a dating app, FindFace, that lets people take photos of strangers and then discover their identities, provided they have a photo on the social media network VK, according to the *Guardian*, a British newspaper.

Schwartz says there's very little people can do to prevent others from using this kind of software. "It is very easy for someone to get your face without your knowledge or permission," Schwartz says. "There's nothing we can do to hide our faces, short of wearing ski masks all the time."

HOW ACCURATE IS IT?

Alvaro Bedoya, a professor at Georgetown Law and executive director of the Center on Privacy & Technology, says use of the technology by the police might discourage people from engaging in political activity, including protests.

"There's a real risk with regard to freedom of speech," Bedoya says. "Are you going to go to a rally against the president, or a gun rights rally for that matter, if you know that law enforcement can take a photo of you and identify you from far away?"

According to Bedoya, some prior studies have suggested that facial recognition is less accurate than fingerprints, which raises the possibility that people will be targeted by the police based on incorrect identifications.

Accuracy levels depend on myriad factors, including the conditions under which the photo was taken. In general, the technology has a high accuracy rate for posed photos, such as passport pictures, in which people are told to look directly at the camera, says Anil Jain, a computer science professor at Michigan State University.

But the technology is less accurate for photos taken under

noncontrolled conditions, such as when street cameras capture images as subjects are looking away, wearing caps or making expressions that distort their features.

LEGAL ACTIONS

No federal laws currently constrain the use of facial recognition software, and most observers think national legislation is unlikely, given the divided political environment.

But on the state level, Illinois, Texas and Washington have laws that aim to protect people's biometric privacy in the commercial sphere. Other states, including Alaska, Connecticut, Montana and New Hampshire, are considering regulating the use of the facial recognition technology.

The Illinois Biometric Information Privacy Act, which was passed in 2008, prohibits private sector companies from collecting some kinds of biometric identifiers, including scans of facial geometry, without obtaining people's written consent.

That law has already sparked several lawsuits, including putative class actions against Facebook, Google and Shutterfly. The plaintiffs in those cases allege that the tech companies illegally created "face-print" databases. Google declined to comment, and Facebook and Shutterfly didn't respond to interview requests.

Shutterfly settled one lawsuit in spring 2016 and was sued a second time last fall. Facebook and Google have been fighting the allegations in court since 2015.

The companies raise several arguments, including that the Illinois statute is ambiguous about whether it applies to photos. The law says the restrictions don't apply to photos or information derived from them, but the statute also appears to be aimed at regulating the technology.

Attorney Jeffrey Neuburger, co-chair of the technology, media and telecommunications group at Proskauer Rose, says the Illinois law was written before biometrics were prevalent, and that there's very little legislative history to shed light on

why photographs were excluded from the law's definitions.

The plaintiffs argue that the law wouldn't make sense unless it covers face scans derived from photos. So far, the plaintiffs have prevailed with that argument. "Courts have said excluding that kind of information undermines the purpose and effect of the statute," Neuburger says.

Those lawsuits also pose questions about whether states can regulate the use of facial recognition software by a national company.

RISK OF IDENTITY THEFT

Jay Edelson, a plaintiffs lawyer in Chicago who is involved in the Facebook case, says that biometric databases could expose people to the risk of fraud.

Databases of fingerprints, voiceprints and faceprints will "be a major target for identity thieves and other bad actors out there," he says.

Edelson speculates that fraudsters could use a 3D printer to create a mask based on a faceprint, and that it could fool cameras.

But others say there's no call for laws that could restrict companies from rolling out new services that at least some consumers seem to like—such as Facebook's tagging feature, which can use facial recognition technology to help people automatically attach their friends' names to photos.

"Identity theft is illegal today, whether it's done by impersonating me or by going to a photo database, downloading a model of my face, and printing a 3D mask like in *Mission Impossible*," says Carl Szabo, senior policy counsel at NetChoice, a trade group that represents internet companies.

Szabo points out that the technology can have "a multitude of potential positive uses," including improved security at banks and other establishments.

"Where we see abuses, we should target those abuses," he says. "What we need to make sure we avoid is the privacy panic." ■

Model Prisons

Attorney hopes to import the best of European practices to the United States **By Rebecca Beyer**

National Pulse

Attorney Donald Specter spent more than three decades working to protect the rights of incarcerated

people before he finally saw a prison he believed in.

He was in Europe, having just won perhaps the biggest ruling of his career—a 2011 U.S. Supreme Court decision in *Brown v. Plata* that required California to reduce its inmate population by more than 40,000. But Specter, executive director of the Berkeley-based Prison Law Office, wasn't there to celebrate. He was a co-instructor on a study-abroad trip about correctional practices with University of Maryland students.

This trip included visits to prisons in Denmark, Germany and the Netherlands. Specter says he was blown away. The prisons were nothing like those he had spent his career trying to change in the United States. For starters, they were physically different—built to resemble life on the outside. Inmates had their own rooms and, in some cases, were allowed to cook in communal kitchens. But what struck Specter most was that the prisoners were treated differently, too.

"They still regarded the people in prison as members of the community who were going to return to the community," he says. "That has a whole bunch of implications."

Specter, who began his legal career as a volunteer at the Prison Law Office, had long been frustrated by the limits of litigation to bring about meaningful change. In Europe, he began to wonder whether there might be a different way to approach his life's work.

"By the end of the trip, [the students'] basic question was: Why do we have such lousy prisons when they can be so much better?" he says. "I started thinking about whether the same kind of transformation could happen with people who were a little older

and more experienced—hardened correctional officers and the like."

A PROGRAM IS BORN

In 2013, Specter launched the U.S.-European Criminal Justice Innovation Program, sponsoring weeklong tours of European prisons for U.S. corrections officials, judges and lawmakers. He funds the trips using fees from his lawsuits, including some of the \$2.2 million his office was awarded after the high court's ruling in *Brown*.

In that case, Specter represented prisoners who challenged the delivery of health care in the California prison system. The high court affirmed an earlier appeals court ruling that overcrowding was the primary cause of the deficient system and ordered the state to reduce its inmate population.

Specter's first overseas trip was with representatives from Colorado, Georgia and Pennsylvania and included stops in Germany and the Netherlands. Subsequent tours, including one this fall with officials from Alaska, have focused on Norway, which is known for the freedoms it grants eligible inmates.

So far, officials from eight states have participated, including the executive director, president and vice president of the Association of State Correctional Administrators, which has members who oversee 400,000 correctional personnel and 8 million inmates or former inmates.

Although the United States has the highest incarceration rate in the world—676 inmates per 100,000 people, according to the United Nations Office on Drugs and Crime—Specter thinks Americans still have a lot to learn about how to prepare prisoners for life on the outside. (Norway's incarceration rate is 80 inmates per 100,000 people.)

At least 95 percent of inmates in U.S. state prisons will return to their communities upon release, according to the Bureau of Justice Statistics,

THE INDIANA LAWYER.com

[Home](#)

Bour: Google records your voice texting — and much more

[Stephen Bour](#)

October 18, 2017



Communicating with others via texting has become one of the most regularly used features on my smartphone. However, I don't particularly enjoy fidgeting with the tightly spaced keys on the touchscreen. Manipulating them can be difficult — and a dangerous thing for those who do so while driving — so I prefer to do most of my texting using the voice-to-text feature. A simple tap on the microphone icon turns on the voice recognition and allows me to simply dictate my text messages. Now, admittedly (and surprisingly), I am disappointed by how often “smart” phone mistranslations still occur, but I can accept the inaccuracies for the convenience.

Recently, an unsettling notification started popping up on my screen each time I tapped the microphone icon. It said, “Saving audio to _____@gmail.com.” What? It's saving my voice to my Google account? It referenced the Gmail ID I created when I initialized the service years ago. Why would it do that? The notification flashes up there quickly, then disappears. It did not used to do that. I called Tech Support at Verizon to get some clarity, but they were as surprised as I was. It was unclear whether this feature was something added by Verizon, by Samsung or by Google. My investigation revealed that my smartphone is gathering and retaining even more data than I previously suspected or realized. The truth turned out to be that this notification was added by the data-gathering leviathan, Google.

While it's not widely publicized, it's no secret Google has been recording the audio from your “OK Google” searches for years. This is their Siri-like feature, similar to the iPhone app. Later, I will tell you how to log in and listen to every silly question you have asked the service. However, I was unaware that every feature that uses the voice recognition technology on your phone is subject to recording by Google. This includes asking for map directions and using voice-to-text. Apple iPhone users are subject to similar storage of recordings with Siri, but users are unable to access that audio.

My impression is that Google has probably always been recording my voice text messages. They only recently added the notification about doing so because they probably got caught, so they included the

notification to cover themselves. I had always assumed that the voice recognition feature for texting was a separate function that was part of the Verizon messaging app.

For lawyers and investigators, these saved audio text files could prove to be a valuable new source of information. Just as a video deposition can convey more meaning than the written word in a transcript, the actual tone of voice could provide much more meaning to an ambiguous string of text messages, plus background noises could also provide useful clues.

To listen to and delete your audio history, sign on to your Google account and within the Activity Controls section visit the Voice & Audio Activity page. Within all the Activity pages, you may be shocked to see how much data Google is gathering, including extensive location data, history of all Google searches as well as all YouTube videos viewed. But staying focused on audio, you will be able to review and play audio from every voice text message and every “OK Google” query for as far back in time as you care to scroll. You can choose to delete individual audio clips, or you can choose to delete by date range or other filters. You can also choose to delete it all. If you want to turn off future recording, there is a button for that back on the Voice & Audio Activity page. But be vigilant. It is likely that Google will automatically turn the feature back on the next time you receive a Google update.

Unfortunately, even if you turn it off, you are still not off the hook. Google advises that while your voice inputs will no longer be saved to your Google account, they still may be saved to Google using anonymous identifiers. Big Brother — I mean Google — is still listening!

If you choose to leave the Voice & Audio Activity features on, be aware of these two disquieting features. Google advises that audio can be saved even when your device is offline. I think that means that it is still listening even in Airplane Mode. Another note reports that Google also records “a few seconds before” you say the command “OK Google”. That means it has to be listening, and thus could presumably be recording all the time.

I had one experience recently that made me suspicious about this. Pop-up ads are typically expected after you do a Google search for a particular service or product. But I began to get some very unusual pop-up ads for a very unique thing which I had never searched for by voice or by typing. The only time I had ever mentioned this item was during a dinner conversation with friends several days prior. I cannot exclude the possibility that Google might have been eavesdropping on that conversation. •

• Stephen Bour (*bourtech@iquest.net*) is an engineer and legal technology consultant in Indianapolis. His company, the Alliance for Litigation Support Inc., includes Bour Technical Services and Alliance Court Reporting. The opinions expressed in this column are those of the author.

Mobile Device Collection

More Than Just a Phone



International
Legal Technology
Association

More than just a phone...



Cell phone



Address book



Planner & Organizer



Messenger



Photo & Video camera



GPS navigator



Web client



Platform for 3rd party apps

Tech is where the evidence is at...

- Widespread Adoption of legal forensics has increased –quickly moved from primarily federal use to local level law enforcement and now business in the enterprise, prisons and schools.
- 92% of AAML divorce attorneys cited an increase in cases using **evidence taken from smart phones** during the past three years.
- In the same survey, 94% noted an increase in **text message evidence**.
- 81% of AAML members say they have seen increased use of **evidence from social networking websites** during the past five years (with Facebook being cited as the primary culprit).



Facebook Photo Sinks Man Who Stole Police Gas

Siphoner posted image of theft from Kentucky cop car



212



8



Like 3,232 people like this. Sign Up to see what your friends like.

Comments(232)

Share



VIEW THE DOCUMENT

Stealing From Cops

SUBMIT A

TIP!

SIGN UP
FOR THE **tsg**
NEWSLETTER

APRIL 18--A Kentucky man is facing a misdemeanor rap after he siphoned gasoline from a police car, a theft that came to the attention of cops after the perp posted a Facebook photo memorializing the crime.

As seen in the above photo ([click to enlarge](#)), as Michael Baker, 20, was swiping the gas last month from a Jenkins Police Department squad car, he made sure to flip the bird as his girlfriend snapped a picture.

After obtaining a copy of the photo (which began circulating in Jenkins) police arrested Baker Monday evening for theft by unlawful taking, [according to an arrest warrant](#), which alleges that he "stole gas from a Jenkins City Police Cruiser" and then "posted a picture of his theft on facebook."

Baker, pictured in the mug shot at right, is scheduled to be arraigned today in Letcher County District Court.

While the siphoning photo has been removed from his [Facebook page](#), Baker yesterday updated his 380 friends on his legal problems. "just got out of jail," he wrote in one post, adding later that "yea lol i went too jail over facebook." Responding to a friend who had not seen the image before it was yanked, Baker assured, "yea lol u would just have to see it it was funny as hell tho." (1 page)



International
Legal Technology
Association

Cell Phone & Email Forensics Investigation Cracks NYC Times Square Car Bombing Case

Forensics Blotter

 Author: Forensicon  May 4th, 2010

NEW YORK CITY: May 4th, 2010: Faisal Shahzad thought he was doing a pretty good job covering his tracks as he began his quest to detonate a homemade bomb in Times Square on a busy Saturday evening. Shahzad took a number of steps including removing the VIN number from the Nissan Pathfinder he purchased on Craigslist. Authorities were able to identify the suspect by tracking the email he used to negotiate the purchase of the vehicle. Craigslist's seller records were used by investigators to track down the cell phone number used by the purchaser. Even though the cell phone used was apparently thrown away, forensic investigators were able to use the archived cell phone records, which often include GPS positioning coordinates and numbers dialed, to help piece together what had transpired. Additionally, municipal and private enterprise web cameras are often used to validate the computer data stored by telecommunications providers. The convergence of electronic information from multiple sources and correlation of this information by forensic investigators enable authorities to move with confidence in detaining the suspect prior to his attempt to leave the country.

Forensicon's President Lee Neubecker reports, "Cell phones are more and more frequently used when conducting a forensic investigation involving theft, terrorism or deception of any kind. Many individuals falsely assume if they destroy their computer hard drive or cell phone that the data is gone. This just is not always the case."

Feds Caught the Silk Road Mastermind With... A Google Search



Kate Knibbs

Filed to: SILK ROAD 1/30/15 12:15pm

64,393 🔥 6 ★



1 2 3 4



International
Legal Technology
Association

FBI's most wanted cyber criminal caught out by pet cat password

Hacktivist Jeremy Hammond probably regrets his pet cat-inspired password followed by '123'



0



0



0



0



0



Email



Hacker Jeremy Hammond is serving 10 years in jail Photo: Chicago Police Department

By Mark Molloy and AP

4:09PM GMT 13 Nov 2014

A 'mastermind' hacker has revealed how he was arrested when FBI detectives worked out his ridiculously easy to guess computer password, the name of his pet cat followed by 123.

Print this article

USA

[News »](#)
[How about that? »](#)
[North America »](#)
[Mark Molloy »](#)



International
Legal Technology
Association

Mobile Forensics 101

- Mobile Device Data Acquisition Today is Used Widely Around the World.
 - 80% of All Criminal Investigations in Europe Involve Mobile Device Acquisition.
 - 90% of All Criminal Investigations in UK.
 - 70% in US (estimate and growing).
- Quickly Becoming The Necessary Part of Every Investigation.

Mobile Forensics 101

- Types of data available for forensic exam can be different based on the type of device, but typically:
 - Call logs
 - Texts (MMS, SMS)
 - Contacts
 - Calendar items
 - Photos
 - Music
 - Videos
 - “Snapchat” data

Mobile Forensics 101

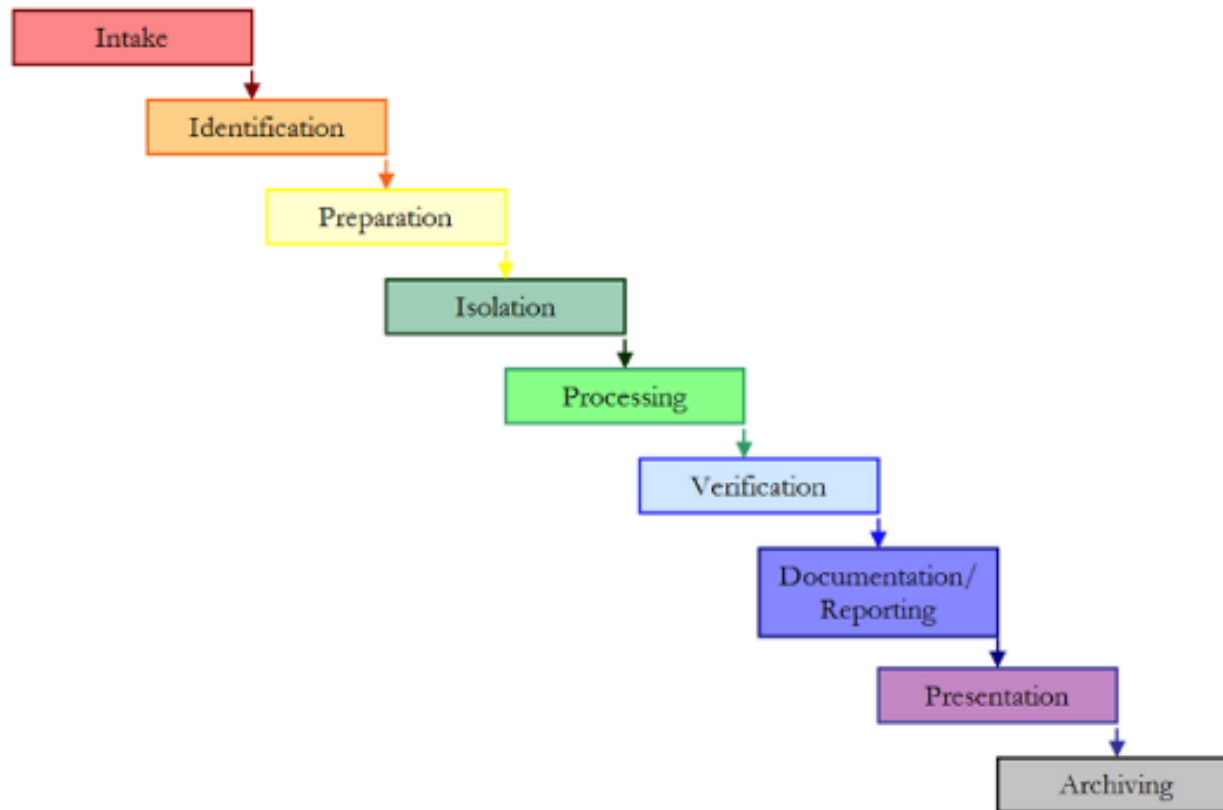
- And more...
 - Facebook Contacts, Skype, YouTube data
 - MySpace Usernames and Passwords
 - Locations from GPS, Cell Tower and Wi-Fi networks
 - Memos
 - Notes
 - Email
 - Geolocation data (phone, pictures)
 - Map histories
 - Wireless access history
 - Deleted information

The Mobile Forensic Process

- Seizure.
 - If device is found off, leave off, place in Faraday Bag.
 - If device is found on, leave on, place in Faraday Bag, and if possible, place in Airplane Mode.
 - Document everything.
 - Maintain a clear Chain of Custody.



Post-Seizure Process



Mobile Forensics 101

- Data Collection Tools
 - Constantly evolving.
 - May lag behind device introduction
 - Contribute to cost consideration.
 - Importance of validation.



Example: UFED Touch Ultimate

- Favorite of LE, can download entire contents of a phone in ~2 minutes.



Discovery Plan Checklist

- Need to have the end goal (somewhat) defined.
 - May affect acquisition strategy
 - And cost
 - Will affect the overall discovery plan
 - Essentially answering the following question:

“I need _____ to prove _____.”



Discovery Plan Checklist

- Are there any issues that require a Meet & Confer?
- After deciding on type of evidence needed, you need to specify the form or “filetype” you’re going to receive it in after collection.
- Does collected data need further processing?
 - Metadata extraction
 - Hashing

Discovery Plan Checklist

- Does the collected data need further review?
- How do you intend to produce? Or is production even needed?
- How intend to use data?
 - If intending to introduce in Court, you still have to meet fundamental evidentiary foundations of authenticity and relevance.

Authentication and Hashing

- **How do you know that you have an exact forensically-sound copy of the target device?**
- Hashing:
 - A cryptographic hash function is an algorithm that takes data and returns a hash value so that any accidental or intentional change to the data will (with very high probability) change the hash value.
 - The data to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digest.

Hash Example Comparison



DFCD394050BB2909242D90CCDEFB82AB49928DDF



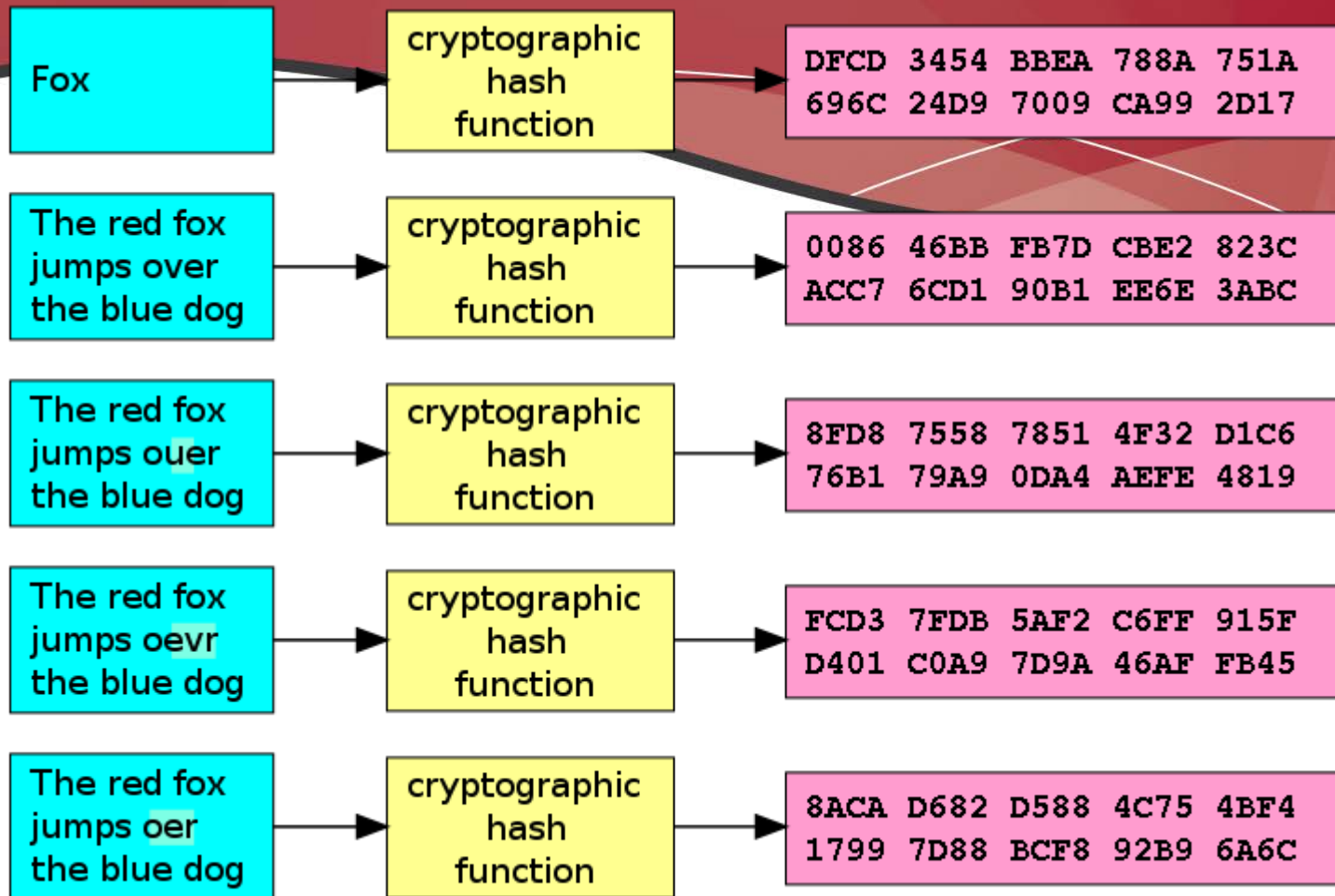
E98329BCAA928594FD78FF8A9827091D8C8FFDC4



International
Legal Technology
Association

One Pixel is Different





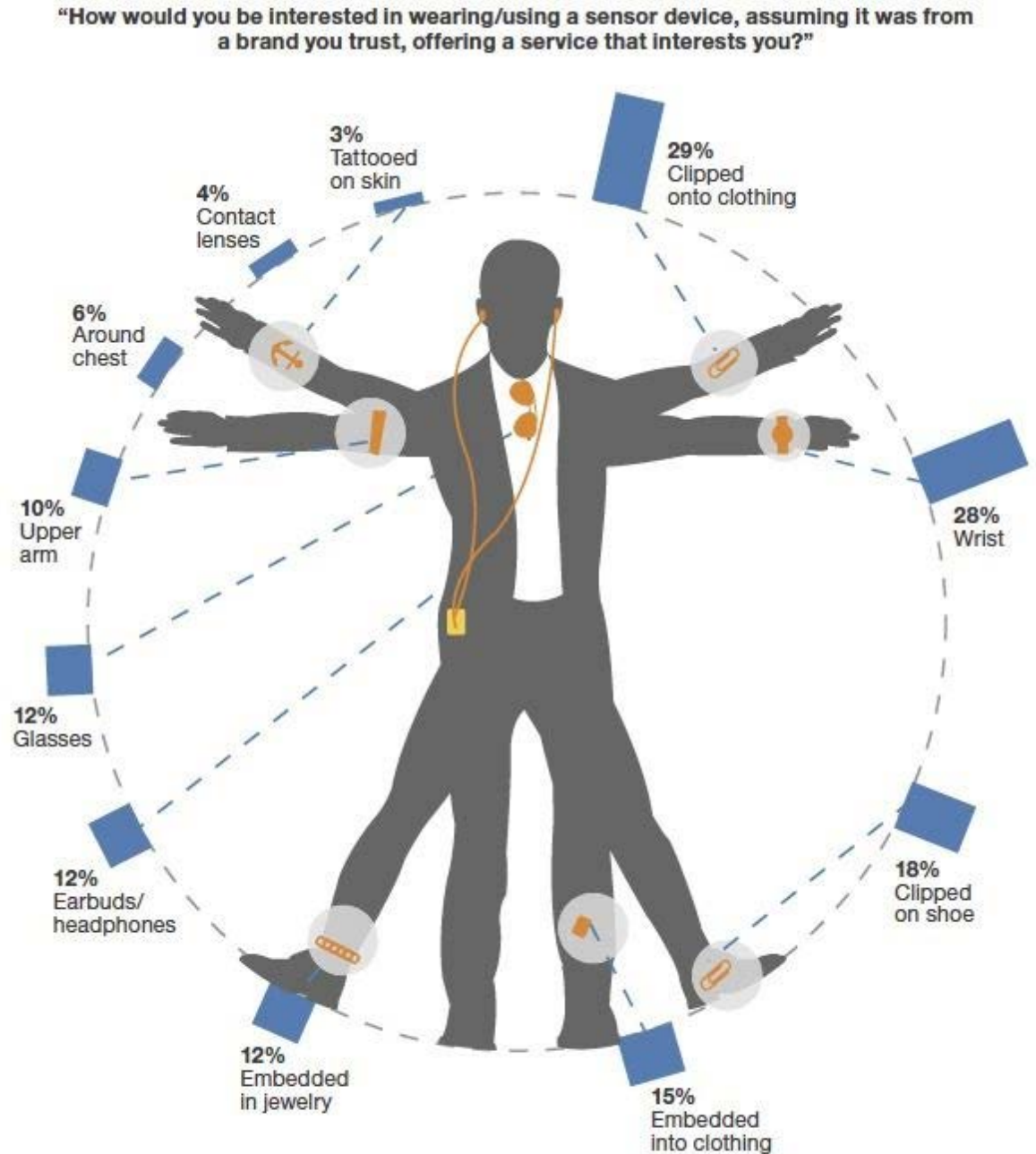
Practical Considerations

- Difficult to define an industry standard.
- Cost.
- Length of time necessary.
- Expiration of data/time elapsed since “incident”.
- BYOD.
- Explanation of technical terms to the Court.

Really Deleting Mobile Device Data

- Perform a Factory Reset.
 - Wipes out the device's existing encryption key, meaning that even if a file has survived, the phone will no longer be able to read it.
- Physically Destroy.
- Remotely Wipe.
 - The importance of a Faraday Bag.
- Use a phone with a Chinese chipset—generally difficult to extract due to poor build quality.

The Future?



Base: 4,657 US online adults (18+)
(multiple responses accepted)

Contact Information



sschaffer@watermarklabs.com



sschaffer@bladetechinc.com



[@sschaffer](https://twitter.com/sschaffer)



www.linkedin.com/in/scottschaffer314



International
Legal Technology
Association

Questions?

BLADE
TECHNOLOGIES



watermark
digital forensics



International
Legal Technology
Association