CHAPTER

Legal

7

"I am not an advocate for frequent changes in laws and constitutions, but laws and institutions must go hand in hand with the progress of the human mind ... as new discoveries are made ... institutions must advance also to keep pace with the times."

—Thomas Jefferson

INFORMATION IN THIS CHAPTER:

- The Legal Aspects of Digital Forensics
- The Fourth Amendment and Its Impact on Digital Forensics
- Electronic Discovery
- Duty to Preserve Potential Digital Evidence in Civil Cases
- Private Searches and Establishing the Need for Offsite Analysis
- Overview of the Electronic Communications Privacy Act
- Searching Digital Evidence With and Without a Search Warrant

INTRODUCTION

No discussion of digital forensic fundamentals can be complete without including the legal aspects of the discipline. The legal community has been playing a perpetual game of catch up with technology since the very beginning. With computer and other technologies becoming so intertwined in our work and private lives, it was inevitable that electronic data would find its way into the courts. It's not just about the child pornographers and identity thieves; digital evidence plays a huge role in civil litigation as well.

With these newfangled technologies came new criminal behaviors that necessitated new statutes outlawing them. Some of these are simply old crimes with a new twist. In this instance, the technology just facilitated the crime in an up-to-date, more efficient way.

Search authority is the very first step in the digital forensic process. The authority itself can take many forms, depending on which venue you're working in at the time.

Whether it be a civil or criminal case, having valid search authority is a requirement. In fact, it's the first step in the digital forensic process. In this chapter, we'll examine the fundamental legal issues in both criminal and civil litigation.

THE FOURTH AMENDMENT

The Fourth Amendment of the U.S. Constitution serves as the "litmus test" for all governmental searches and seizures. Any evidence deemed to be seized in violation of the Fourth Amendment is inadmissible in a court of law. Americans have had a long-standing distaste for governmental intrusion into their private lives. Before the American Revolution, British soldiers, operating under Writs of Assistance, routinely invaded the homes of citizens without cause. The Fourth Amendment to the Constitution was crafted with this travesty in mind. The Fourth Amendment says: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" (FindLaw, 2011).

CRIMINAL LAW—SEARCHES WITHOUT A WARRANT

Two key questions must be answered from the beginning. First, did the government act? Second, did that action violate the individual's reasonable expectation of privacy? If the answer to the first question is "no," then the Fourth Amendment doesn't apply. It only covers searches by the government (or its agents), not ones by private citizens.

For Fourth Amendment purposes, a person becomes an agent of the government if acting at the request of law enforcement. Under that scenario, it would be no different than if a police officer conducted the search.

REASONABLE EXPECTATION OF PRIVACY

What exactly is a "reasonable expectation of privacy"? That's a great question with no easy answer. There is no clear-cut rule or test that would help us define it. Much of the interpretation centers on what society as a whole would consider as being reasonable. For example, people would reasonably have a greater expectation of privacy on their personal computers than they would at a public library. As a rule of thumb, you can consider the computer as a closed container. If the officer lacks the authority to open a desk drawer or box, the same would be true with a computer (Executive Office for United States Attorneys, 2009).

If the person has a reasonable expectation of privacy, the government must first obtain a search warrant, or the search would have to meet one of the documented exceptions to the warrant requirement.

What about individual files? Should they be seen as separate, closed containers? It seems that courts aren't sure either. Rulings have been handed down supporting both positions. In *United States v. Slanina*, the Fifth Circuit ruled that, when a proper search is conducted on a portion of a disk, defendants no longer have a reasonable expectation of privacy in regard to other files. (United States v. Slanina, 2002).

In contrast, the Tenth Circuit took the opposite stance, saying "[b]ecause computers can hold so much information touching on many different areas of a person's life, there is greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer" (*United States v. Walser*, 2001).

Information that an individual knowingly exposes to others is not protected by the Fourth Amendment. Examples here could include public computers such as those in a classroom or "shared drives" on a network (Executive Office for United States Attorneys, 2009).

PRIVATE SEARCHES

Private searches are not afforded Fourth Amendment protection unless the search is done at the request of the government or with its knowledge or involvement. Take the Geek Squad at Best Buy, for example. Let's say that someone gives them permission to work on a home computer and, in the process, they find child pornography images on the machine. The images found by the repair technician would be admissible as long as the technician was not searching at the request of the government, thereby acting as its agent.

E-MAIL

By and large, an individual maintains Fourth Amendment protections when an e-mail is being transmitted, but would lose those protections when it reaches its final destination. E-mail is viewed in a similar fashion as regular "snail mail." The legal interception of an individual's e-mail or other electronic communication is tightly controlled. Known as the Wiretap Act, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 prohibits unauthorized monitoring and lists the procedures needed to obtain a warrant for wiretapping (DOJ, Office of Justice Programs, 2010).

THE ELECTRONIC COMMUNICATIONS PRIVACY ACT

The purpose of the Electronic Communications Privacy Act (ECPA) was to ban a third party from intercepting and/or disclosing electronic communications without prior authorization. This federal statute was passed originally in 1968 as an amendment to the Wiretap Act of 1968. The ECPA underwent its first change in 1994, when it was amended by the Communications Assistance to Law Enforcement Act (CALEA). It was modified once again after the 9-11 attacks by the USA Patriot Act. The Patriot Act was authorized again in 2006 (TechTarget, 2005).

EXCEPTIONS TO THE SEARCH WARRANT REQUIREMENT

There are several well-known exceptions to the search warrant requirement. A warrantless search is valid with consent as long as the person giving the consent

is authorized and the consent is truly voluntary. The voluntariness of the consent is judged on the totality of the circumstances. The Supreme Court recognized age, education, intelligence, and the physical and mental condition of the person giving consent as important factors to consider. Other considerations would be whether the person was under arrest at the time of consent and whether the person had been advised of his right to refuse consent. If the validity of the search relies on consent, the burden is on the government to prove that the consent was, indeed, given voluntarily.

Consent may be revoked at any time. The search must cease immediately when the consent is withdrawn. What happens if the suspect has second thoughts after his or her computer has been collected and taken to the lab for processing? The same standard applies—almost. The search must stop when the suspects revokes consent. That said, courts have found that this does *not* apply to forensic clones. In other words, although the original must be returned, any clones that have been made do not. Defendants do not have a reasonable expectation of privacy with a forensic clone (*United States v. Megahed*, 2009). For this very reason, cloning a drive sooner rather than later is a very wise move.

The scope of a consent search is sometimes at issue in a criminal case. If the suspect gives you consent to search the house, does that include closed containers and computers? Well, that depends on the particular details of the situation. Courts will again apply the reasonableness standard in making a determination. What would a reasonable person have understood the scope to be under those conditions?

The party granting consent may set forth restrictions on the search. Should that be the case, officers must abide with this request. To do otherwise could very well result in the suppression of any evidence recovered.

MORE ADVANCED

CONSENT FORMS

In searches that hinge on consent, it often comes down to one side's word over the other. What exactly was said, how it was said, and what the suspect understood at the time could all be scrutinized. A well-crafted consent-to-search form will go a long way in countering any attack on the search. The form should include details specifically relating to digital evidence. The form should seek permission to search not just computers but any storage media, including cell phones, manuals, printers, and more. The form should ask for permission to take these items from the location for offsite examination (Executive Office for United States Attorneys, 2009).

In the end, it's important to remember that consent searches can be highly nuanced and heavily dependent on the facts or circumstances that arise during that specific incident. While searching without a warrant is sometimes a necessity, the best practice is to get a search warrant whenever possible. Your case will rest on much more solid ground with a warrant than without.

Third parties can sometimes consent to the search of private property. Roommates, spouses, and parents are just a few of the examples. Normally, if a device is

shared, all parties have the authority to provide consent to search its common areas. In this situation, none of them would have a reasonable expectation of privacy in the common areas, since the device is shared with other people. The notion of common areas is significant. Areas such as those that are password-protected would not qualify as common areas. The third party would not be likely to have the authority to consent to a search of those areas. However, if the suspect has shared the password with the third party, then this constraint no longer applies. The suspect's reasonable expectation of privacy has been greatly diminished.

It's foreseeable that, in the end, the third party in question really didn't have the authority to consent. This is not necessarily a deal breaker as far as the admissibility is concerned. Officers in the field can only do what a reasonable person would do when determining a third party's legal ability to provide consent. If the suspect is present at the scene, a third party is not permitted to grant consent.

Spouses, under normal circumstances, can consent to the search of common areas. Parents may or may not be able to provide consent to search a child's property. If the child in question is younger than eighteen years of age, parents are generally permitted to give consent. If the child is over age eighteen, it gets a bit more complicated. Factors that will affect this determination include the child's age, whether or not the child pays rent, and what steps (if any) the person has taken to restrict access.

Technicians are often in the position of uncovering evidence during the course of their work. The courts have been split when deciding if the technician has the authority to consent. Officers may recreate the technician's search or observe them retrace their steps. Officers may not, however, expand the technician's search or direct the technician to look deeper. Should a technician locate evidence, those findings are normally used as the basis for a search warrant.

Exigent circumstances arise from time to time requiring the immediate seizure and possible search of a digital device. This is generally permitted under one of these three conditions: The evidence is under imminent threat of destruction, a threat puts law enforcement or the public in general in danger, or the suspect is expected to escape before a search warrant can be acquired. This exception may apply to the seizure of an item or device, but not automatically to the search of it. Once the item has been seized (secured), the exigency may no longer exist, thus requiring a search warrant to continue.

Officers have the right to charge suspects with evidence they see if the officers are legally permitted to be where they are, and if the item is immediately apparent to be incriminating. This is known as the "plain view doctrine." This situation typically arises in a digital forensic context when an examiner is analyzing a drive for evidence of one crime and finds evidence of a completely different one. For instance, an examiner searching a hard drive for photos of stolen artwork comes across images of child pornography. At this juncture, the search should cease until a separate warrant pertaining to the possession of child pornography can be obtained.

Border searches and searches by probation and parole officers are afforded much more latitude than those conducted by police officers. From the court's perspective, individuals entering the country can be searched with probable cause or even

reasonable suspicion. The court recognizes the government's need to secure the border from contraband and like material. Those individuals on probation or parole have less of an expectation of privacy than other citizens. For example, sex offenders may be prohibited from using the Internet during their supervised release. This stipulation would permit the parole or probation officer the authority to search the offender's computer at any time to ensure compliance. There is even some case law permitting this type of search without these specific conditions in place.

Employees in the workplace may or may not possess a reasonable expectation of privacy on their work computers. This expectation will vary depending on the facts, including whether the employee is a government employee. Normally, officers can search an employee's computer without a warrant if the employer or another co-worker (with shared authority) gives permission. Government employees are looked at a bit differently. That's not to say that employers can't search the employee's system; it just means that the search must be "work-related, justified at their inception, and permissible in scope" (Executive Office for United States Attorneys, 2009).

ALERT!
CELL PHONE SEARCHES: THE SUPREME COURT WEIGHS IN

Can police officers peruse someone's text messages and photos after the person has been arrested? The U.S. Supreme Court has now answered that question, much to the disappointment of many police officers. Basic search-and-seizure law says that a warrantless search is only permissible when it falls within certain specified exceptions. One of these exceptions is a search incidental to a lawful arrest. Traditionally, if someone is lawfully arrested, police officers are permitted to search the arrestee's person and the area under the arrestee's immediate control (often described as the arrestee's "wingspan"). An arrestee's cell phone was often routinely searched based on this exception. That practice has now come to a screeching halt.

In *Riley v. California*, Riley was stopped after police observed him driving a car with expired registration tags. This traffic stop ultimately resulted in his arrest for weapons charges. Police then searched his cell phone incidental to his arrest and found other incriminating evidence. The evidence recovered from his cell phone led to further charges, as well as an enhanced sentence for gang membership.

Historically, the search of an area under a suspect's immediate control was justified for two basic reasons: officer safety and preventing evidence from being destroyed. The U.S. Supreme Court rejected both of those reasons in this case. In addressing the safety issue, the court said that "Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape" (*Riley v. California*, 2014). While the concern for the destruction of evidence is a little more realistic, it still wasn't enough to justify a search without a warrant. In rejecting this rationale, the court noted, "law enforcement currently has some technologies of its own for combatting the loss of evidence."

The court also went on to compare the intrusion of privacy represented by a search of someone's physical possessions and that of a search of the person's cell phone. A search of the items found in an arrestee's pocket constitutes a "narrow intrusion on privacy." That cell phone is a new matter entirely. Cell phones contain massive amounts of various types of data. This data represents a "digital record of nearly every aspect of their lives." The good news for law enforcement is that this treasure trove of potential evidence isn't "immune from search" as the court says. Law enforcement officers will just need a warrant before the search of a phone can begin.

SEARCHING WITH A WARRANT

Absent one of the well-defined exceptions described here, police officers must have a search warrant before searching someone's private property, including a computer.

A search warrant is an order that is obtained by a law enforcement officer from a judge, granting them permission to search a specific place and seize specific persons or things.

A judge will issue the warrant when he or she believes that there is probable cause that a crime was committed and that the people or things specified in the warrant will be found at that location. The Supreme Court said that probable cause is established when there is "a fair probability that contraband or evidence of a crime will be found in a particular place" (*Illinois v. Gates*, 1983). Another way to look at this is whether the items or persons to be seized will be more likely than not to be found at that specific location. Mathematically, this would equate to a probability of 51 percent.

When applying for a warrant, it's helpful to determine the role of the computer in the crime. The computer can be considered contraband if it contains child pornography or is stolen property. The computer can also be used to store evidence, such as incriminating documents. Finally, the computer can serve as a tool or instrumentality of the crime. This is the case when the computer is used to hack into a company's network, for example.

SEIZE THE HARDWARE OR JUST THE INFORMATION?

We know from the Fourth Amendment that a search warrant must "particularly describe the place to be searched and the person or things to be seized." To effectively meet that requirement, we first need to understand precisely what we need to seize. In short, is it the hardware or the information held by the hardware? If the computer is contraband, evidence, or fruits or instrumentalities of a crime, then we need to establish probable cause to seize the hardware. Otherwise, our focus is on the information alone.

PARTICULARITY

Courts frown heavily on overly broad affidavits that lack the particularity mandated by the Fourth Amendment. Affidavits should make it clear what items can be seized

and what can't. "Particularly" describing things that you likely have never seen may seem like an impossible task. It's really not. Serial numbers and the like are not required.

Here is some sample language I recommend that could be used:

> *"Any and all personal computer(s)/computing system(s) located at the residence of (INSERT ADDRESS HERE), to include input and output devices, electronic storage media, computer tapes, scanners, disks, diskettes, optical storage devices, printers, monitors, central processing units, and all associated storage media for electronic data, together with all other computer-related operating equipment and materials."*

Describing the information can be done in a somewhat similar fashion. Although we probably don't know the file names, for example, it's quite possible that we would know the suspect's name, the time period, and the specific crime that's being investigated. The courts are looking for some type of limiting language. Asking for "any and all files" on a suspect's hard drive stands a very good chance of being deemed overly broad, resulting in the suppression of any evidence found.

ESTABLISHING NEED FOR OFFSITE ANALYSIS

The forensic analysis of a hard drive can be a very time-consuming process. For a variety of reasons, this is best done at the lab or police station. For all intents and purposes, doing this at the scene contemporaneously with the search should not be the first option. The search warrant affidavit should spell out, in clear terms, the logic and need for this practice. Reasons can include the amount of time and data involved and potential use of anti-forensic techniques, as well as the need to perform this task under the more controlled conditions (like those found in the lab). This is one way to make this point in an affidavit:

> *"Computer storage devices (like hard disks or CD-ROMs) can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search [onsite].*
>
> *"Technical requirements. Searching computer systems for criminal evidence sometimes requires highly technical processes requiring expert skill and [a] properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert is qualified to analyze the system and its data. In any event, however, data search processes are exacting scientific procedures designed to protect the integrity of the evidence and*

to recover even "hidden," erased, compressed, password-protected, or encrypted files. Because computer evidence is vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code imbedded in the system as a "booby trap"), a controlled environment may be necessary to complete an accurate analysis" (Executive Office for United States Attorneys, 2009).

STORED COMMUNICATIONS ACT

The Stored Communications Act (SCA), enacted in 1986, provides statutory privacy protection for customers of network service providers. The SCA controls how the government can access stored account information from entities such as Internet Service Providers (ISPs). This account information typically includes e-mail, as well as subscriber and billing, information. Specifically, the SCA lays out the process that state and federal law enforcement officers must adhere to so they can force disclosure of these records by the provider.

The SCA seeks to codify the type of information sought, privacy expectations associated with it, and legal instrument required for the government to access it. The SCA breaks down service providers into two separate and distinct groups: "electronic communication service" providers and those organizations that provide "remote computing services." Understanding these differences is essential to deciphering the SCA and its legal requirements.

According to the SCA, specifically 18 U.S.C. § 2510(15), an electronic communication service (ECS) provider is "any service which provides to users thereof the ability to send or receive wire or electronic communications." ECS examples would include companies that deliver telephone and e-mail services (Executive Office for United States Attorneys, 2009). America Online comes to mind, as does Hotmail. It may surprise you to know that any company, no matter what its focus, can qualify as an ECS.

Title 18 U.S.C.§ 2711(2) defines a remote computing service (RCS) as "the provision to the public of computer storage or processing services by means of an electronic communications system." Put another way, an RCS is provided by an "[offsite] computer that stores or processes data for a customer" (Executive Office for United States Attorneys, 2009).

The SCA also addresses the variety of information these providers store. This can include basic subscriber information like name, address, and credit card number. Other potential information includes logs and opened, unopened, draft, and sent e-mails.

ELECTRONIC DISCOVERY

The Sedona Conference defines e-Discovery as "The process of collecting, preparing, reviewing, and producing electronically stored information ("ESI") in the context of the legal process" (Sedona, 2007).

Digital evidence is alive and well in civil cases. Parties involved in litigation need to review all of the potentially relevant data, as well as any data that may have to be disclosed to the opposing party. Common means of discovery include interrogatories, depositions, and requests for document production (Sedona, 2007). Electronically stored information (ESI) presents some challenges that paper records do not. For example, ESI is easily modified, volatile, and easily duplicated and dispersed. For these reasons, the rules of evidence for both state and federal courts are changing to specifically address ESI.

DUTY TO PRESERVE

Evidence that was once confined to paper memos and filing cabinets is now found in Microsoft Word documents and backup tapes. Digital evidence is significantly different from the paper-based evidence that so many lawyers were accustomed to dealing with. For example, digital evidence is far more volatile and easier to alter or destroy. Volume is another key difference. There can be such a mind-boggling amount of data in a case that it can cost millions of dollars just to produce and review them.

In December 2006, the federal courts took the first substantive step in addressing and dealing with digital evidence by changing the Rules of Civil Procedure. These rule changes mandate that opposing attorneys work together to deal with the ESI in a case very early in the process. Addressing ESI early in a case reduces costs, time, and the chance of relevant evidence being overlooked. Not all lawyers and judges have embraced these changes. Like many folks, some lawyers and judges are very uncomfortable with technology, even going as far as to have someone else check and then print out their e-mail.

Zubalake v. USB Warburg was a series of landmark electronic discovery cases. Judge Shira Scheindlin's rulings addressed many of the fundamental concerns in cases that involve ESI. Some of the concerns included the duty to preserve electronic data, a lawyer's duty to oversee a client's compliance with these guidelines, data sampling, cost shifting, and sanctions. (Zubalake v. USB Warburg, 2003).

The duty to preserve potentially relevant data begins when there is a "reasonable anticipation of litigation." Failing to recognize this trigger and take action can result inspoliation of the evidence and potentially severe sanctions to boot. Like other legal standards addressed in this chapter, defining a reasonable anticipation of litigation can be difficult; quite difficult, in fact. The duty to preserve is not caused only by the arrival of a subpoena. It's very likely that the duty kicked in well before that time. Duty to preserve is a very fact-specific determination that will vary from case to case. The firing of a disgruntled employee could be enough to trigger it; likewise, so could an accusation of sexual harassment by an employee against a supervisor.

Judge Scheindlin also addressed a lawyer's duty to oversee a client's attempts to identify, preserve, collect, and produce potentially relevant evidence. She said, in part, "Counsel must take affirmative steps to monitor compliance so that all sources of discoverable information are identified and searched. (Zubalke v. USB Warbur, 2003)" Furthermore, she said that the attorney should draft and distribute a "litigation hold"

that directs a company and its employees to protect the relevant data and ensure they're not destroyed or compromised in any way.

Data sampling is a way to test a large collection of ESI for the "existence or frequency of relevant information" (Sedona, 2007). The volume of potentially relevant data can be staggering, especially in a large corporate environment. Data sampling is one of the best ways to save time and reduce costs during the e-Discovery process.

The costs incurred during the e-Discovery process can be massive, rising into hundreds of thousands or even millions of dollars. Typically, in traditional discovery, the producing party bears the cost of production. Under certain conditions, the costs of production may be shifted to the requesting party. In the *Zubalake* case, Judge Scheindlin addressed this concern and devised a seven-factor test to be used to determine if cost shifting is warranted. (Zubulake v. USB Warburg, 2003).

The seven factors are "(1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production compared to the amount in controversy; (4) the total cost of production compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issue at stake in the litigation and; (7) the relative benefits to the parties of obtaining the information" (*Zubulake v. UBS Warburg*, 2003).

PRIVATE SEARCHES IN THE WORKPLACE

It's not uncommon for work computers to be the subjects of searches for criminal, civil, or administrative actions. From the private side, employers have a fair bit of latitude to search an individual's company computer. A company computer use policy that clearly spells out that work computers, e-mail, and so on are for work purposes only and that they may be searched at any time is an accepted best practice. For Fourth Amendment purposes (law enforcement or its agents), a work computer can be searched with consent of a supervisor or another employee as long as that person has common authority over the area to be searched. It is also important to note that federal privacy statutes and the Stored Communications Act may come into play as well.

In the end, consult with the prosecuting attorney or corporate/in-house counsel for guidance. Getting their input can help ensure that the case is on the strongest legal footing (Executive Office for United States Attorneys, 2009)

ALERT!

INTERNATIONAL e-DISCOVERY

With the cloud environment and data regularly flying across borders, international electronic discovery is becoming an issue. Not every country has the same views on privacy or the same legal standards and procedures for discovery. As a result, gaining access to data in a foreign country is very complex. The Sedona Conference's

Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery is an excellent introduction to the complexities involved in international e-Discovery. You can download it for free from http://www.thesedonaconference.org/.

EXPERT TESTIMONY

As a digital forensic examiner, you must be prepared to testify in court as an expert witness as to your findings and procedures. What's the difference between a witness and an expert witness? A major difference is that a qualified expert witness can give an opinion, but a "regular" witness can't.

Determining whether or not an individual is an expert is a matter for the court to decide. An expert doesn't have to have a Ph.D or other lofty credentials. FindLaw defines an expert as someone "who by virtue of special knowledge, skill, training, or experience is qualified to provide testimony to aid the factfinder in matters that exceed the common knowledge of ordinary people" (FindLaw).

Under this definition, bakers, tailors, accountants, medical doctors, and school bus drivers could be qualified as experts. Certainly credentials help, but they are not a requirement.

Two cases form the foundation for the admissibility of expert testimony. The first is a 1923 case, *United States v. Frye* (1923). The *Frye* case centered on the admissibility of new lie-detection technology. Out of this case came what became known as the "Frye Test." The test said that "the results of scientific tests or procedures are admissible as evidence only when the tests or procedures have gained general acceptance in the particular field to which they belong" (*United States v. Frye*, 1923).

Eventually, the Frye Test fell by the wayside. In *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, 509 U.S. 579 (1993), the U.S. Supreme Court ruled that the Federal Rules of Evidence superseded the Frye Test. Merrell Dow Pharmaceuticals Inc. was sued by plaintiffs who claimed that its drug, Bendectin, had caused significant birth defects. The lower court granted Merrell Dow's request for summary, citing that the scientific evidence presented by the plaintiff had not yet gained approval within the scientific community. The Supreme Court agreed.

In *Daubert* (1993), the court said that the admissibility should be evaluated on "whether the testimony's underlying reasoning or methodology is scientifically valid and properly can be applied to the facts at issue. Many considerations will bear on the inquiry, including whether the theory or technique in question can be (and has been) tested, whether it has been subjected to peer review and publication, its known or potential error rate and the existence and maintenance of standards controlling its operation, and whether it has attracted widespread acceptance within a relevant scientific community" (Daubert, 1993).

Understanding this groundwork will help examiner sbetter comprehend the admissibility of their testimony within the context of the law.

ADDITIONAL RESOURCES

EXPERT TESTIMONY

Fred Smith and Rebecca Bace's book on expert testimony, *A Guide to Forensic Testimony: The Art and Practice of Presenting Testimony as an Expert Technical Witness*, contains a tremendous amount of practical information. One of the best aspects of the book is that it is written for information technology experts. The book covers the topic well and is quite readable. (Smith, F. and Bace, R., 2002).

SUMMARY

Proper search authority is a necessary first step in the forensic examination process. Evidence collected without it is very likely to be excluded. The Fourth Amendment to the U.S. Constitution protects citizens from unreasonable searches and seizures. The protections afforded by the Fourth Amendment only cover actions by the government. It does not apply to private citizens acting on their own. Law enforcement can search and seize digital evidence with and without a search warrant. Searches with a warrant are always better, from a legal standpoint, than searches without one. That said, exigent circumstances can and do arise that would permit officers to do otherwise.

On the private side, supervisors and employers are likely to have broad authority to search company computers, especially if the employee read and signed a computer usage agreement clearly stating that the company computers, e-mail, and so on could be searched at any time.

Consulting with the appropriate legal counsel before searching or seizing digital evidence is never a bad idea. If you have questions or concerns, those should always be raised in advance.

REFERENCES

Daubert v. Merrell Dow Pharmaceuticals Inc., 1993. 509 U.S. 579. Retrieved from: <www.caselaw.lp.findlaw.com/scripts/getcase.p1?court=us&vol=509&invol-579.com> (accessed 09.14.11.).

Executive Office for United States Attorneys, 2009. Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations. Office of Legal Education. United States Department of Justice, Washington, DC.

FindLaw, 2011. Fourth Amendment—Search and Seizure. Retrieved from: <http://caselaw.lp.findlaw.com/data/constitution/amendment04/> (accessed 11.10.11.).

Frye v. United States, 1923. 293 F. 1013. DC Cir. Retrieved from: <www.law.ufl.edu/_pdf/faculty/little/topic9.pdf> (accessed 11.10.11.).

Illinois v. Gates, 1983. 462 U.S. 213, 238. Retrieved from: <www.casebriefs.com/blog/law/criminal-procedure/criminalprocedure-keyed-to-isreal/arrest-search-and-seizure/illinois-v-gates-2/> (accessed 11.10.11.).

Riley v. United States, 2014. 573 US. Retrieved from: <https://supreme.justia.com/cases/federal/us/573/13-132/> (accessed 11.10.11.).

Sedona Conference, 2007. The Sedona Conference Glossary: E-Discovery & Digital Information Management, second ed. Sedona Conference, Sedona, AZ.

Smith, F., Bace, R., 2002. A Guide to Forensic Testimony. The Art and Practice of Presenting Testimony as an Expert Technical Witness Pearson Education, Boston, MA.

TechTarget, 2005. Electronic Discovery. Retrieved from: <http://searchfinancialsecurity.techtarget.com/definition/electronic-discovery> (accessed 11.11.11.).

U.S. Department of Justice, Office of Justice Programs, 2010. Privacy and Civil Liberties. Retrieved from: <http://www.justice.gov/opcl> (accessed 10.10.11.).

United States v. Megahed, 2009. WL 722481, at *3. MD Fla. Mar. 18, 2009. Retrieved from: <http://fl.findacase.com/research/wfrmDocViewer.aspx/xq/fac.20090318_0000634.MFL.htm/qx> (accessed 11.11.11.).

United States v. Slanina, 2002. 283 F.3d 670, 680. 5th Cir. Retrieved from: <http://openjurist.org/283/f3d/670/united-states-v-slanina-j> (accessed 11.11.11.).

United States v. Walser, 2001. 275 F.3d 981, 986. 10th Cir. Retrieved from: <http://leagle.com/decision/20011256275F3d981_11155.xml/U.S.%20v.%20WALSER> (accessed 11.11.11.).

www.wisdomquotes.com/authors/thomas-jefferson/.

Zubulake v. UBS Warburg, 2003. 217 F.R.D. 309. S.D.N.Y. Retrieved from: <http://www.casebriefs.com/blog/law/civil-procedure/civil-procedure-keyed-to-friedenthal/pretrial-devices-of-obtaining-information-depositions-and-discovery-civil-procedure-keyed-to-friedenthal-civil-procedure-law/zubulake-v-ubs-warburg-llc/> (accessed 11.11.11.).