Overview of Licensing and Legal Issues for Digital Forensic Investigators

Digital forensic examiners face challenges outside the technical aspects of collecting, investigating, and storing digital information. Rules about admissibility and the licensing requirements for forensic professionals must also be taken into account.

Gavin W. Manes and Elizabeth Downing
Avansic

The use of digital data in an expanding number of US court cases and business investigations has precipitated changes in evidence handling and admissibility requirements, most notably in the 2006 changes to the Federal Rules of Civil Procedure. Knowledge of these rules and the ensuing case law is an essential component of any examiner's toolkit because improper evidence handling can lead to inadmissible evidence. The court's acceptance of such evidence is also greatly affected by the examiner's proper licensure. Unfortunately, these requirements vary by state (sometimes even by city) and are constantly changing. Therefore, digital forensic investigators must heed both the court's rules regarding evidence handling and the state's rules for licensing in order to be most effective.

Evidence in US Courts

The governance and definition of the use of evidence in court systems, including electronic information, is ruled by international, national, and regional laws managed at multiple levels. US courts have a specific and strict set of rules regarding prosecutorial procedure and the admissibility of any type of evidence, including anything obtained from digital devices. Digital forensic practitioners must be aware of the judicial standards that govern evidence because they're ultimately responsible for following those rules during the collection, investigation, and handling of such information.

In the US, the Federal Rules of Civil Procedure provide guidelines for prosecution. These longstanding rules apply to every type of evidence, not just digital information; however, changes implemented in 2006 focus a great deal of attention on all aspects of the digital forensic process. Three major guidelines now govern rules about the specific handling of digital evidence: the Federal Rules of Evidence (FRE), the Daubert standards, and case law.

Note that although some states have differing rules regarding evidentiary presentation, the FRE are considered best practice. Indeed, many state court systems have begun to adopt federal practices, a trend that is expected to continue.

Federal Rules of Evidence

Evidence presented in all civil cases is subject to the FRE, including both traditional and digital evidence. Forensic practitioners have solved most of the digital forensic issues described in the FRE by applying industry-accepted tools and techniques, such as maintenance of the chain of custody and the verification of collected data via hashing. However, most controversies related to the rules involve expert testimony.

Rule 702 in particular addresses expert testimony,[1] thus a thorough understanding of it is crucial in preparation for expert witness testimony. It states that the court must scrutinize five factors when considering an expert's testimony: whether the scientific expert's theories and techniques have been tested, whether they have been subjected to peer review and publication, whether they have a known error rate, whether they are subject to standards governing their application, and whether these theories and techniques enjoy widespread acceptance.

Although this list is neither inclusive nor definitive,

it provides a strong basis that can be refined for individual cases. Additionally, testimony is still potentially admissible if one of these factors is unsatisfied. Indeed, the judge's opinion in *Daubert v. Merrell Dow Pharmaceuticals, Inc.* stated that "the admissibility inquiry must focus solely on the expert's principles and methodology, and not on the conclusions they generate."[2] This is a particularly important distinction for digital evidence, as the methods for collection and investigation are somewhat new to the court system. Investigators must take care to perform their duties systematically and stay up to date on their techniques to ensure admissibility of evidence as well as protection of their professional reputations.

Most licensing organizations impose both penalties and fines if examiners don't follow the proper evidentiary handling rules.

The Daubert Standard

The Daubert standard was established to apply to all evidence, including anything derived from digital devices. This standard contains some of the same elements as Rule 702—all evidence must be relevant, reliable, subject to empirical testing, be peer reviewed, possess a known error rate, have guidelines controlling the employed technique's operation, and operate on theories and techniques that a relevant scientific community has accepted.

Clearly, these definitions are subject to interpretation, but a significant body of case law exists for challenges made to each component of the standard. Ultimately, the Daubert standard presents a very solid basis for the treatment of scientific evidence in civil court cases.

Case Law

The US employs a "common law" legal system that allows judges to create or refine the law. Therefore, case law is often used to help determine the admissibility of digital evidence. Attorneys can cite the relevance of either civil or criminal cases when arguing any case before the court. In many state courts that have yet to adopt rules similar to the Federal Rules of Civil Procedure, case law can serve as a guideline.

The requirement to preserve electronic documents during the course of litigation came to the court's attention in the landmark digital forensics case *Zubulake v. UBS Warburg*, which involved an employment-related sexual discrimination and retaliation lawsuit. After a three-year litigation process that ultimately provided several guidelines for digital forensic sampling in modern litigation, the jury awarded Zubulake US$9 million in backpay and $20 million in punitive damages. The damages were enacted due to the failure of UBS to preserve and produce critical emails during the discovery phase of the litigation process. Other companies have received similar sanctions: Morgan Stanley[3] has settled harassment suits for millions of dollars involving inappropriate emails circulated within its offices. Although many of the damages for the case were recently overturned, none were connected with the failure to preserve pertinent information.

In some cases, the alteration of important electronic evidence, intentional or not, can lead to significant sanctions or disciplinary actions by the court. *Spoliation* includes the destruction or alteration of evidence—either by accident or on purpose—that might be necessary for current or future litigation; it also includes the lack of preservation of such information. The complexity in the duty to preserve is that evidence isn't limited to what's admissible—it also includes all that appears likely to lead to the discovery of admissible evidence. Forensic examiners must know the scope and expectations of the law when advising clients themselves or through legal counsel.

Forensic Investigator Licensing Requirements

Licensing requirements for forensic examiners have yet to be standardized on a national level, but most states require some type of license to handle evidence and perform investigations. The general field of forensic science has dealt with the licensing issue for many years now, for a variety of jobs ranging from fingerprint experts to pathologists to fraud accountant examiners. In most cases, forensic scientists are generally classified as private investigators. However, much like digital forensic experts, no national standard exists for most forensic science professionals.

Most states require digital forensic professionals to obtain a private investigator license; however, three states (Alabama, Alaska, and Wyoming) have licensing requirements only in certain cities, and others (Colorado, Idaho, and South Dakota) have no licensing requirements whatsoever. Very little reciprocity exists between states regarding licenses, so forensic practitioners must take care to ensure that separate licenses aren't necessary for the state in which evidence is to be collected or the state in which the evidence is to be investigated. Examiners would be wise to perform thorough research ahead of any forensic investigation, as these rules are constantly changing. This issue was recently brought to a point with the American Bar Association's open letter requesting that the licensing requirements for electronic discovery and digital forensic personnel be removed.[4]

Each state's laws are unique, but most have private investigator statutes that specifically handle

investigations performed for profit. Investigating a computer in the state of Oklahoma, for example, requires a private investigator license as interpreted by Title 59 Section 1759.1.[5] To both collect and investigate a computer in Arkansas requires an Arkansas private investigator license as interpreted by Class A licenses.[6] To hire someone to collect and investigate a computer in Texas requires that the individual hired has a license as interpreted in Chapter 1702 of the Texas Occupations Code, otherwise the employer could be fined.[7,8] Clearly, these rules exist in myriad places in each state's laws. As a general rule, the licensure of private investigators is controlled by an entity within the government: in Oklahoma, the Council of Law Enforcement and Training manages it; in Arkansas, the State Police; and in Texas, the Department of Public Safety. The common thread among these application processes is a fee and a mandatory federal background check. Some states also require in-state testing, college courses, or private investigator experience.

Unfortunately, no single source provides information about licensing in each state. This is in contrast to organizations such as the American Medical Association, which explains the proper methods of transferring licenses between states, as well as each state's specific requirements. However, Kessler International recently conducted a private study into the matter of forensic investigation licensing; it sent letters to the attorneys general of all 50 states, asking if fraud or computer investigations within the state required a license. The results appear on www.thekesslernotebook.com, which also contains a map with licensing information by state. The site also posts updates on the changing laws for each state. Although this is a good resource, investigators should always study each particular state's laws before commencing investigatory work.

Most states have exceptions to licensing requirements, including individuals currently practicing law enforcement, internal investigators examining cases within their own company, and people licensed by another board in the state (such as a medical doctor performing a medical forensic examination). These exceptions vary from state to state, and no taxonomy of these laws has been created or made readily accessible to the public.

Traditionally, states have controlled their own licensing related to a variety of professions outside of forensics—for example, there's no license to practice law or medicine in the entirety of the US, only within a certain state. Although private investigator licensing within each state might be cumbersome due to costs, time frames, and availability of licenses, it isn't an unreasonable system compared to those in other professions that require licenses. No national certification for private investigators currently exists, but a consumer of digital forensic services has no other method of gaining assurance about the individual they're hiring.

Most licensing organizations impose both penalties and fines if examiners don't follow the proper evidentiary handling rules. The specific injunctions vary by state, but typically include both financial sanctions and license revocation. For some states, even the attorney engaging an investigator's services can be implicated and fined thousands of dollars if he or she knowingly hired an unlicensed person.[6] Such activity can also carry sanctions or worse—inadmissible evidence. Less calculable consequences exist for operating without the proper licensure, including damage to professional reputation and the inability to provide expert testimony.

Forensic Investigator Certifications

The origins of a standard certification for digital forensic professionals began with a discussion among government agencies, but they never reached an agreement. This type of discussion has continued within the High Tech Crime Investigators Association since its inception, but it has yet to come to fruition. More recently, degrees, vendor certifications, and trade school certifications have become widely available due to the industry's popularity; unfortunately, these disparate awards don't provide a cohesive certification. The American College of Forensics Examiners Institute offers certifications for forensics consultants in general (www.acfei.com/forensic_certifications), and it exists on a national scale, but specific certifications have yet to be established.

Given that this is a relatively recently established field, it's likely that a national certification for digital forensic examiners is on the horizon. However, an overall standard would apply to a certification and not necessarily licensing. Many efforts for national certification in the digital forensic industry have come and gone since the mid 1990s, and it remains to be seen whether any new movement will be successful. The best recommendation for those wishing to hire a digital forensic professional is to consider a combination of experience, the forensic vendor's reputation, and academic certifications. This is particularly the case since the FRE changes all but mandate the use of such experts to handle digital information, and the amount of such information in the modern business landscape is increasing exponentially. The best recommendation for digital forensic professionals is to carefully research the laws in their state and stay up to date on changes in legislation that could affect those requirements.

The present FRE represent a significant step forward in the recognition and handling of elec-

tronic evidence in legal proceedings, but the courts can't keep pace with technology's evolution. This is a particularly difficult state of affairs for digital data and computer forensic examiners because they operate in a space in which the guidelines for their process are both questioned and changeable. Further adding to this uncertainty is the lack of a systematic licensing process. However, the youth of the digital forensic field combined with its increased profile in several significant legal cases will propel advances in both of these areas. In the meantime, forensic investigators must carefully monitor any changes to the court's rules or the licensing requirements in the states in which they operate to ensure that they follow the best possible practices. □

References

1. US House Judiciary Committee, *Federal Rules of Evidence*, Article VII, Rule 702, 2006.
2. *Daubert v. Merrell Dow Pharmaceuticals, Inc.*, vol. 509, 1993, p. 579.
3. *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, WL 679071, Florida Circuit Court, 1 Mar. 2005.
4. Am. Bar Assoc. Section of Science & Tech. Law, *Report to the House of Delegates, Recommendation*, 2008; www.abavideonews.org/ABA531/pdf/hod_resolutions/301.pdf.
5. *The State of Oklahoma Statutes*, Title 59, Section 1759.1.
6. *Arkansas Private Investigators and Private Security Agencies Act*, section 17-40, pp. 101–107.
7. Texas Dept. of Public Safety, TXDFP Private Security Bureau: Administrative Rules, 2007.
8. State of Texas, *Private Security Act*, Chapter 1702 of the Texas Occupation Code.

Gavin W. Manes *is the president and CEO of Avansic. His technical interests include information security, digital forensics, and telecommunications security. Manes has a PhD in computer science from the University of Tulsa. Contact him at gavin.manes@avansic.com.*

Elizabeth Downing *is a technical writer at Avansic. Her technical interests include digital forensics, information security, and arts writing. Downing has a BA in biology from Middlebury College. Contact her at beth.downing@avansic.com.*