Annual ADFSL Conference on Digital Forensics, Security and Law

2007
Proceedings

New Federal Rules and Digital Evidence

Gavin W. Manes
Oklahoma Digital Forensics Professionals, Inc., Tulsa, OK USA, gavin@okdfp.com

Elizabeth Downing
Oklahoma Digital Forensics Professionals, Inc., Tulsa, OK USA, beth@okdfp.com

Lance Watson
Oklahoma Digital Forensics Professionals, Inc., Tulsa, OK USA, lance@okdfp.com

Christopher Thrutchley
Newton, O'Connor, Turner & Ketchum, Tulsa, OK USA, chris@newtonoconnor.com

New Federal Rules and Digital Evidence

Gavin W. Manes
Elizabeth Downing
Lance Watson
Oklahoma Digital Forensics Professionals, Inc.
Tulsa, OK USA
gavin@okdfp.com
beth@okdfp.com
lance@okdfp.com

Christopher Thrutchley
Newton, O'Connor, Turner & Ketchum
Tulsa, OK USA
chris@newtonoconnor.com

ABSTRACT

The newly revised Federal Rules of Civil Procedure and developments under the Federal Rules of Evidence have a significant impact on the use, collection, and treatment of digital evidence for legal proceedings. The Rules now formally grant electronic documents and digital evidence the same status as paper and other forms of tangible evidence. As a result, the availability and proper preservation of potentially relevant electronic evidence must be considered, at the very latest, in the preliminary stages of litigation and, at the earliest, as soon as litigation is reasonably anticipated. It is important for professionals to be familiar with the specific rules and developing laws pertaining to the preservation and production of digital evidence prior to an incident or the initial stages of litigation and discovery.

Keywords: digital forensics, electronic discovery, evidence production, privilege, civil procedure

1. INTRODUCTION

The new Federal Rules of Civil Procedure strive to accommodate the daunting challenges of the digital era of modern litigation. Like it or not, digital litigation is upon us, and many professionals, must begin learning the rules of the digital game. According to a 2004 Survey conducted by the American Management Association and The ePolicy Institute, "One in five U.S. companies (20%) has had employee e-mail subpoenaed in the course of a lawsuit or regulatory investigation, up from 14% in 2003. Another 13% have battled workplace lawsuits triggered by employee e-mail" [1]. In response to a 2005 litigation trends survey, corporate counsel identified ediscovery as the number one new litigation burden for companies [9]. "The advent of electronic discovery, coupled with more stringent record keeping requirements, has exponentially added to the burdens imposed by litigation," said Robert D. Owen, a Fulbright & Jaworski, LLP litigation partner and leader of the firm's records management and e-discovery practice group [9].

What's more, the digital dilemma dawns long before litigation erupts. An increasing number of business and legal investigations include evidence extracted from digital devices such as computer hard drives, PDAs and cell phones. When it becomes apparent that digital information must be used in the course of an investigation or discovery process, forensics experts should be employed to carefully identify, gather, preserve, and examine pertinent evidence. The "snapshot" of information from a digital device must be collected in a detailed and methodical manner, since any or all evidence collected can be used in discovery, depositions, or trial. The new Federal Rules give general guidelines as to the discussion and handling of electronic documents in modern litigation. This paper briefly highlights key components of the new rules and other basic digital evidence issues with which legal,

forensics and information technology professionals, and their clients or businesses should become familiar.

2. FEDERAL RULES OF EVIDENCE

While the Federal Rules of Evidence have not been modified, careful attention must be given to how courts are applying them to digital evidence. Counsel should consider ultimate issues of admissibility as soon as sources of potentially relevant digital evidence are identified for preservation and collection. As the use of paper declines and the reliance on digital information soars, more and more cases are turning on the admissibility of electronic information. The admissibility of electronically stored data often depends on how it is collected, preserved, and produced. Courts are imposing high standards for the collection and analysis of digital evidence to ensure its authenticity under Rule 901. Establishing authenticity often hinges on the testimony of digital forensic experts, whose opinions must pass the scrupulous reliability test imposed by Rule 702 and the standards developed under *Daubert v. Merrell Dow Pharms., Inc*., 509 U.S. 579, 589-90 (1993), and its progeny.

2.1 Authenticity of Digital Evidence

Authentication of digital evidence, like paper, "requires evidence sufficient to support a finding that the matter in question is what its proponent claims" [11]. If the judge decides there is sufficient evidence for a jury to conclude that the evidence is authentic, then the judge will deem the evidence admissible. Actually deciding the authenticity of the evidence is left to the jury, who will determine the weight given to evidence after it has been subjected to vigorous cross-examination, presentation of contrary evidence, and instructions from the judge on the burden of proof.

Authenticating digital evidence presents unique challenges. With paper records, modifications can be readily discerned and the author or custodian identified by a signature or writing style. In contrast, alterations of electronic information can be difficult or impossible to detect and the author or creator may be impossible to discern.

Like paper, electronic records can be authenticated with direct or circumstantial evidence. The creator of an excel spreadsheet, for example, could provide direct testimony of authorship. The problem, however, is the ease with which digital information can be altered, destroyed, or manufactured in a convincing way. This can even be accomplished intentionally or accidentally by a novice computer user, and is, according to one expert, "alarming" [14]. The reality is that proving the integrity of digital evidence requires the use of digital forensic experts with the knowledge, skill, and experience to use and apply an array of complex methods and tools of computer science and information security [14]. Digital forensic experts use their skills and tools to generate circumstantial evidence of the integrity and trustworthiness of the evidence, or they provide evidence and opinion testimony attacking the authenticity of electronic information.

When calling upon such an expert to establish authenticity, care must be taken to ensure that the chain of custody has been securely maintained to refute any suggestion of possible adulteration. A break in or plausible doubt about the chain of custody from the time it is collected, transported, preserved, and analyzed can severely weaken the weight and credibility of the digital evidence.

2.2 Expert Testimony and Daubert

Because the authenticity of digital evidence is generally determined by experts using scientific methods beyond the knowledge and understanding of the lay juror, *Daubert* challenges to the admissibility of expert testimony should be anticipated. An expert may provide opinion testimony under Rule 702 if it is based on "scientific knowledge" that will help the jurors "understand or determine a fact in issue" [11] With regard to digital evidence, the fact usually at issue is whether the electronic information can be relied on as pure and unadulterated.

In *Daubert v. Merrell Dow Pharms., Inc*., the U.S. Supreme Court laid down guidelines by which a trial judge is to decide if "the reasoning or methodology underlying the testimony is scientifically

valid" and reliable. The *Daubert* Court provided a non-exhaustive list of factors the judge must consider in deciding whether to permit the expert testimony:

- Whether the theories and techniques employed by the expert have been tested
- Whether they have been subjected to peer review and publication
- Whether the techniques employed by the expert have a known error rate
- Whether they are subject to standards governing their application
- Whether the theories and techniques enjoy widespread acceptance [7].

The list above is neither inclusive nor definitive, and testimony may still be admissible if one or more of the factors are unsatisfied [7]. Additionally, the Court has clarified that "the admissibility inquiry must focus 'solely' on the expert's 'principles and methodology,' and 'not on the conclusions that they generate'" [7]. "So, digital forensic evidence proposed for admission in court must satisfy two conditions: it must be (1) relevant, arguably a very weak requirement, and (2) it must be 'derived by the scientific method' and 'supported by appropriate validation'" [22].

2.3 Best Evidence Rule vs. Printouts

There are still many lawyers who are surprised to learn that a printed version of a word processed document will likely be deemed inadmissible under the best evidence rule, if challenged due to the existence of the original digital document. The best evidence rule, collectively Rules 1001 through 1008, is designed to eliminate the risk that documentary evidence is really a fraud by requiring the proponent to offer the original unless certain exceptions are met [11].

An issue created by digital documents is whether a paper copy of the original digital version satisfies the best evidence rule when the digital document contains metadata. Metadata is embedded information stored in electronically created materials, but which is not visible when the digital document is printed. Usually metadata is not even seen when viewing the digital document on a computer monitor through an application software program. For example, a word processing document automatically creates metadata that describes the document, its author, its date of creation, and the dates on which changes were made, if any. As for email, metadata will tell you who was blind-copied or when it was read, while the paper printout will not reveal such nuggets. In some cases, metadata can be hugely relevant. In others, it may have no value, and its paper counterpart will suffice.

Once sources of potentially relevant electronic information have been identified, thought must be given to the proper process for collecting, transporting, preserving, analyzing, and producing it in a fashion that will not destroy its potential admissibility. The most cautious approach would entail retaining a digital forensic expert to assist with the process and to assist with the authentication of the evidence, as needed.

3. CHANGES TO THE FEDERAL RULES OF CIVIL PROCEDURE

The new Rules recognize the importance of electronic information. Indeed, it is now a requirement to discuss the preservation of digital information before the court's scheduling conference and at discovery-planning conferences [10]. The Rules give digital documents the same weight and status as paper in terms of production [10]. The revisions underscore the fundamental shift of modern litigation towards the inclusion of electronic information in the process. Although the implications of these changes will not be clear until they are tested, demand has and will continue to increase for properly performed data collection and digital forensics investigations.

3.1 Rule 16(b): Pretrial Conferences, Scheduling, Management

The changes to Rule 16(b) now explicitly encourage parties to address ediscovery issues for possible inclusion in the scheduling order. Parties that have not consulted a digital forensics specialist prior to

conducting the Rule 26(f) planning conference with opposing counsel should seriously consider doing so in order to be thoroughly educated about the issues and in order to thoroughly evaluate the various discovery management and scheduling questions uniquely raised by digital evidence. Some of the challenging issues to be considered include the types of media involved; the cost and methods of collection, preservation, restoration, production, and analysis; possible cost sharing; the form in which the digital evidence will be produced, such as native versus image; timing of the various phases; custodians of digital evidence; treatment of privileged information, etc. Matters to which the parties cannot agree prior to the scheduling order can certainly be resolved by the court and included in the scheduling order to expedite discovery. Not only will digital forensics professionals be helpful to assist the counsel and the court in resolving any e-discovery management issues, they also will be an important part of the litigation support process.

Rule 16(b) also affords the parties the opportunity to enter into "clawback" agreements of their own design, rather than relying exclusively on the default clawback contained in Rule 26(b)(5) [10]. Clawback agreements state that full production will proceed without privilege review, and that any documents discovered to be privileged can be later removed from production without waiver of the privilege. The agreement sets forth the terms and conditions by which a party that inadvertently produces privileged information or work product can "claw" the information "back." Generally, such agreements must include a third party to ensure maximum effectiveness. However, these types of agreements are a temporary solution to the general problem of removal of privileged documents from electronic production for which there is no clear answer at this time.

Screening electronic documents for privilege is made substantially more difficult by the volume of digital documents and by the informal and prolific nature of electronic communications, such as email, instant messaging, and other chat programs [2,20]. Therefore, privilege review of electronic information can quickly become costly and time-consuming. Further, the inclusion of metadata can be a concern relating to privilege, and whether this information should be captured is a topic of discussion during the discovery-planning conference. In recognition of these challenges, Rule 26(b)(5) also contains a clawback process. Despite the default provision of Rule 26(b)(5), counsel should think through the benefits of reaching their own terms and conditions in light of any unique aspects of each case, as permitted by Rule 16(b).

Attorneys should seriously consider consulting digital forensics specialists to assist in navigating clawback and other discovery issues. Most companies and individuals that use information systems are unaware of the types and locations of digital evidence may hide or linger. As such, the examiner may be asked to inspect and review information systems and deployments through sampling before making recommendations regarding discovery requests and preservation orders. Privileged documents are a significant concern within these proceedings, and the digital forensics specialist may be the key player in "clawback" agreements in order to facilitate reviews and exchanges.

3.2 Rule 26: General Provisions Governing Discovery, Duty of Disclosure

Rule 26(a)(1)(B) now makes clear that electronically stored information is included among the documents and things that must be included in a party's mandatory initial disclosures. If a party may use digital evidence to support its claims or defenses, then the party must disclose a copy of the digital evidence or a "description" of it "by category and location" [10]. To fulfill this obligation, counsel will need to meet with the client's key players, including information technologists, to compile the necessary information to be included in the initial disclosures. Parties are now directed to also discuss the form of electronic information production.

Rule 26(b)(2)(B) requires production of relevant, non-privileged, responsive digital information that is "reasonably accessible" [10]. The change recognizes that certain forms of electronically stored information are burdensome and costly to produce. If a party objects on the basis of undue burden or cost of producing information that is not so readily accessible, the objecting party must prove the

legitimacy of its objection. The Advisory Committee Notes point out that the requesting party may need to conduct discovery to test the legitimacy of the objection.

Significantly, the Advisory Committee Notes instruct that the "responding party must also identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing. The identification should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources" [22]. Counsel should consider discussing such matters at the Rule 26(f) scheduling and discovery planning conference.

The revisions to Rule 26(f) correspond to the modifications of Rule 16(b). For discovery planning and litigation management purposes, Rule 26(f) directs the parties "to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan that" addresses "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced" [10]. In that regard, the Advisory Committee Notes explain that "volume and dynamic nature of electronically stored information may complicate preservation obligations. The ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information. Failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes" [10].

3.3 Rule 33: Interrogatories

The change to Rule 33(d) permits the responding party to answer an interrogatory by specifying the records from which the answer may be derived and allowing the opposing party access to examine the records. This option is available only where the burden of deriving that answer is substantially the same for both parties. If the responding party chooses to respond by providing electronic information, it must ensure that the interrogating party can access the information and ascertain the answer as easily as the producing party.

3.4 Rule 34: Production of Documents, Electronically Stored Information, and Things

Originally, Rule 34 focused only on "documents" and "things," but the term "documents" was later amended to include "data compilations." In years since, courts have interpreted the term "documents" to include electronically stored information, which can be stored in forms that are different than they would appear on paper. The new Rule 34(a) defines "documents" as including "electronically stored information," and the phrase is even included in the new title of the Rule, affirming that the discovery of electronic data stands on equal footing with discovery of paper documents [10]. Therefore, recipients of requests for production of "documents" now have a clear duty to assume the request encompasses not only paper documents, but also all responsive electronically stored information, regardless of the media on which it is retained.

The amendment to Rule 34(a) clarifies that the parties may request an opportunity to "test" or "sample" responsive documents or other tangible things, including electronically stored information. The Advisory Committee Notes caution, however, that this amendment was "not meant to create a routine right of direct access to a party's electronic information system." The Notes encourage parties and courts to show due regard for issues of confidentiality and privacy and to guard against unjustified intrusiveness.

Rule 34(b) has been modified to permit the requesting party "to specify the form or forms in which electronically stored information is to be produced" [10]. If the requesting party fails to specify the form, the respondent may specify the form or forms in which it will be produced. Regardless of the form in which digital information is produced, Rule 34(a)(1) requires that it be "translated, if necessary, by the respondent into reasonably usable form" [22]. Obviously, it remains to be seen how courts will clarify the wide-open question of when the duty to translate digital information for the opposing party's use actually arises. However, resolving that question will likely require technical

assistance, as will the steps necessary to translate the information once the duty is triggered.

If the requesting party specifies a form to which the respondent objects and the parties are unable to reach an agreement, the respondent "must produce the information in a form or forms in which it is ordinarily maintained or in a form or forms that are reasonably usable" [10]. Producing digital information as it is ordinarily maintained means delivering the information in its native format as it is stored on the device, which may mean including metadata. As a result, the common practice of converting all documents derived from a digital device into TIF will be inadequate unless otherwise agreed or ordered by the Court. Additionally, the production of unreadable slack space files may require the examiner to extract and translate the relevant portions or provide a tool for parties to easily read the information.

As usual, parties must meet and confer to resolve differences before moving to compel production in a particular form. If a motion is filed, the Advisory Committee Notes explain that the court may decide the form regardless of those proposed by the parties.

3.5 Rule 37: Failure to Make Disclosures or Cooperate in Discovery, Sanctions

Rule 37 was modified to include a new subsection (f), which creates a safe harbor from sanctions when digital information is "lost as a result of the routine, good-faith operation of an electronic information system" [10]. This change reflects the fact that the normal use of computer and other electronic systems and devices results in the alteration or loss of digital information without regard for litigation or other legal proceedings. Similarly, the destruction of digital information pursuant to a records retention or information management policy, procedure, or practice is likewise encompassed by the new safe harbor, which appropriately protects from sanctions any such innocent alterations or losses. However, the Advisory Committee Notes emphasize that sanctions may be justified for the deliberate loss or destruction of potentially relevant digital information, as well as for the negligent failure to preserve from spoliation digital information that one should reasonably anticipate is relevant to future litigation.

3.6 Rule 45: Subpoena

Rule 45 has been revised to ensure that electronically stored information can be sought from third parties by subpoena. As usual, the burden of producing digital information and related costs may fall on the responding party unless the responding party objects and persuades the court to shift or reallocate the burden or costs of production. The Rule also states that the responding party need not provide such discovery from devices that are not reasonably accessible unless otherwise ordered by the court.

4. PRESERVATION AND PRODUCTION

For centuries, lawyers and their clients have had a legal duty to take reasonable steps to preserve potentially relevant evidence from "spoliation" [2,13]. Spoliation is the intentional or negligent destruction or alteration of evidence or the failure to preserve property for use as evidence in pending or future litigation [13]. Absent a natural disaster or spilled mug of coffee, preserving paper evidence poses few challenges. "Invisible" digital data is different, primarily due to sheer volume. It is cheap and easy to store a mountain of magnetic data on a few computer hard drives, a server, or backup tapes. The journey of a typical business email illustrates the exponential expansion of the universe of digital evidence. One email creates a number of copies: one in the sent folder of the sender's computer; one on the sender's hard drive; one on the email server; one on the recipient's hard drive; and potentially a fourth if the email is sent to or from a PDA. This digital footprint is very large. A second difference is that innumerable innocent missteps can alter or destroy warehouses of information. Even when properly preserved from spoliation, production in discovery is laden with its own landmines. Making matters worse, courts are quick to sanction those who fail to properly preserve or produce digital evidence.

According to a thorough study of all opinions published during the years 2000 through 2004, whether sanctions are imposed for failing to properly preserve or produce digital evidence turns on two factors, the degree of culpability and the degree of prejudice [23]. The greater the degree of culpability, the less evidence of prejudice is necessary to justify sanctions and vice versa. The study also found that sanctions were granted 65% of the time with defendants being sanctioned four times more often than plaintiffs. Of the cases where sanctions were imposed, 85% involved both the failure to preserve evidence from spoliation and production delays; 49% were based on a finding of willfulness or bad faith; 35% on prejudice; and 9% on mere negligence. When sanctions were granted, 60% included an award of discovery costs or attorneys fees, 30% included evidence or witness preclusion; 23% involved adverse inference jury instructions, and 28% involved two or more these remedies.

Several recent notorious cases graphically illustrate the dangers of failing to properly preserve and production digital evidence. One of the early landmark ediscovery cases is a sex discrimination and retaliation case, *Zubulake v. UBS Warburg, LLC*, which spawned numerous published opinions that have provided guidelines for the management of digital forensics in modern litigation [28]. The federal court sanctioned UBS for many things, including the failure to preserve backup tapes containing highly relevant email and other digital evidence [28]. One sanction included an adverse inference jury instruction. The instruction told the jury they could infer that UBS destroyed relevant evidence because it may have been damaging to its defense. The jury awarded Zubulake, a Wall Street equities trader, $9 million in lost wages and $20 million in punitive damages. Two other major companies, Chevron and Morgan Stanley, have settled harassment suits for millions of dollars due to inappropriate emails circulated within their offices.

The duty to preserve arises as soon as one knows or should have known that materials are relevant to a pending suit or to reasonably anticipated future litigation [4,12]. In *Zubulake*, the court held that the duty to preserve arose at the earliest when UBS managers began to fear that Zubulake may file suit. At the latest, the duty arose when Zubulake filed a charge of discrimination with the Equal Employment Opportunity Commission, the federal agency responsible for investigating alleged employment discrimination [3,18,28].

In another prominent case involving sanctions, Prudential Insurance was fined $1 million after having been found to have negligently destroyed documents [15]. All employees were notified of the litigation, and Prudential was ordered to promulgate a document retention policy.

Arguably the most infamous ediscovery sanctions case resulted in a $1.4 billion jury verdict against Morgan Stanley for securities fraud [5]. Due to the degree of culpability of Morgan Stanley and its attorneys – who not only knowingly failed to properly preserve and produce digital evidence, but also lied to the court about it – the court granted default judgment against Morgan Stanley on the issue of liability. The only issue before the jury was the amount of damages to assess. A sample of Morgan Stanley's abuses include the failure to locate a large number of relevant backup tapes, failure to notify both counsel and court of discovered tapes, and lying to the court about compliance with a preservation and production order. Additionally, they were found to have relied on flawed software written by their in-house information technology staff while searching electronic evidence, including use of an erroneous date range to search for emails and a failure to capture email attachments.

The key to properly preserving and producing digital evidence is promptly developing a thorough plan with counsel and the client's key players. When litigation or an investigation is reasonably anticipated, clients should engage counsel to help design, implement, and monitor a "litigation hold." A litigation hold is a "freeze" on a client's normal document retention and destruction policies, procedures, and practices. The litigation hold is a process designed to preserve all documents and data that may be relevant to the litigation. It covers information reasonably calculated to lead to the discovery of admissible evidence, and information reasonably likely to be requested during discovery. The client must educate its employees about the process and monitor compliance [17]. Although the client is primarily responsible for preserving and producing evidence, the litigation hold process should be

"periodically re-issued so that new employees are aware of it, and so that it is fresh in the minds of all employees" [28]. The amount of money awarded in both verdicts and sanctions, combined with the multitude of costly missteps by high-profile companies, highlights the complexity of the preservation and production problem all businesses and their counsel face.

5. DIGITAL EVIDENCE

While the new Rules have addressed the discovery of electronic information, many of the reported decisions address evidentiary challenges to the admissibility of digital evidence at trial. Not surprisingly, most of the published digital evidence decisions are criminal cases. Long before embarking down the road of discovery, counsel must seriously evaluate the significant road blocks to the ultimate admissibility of digital evidence that are created by ineffective methods of identifying, collecting, restoring, producing, and analyzing it.

Whether the investigation is civil or criminal, the forensic investigation process begins with collection. If performed incorrectly, the evidence could be inadmissible. Currently, the most popular tool for collecting and investigating digital evidence, specifically computer hard drives, is EnCase from Guidance Software Inc [2,20]. To perform collection, examiners use software such as EnCase Imager and/or hardware to copy the hard disk completely without modification byte by byte [8,16]. This process is called "mirror imaging" or "forensics copying," and this methodology is admissible in court as exemplified by *State v. Cook*, 777 N.E.2d 882 (Ohio Ct. App. 2002). In this case, a defendant appealed his conviction based on the inadmissibility of evidence generated from a mirror image taken off of his hard drive. After a detailed discussion of the mirror imaging process, the authenticity of the data taken from the image, and the possibility for tampering, the appellate court found that the trial court properly admitted the evidence. *Id*. at 886-88.

Other copying methods, such as common disk imaging, duplication, and drag-and-drop, do not preserve all of the potentially relevant data [2,6,8]. As a result, such methods provide incomplete collection results and create potent impeachment material for opposing counsel and may raise barriers to admissibility. Indeed, multiple courts have directed third-party, independent forensic examiners to provide a "mirror image" or "clone" of a computer hard drive in order to fulfill the court's discovery requirements [19,21,24,25,27].

Courts are continually refining their requirements for creating evidence grade copies of digital information. In *Taylor v. State*, 93 S.W.3d 487, 507 (Tex. App. 2002), the court recognized the importance of creating hashes of the copied computer to prove resulting copies were not modified. A hash value is a small digital fingerprint of data commonly used to test if data has been altered. In this case, the court overturned a criminal conviction, in part, because the investigating officer did not make note of the hash values, thereby introducing doubt as to the authenticity of the data and any resulting analysis [26].

Counsel should stay abreast of these evidentiary developments regarding digital evidence, and the new Federal Rules of Civil Procedure are certain to result in more definitive rulings regarding the collection and investigation of digital evidence. Lawyers face potential malpractice claims if they negligently fail to advise their clients regarding effective methods of digital discovery that are designed to minimize or completely avoid admissibility problems.

6. CONCLUSIONS

As digital devices become more pervasive, the amount of electronic information used in the legal landscape will continue to explode. The complexity of such devices and the changeable nature of such information have led to confusion and consternation regarding the appropriate treatment of digital discovery and the admissibility of electronic evidence. The changes to the Federal Rules of Civil Procedure have outlined a basic set of procedures for professionals facing these issues. However, these changes are merely the first step in the evolution of the use of electronic information in the legal profession.

7. REFERENCES

[1] "2004 Workplace E-Mail and Instant Messaging Survey," American Management Association, New York, New York 2004.

[2] Arkfeld, M. R. (2005), Electronic Discovery and Evidence, Law Partner Publishing, LLC, Phoenix, AZ.

[3] Byrnie v. Town of Cromwell Bd. of Educ., 243 F.3d 93, 108 (2d Cir. 2001)

[4] Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 175 (S.D.N.Y. 2004)

[5] Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., No. CA 03-5045 AI, 2005 WL 679071 (Fla. Cir. Ct., 15thCir., March 1, 2005); 2005 WL 674885 (March 23, 2005).

[6] Carrier, B. 'Open Source Digital Forensics Tools: The Legal Argument', @stake Research Report, October 2002.

[7] Daubert v. Merrell Dow Pharmaceuticals, Inc., 509 US 579 (1993).

[8] Digital Data Acquisition Tool Specification, Nat'l Inst. Standards & Tech. U.S. Dep't Commerce, Oct. 4, 2004.

[9] Dillard, Stephen C., "Litigation as the Great Equalizer: New Fulbright & Jaworski Survey Finds," *Sarbanes-Oxley Compliance Journal*, 2005.

[10] Federal Rules of Civil Procedure, December 2006.

[11] Federal Rules of Evidence, December 2006.

[12] Fujitsu Ltd. v. Federal Express Corp., 247 F.3d 423, 436 (2d Cir. 2001).

[13] Gorelick, Jamie S., Marzen, Stephen Esq., Solum, Lawrence B., Destruction of Evidence Aspen Law and Business, Aspen, Co, 1989.

[14] Hosmer, Chet, "Proving the Integrity of Digital Evidence with Time," *1st Int'l J. Of Digital Evidence*, 2002.

[15] In re Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598 (D.N.J. 1997).

[16] Kenneally, Erin, "Computer Forensics," ;login: The Magazine of USENIX and SAGE, Volume 27, Number 4, August 2002.

[17] Nichols et al., Defending Your Digital Assets Against Hackers, Crackers, Spies, & Thieves, McGraw-Hill, Inc. New York, NY, USA, 2000.

[18] Mosaid Tech. Inc. v. Samsung Electronics Co., 348 F. Supp. 2d 332 (D.N.J 2004)

[19] Northwest Airlines, Inc. v. Local 2000, 2000 U.S. Dist. LEXIS 22638 (D. Minn. 2000).

[20] Palmer G., 'A Road Map for Digital Forensic Research,' the First Digital Forensic Research Workshop (DFRWS), November, Utica, New York, 2001.

[21] Playboy Enter., Inc. v Welles, 60 F. Supp.2d 1050 (S.D. Cal. 1999).

[22] Ryan, Daniel J., Shpantzer, Gal, "Legal Aspects of Digital Forensics," The George Washington University, Washington, D. C., September 2002.

[23] Scheindlin, Shira A., Wangkeo, Kanchana, "Electronic Discovery. Sanctions in the Twenty-First Century," 11 Mich. Telecomm. Tech. L. Rev. 71, 2004.

[24] Simon Prop. Group L.P. v. mySimon, Inc., 2000 U.S. Dist. LEXIS 8950 (S.D. Ind. 2000).

[25] State v. Cook, 777 N.E.2d 882 (Ohio Ct. App. 2002).

[26] Taylor v. State, 93 S.W.3d 487 (Tex. App. 2002).

[27] United States v. Alexander, 2004 U.S. Dist. LEXIS 27790 (E.D. Mich. 2004).

[28] Zubulake v. UBS Warburg LLC, No. 02 Civ. 1243 (SAS), 2004 U.S. Dist. LEXIS 13574, at *35 (S.D.N.Y. July 20, 2004).

AUTHOR BIOGRAPHIES

Dr. Gavin W. Manes has both taught and performed hundreds of forensics investigations over the past eight years as a student and a professor at the University of Tulsa. Most recently, he founded Oklahoma Digital Forensics Professionals to fill a gap in the Oklahoma economy by offering digital forensics services. Dr. Manes has a background in computer security, information assurance, telecommunications security, and digital forensics. He was responsible for the creation of the Tulsa Digital Forensics Laboratory on the University of Tulsa campus. As a result, both the Tulsa Police Department Cyber Crimes Unit and the Oklahoma State Bureau of Investigation Computer Crime unit have a permanent presence utilizing the facility.

Lance Watson received his Master of Science in Computer Science from the University of Tulsa in 2003. During his time at TU, he focused on computer and network security, including participation in research regarding telecommunications security. He has earned all five of the federal CNSS/NSTISSI information assurance certifications. Currently, Lance Watson is serving as the Vice President of Client Relations at Oklahoma Digital Forensics Professionals, Inc. Mr. Watson oversees company operations including the collection and analyses of digital devices such as computers, cell phones, and PDAs. Information or evidence found is delivered to clients in easy to read non-technical reports. Mr. Watson's ensures the company adheres to the highest standards of quality, confidentiality, and professionalism.

Elizabeth Downing is a Technical Writer at OKDFP. Previously, she has been a paralegal for several attorneys and firms in Oklahoma. At OKDFP she drafts reports and ensures the readability of technical jargon in these reports.

Chris Thrutchley earned his law degree with highest honors from The University of Tulsa in 1993 and served as Editor-in- Chief of the TULSA LAW REVIEW. He is AV® Peer Review Rated, the highest rating a lawyer can receive for ethical standards and legal ability. He represents employers in labor and employment matters before all state and federal courts and agencies. Mr. Thrutchley is a certified Professional in Human Resources, a designation awarded for mastery of the strategic and functional areas of human resources. He has the unique experience of having served as a human resources director with one of Tulsa's largest unionized employers. Mr. Thrutchley is the Chairperson of the Oklahoma Bar Association's Labor & Employment Law section and is a leader with the Tulsa Area Human Resources Association and the Tulsa EEO Coordinator's Association.

Since 2003, Oklahoma Digital Forensics Professionals, Inc. (OKDFP) has been committed to providing digital forensics services to the business and legal communities by investigating and retrieving information from computer hard drives and other digital devices. OKDFP adheres to the highest standards of quality, confidentiality and diligence in the field of digital forensics.