Information Security Journal: A Global Perspective
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uiss20

What Security Professionals Need to Know About Digital Evidence

Gavin W. Manes [a] & Elizabeth Downing [a]
[a] Avansic , Tulsa, Oklahoma, USA
Published online: 04 Jun 2010.

Information Security Journal: A Global Perspective, 19:124–131, 2010

ISSN: 1939-3555 print / 1939-3547 online
DOI: 10.1080/19393550903200466

Taylor & Francis
Taylor & Francis Group

What Security Professionals Need to Know About Digital Evidence

Gavin W. Manes and Elizabeth Downing
Avansic, Tulsa, Oklahoma, USA

ABSTRACT This paper presents the fundamentals of digital evidence for security practitioners. The modern security landscape is expanding to include a digital forensics and investigative skill set for many professionals, particularly those in the corporate realm. This paper introduces security personnel to the Federal Rules of Civil Procedure, case law related to preservation and production of digital evidence, international issues with electronic data, how to handle privilege or sensitive information, and the issues surrounding licensing and certification of computer investigators and digital forensics professionals.

KEYWORDS digital forensics, eDiscovery, lawsuits, licensing, electronic evidence

INTRODUCTION

Successful security professionals must be versed in a substantial array of technical, regulatory, and corporate practices. Through the course of these duties, they may be called upon to handle, produce, or investigate the digital information pertinent to internal or external investigations within their purview. Although there are a number of overlapping skill sets between information security and digital forensics, there are significant differences in the treatment of proprietary corporate data versus digital information bound for use in court. Indeed, the digital forensics field comprises 50% technical know-how, 20% business acumen, and 30% legal knowledge.

It would behoove security personnel to have a working knowledge of the procedures for preserving and producing digital evidence as well as an understanding of the case law decisions that relate to technical practices. This is complicated by rules and regulations that vary by nation, state, and sometimes municipality. Unfortunately, the digital forensics field has no policy so concise as the Payment Card Industry Data Security Standard (PCI) or the Health Insurance Portability and Accountability Act (HIPPA); rather, the handling of digital information that may become evidence in the United States requires an understanding of the Federal Rules of Civil Procedure, Federal Rules of Evidence, and the Daubert standards for evidence (Fed. Rules of Civil Proc., 2007; U.S. House Jud. Comm., 2006; *Daubert v. Merrell*, 1993). This is complicated by differences in laws, court rules, and policies for information retrieved or produced across continental lines since the regulations for electronic evidence vary by country.

Address correspondence to Gavin W. Manes, Ph.D., Avansic, 401 S. Boston, #1701, Tulsa, OK 74103. E-mail: Gavin.Manes@Avansic.com

This knowledge is important for individuals working from executive-level management to help desk support, since decisions at any level can affect the successful outcome of a forensics investigation and, by extension, a lawsuit. It is also critical to understand where a situation warrants the hiring of forensics experts to maintain the impartiality of the digital information in question. However, this decision can be fraught with peril as well, since the licensing and insurance requirements for digital forensics professionals are different for each country and each state and are continually changing. In addition, there are few nationwide or international vendor-neutral certifications for digital forensics professionals, making it difficult to determine an individual's specific qualifications.

FORENSIC INVESTIGATOR LICENSING REQUIREMENTS

Licensing requirements for forensics examiners have yet to be standardized on a national level in the United States, but most states require some type of license to handle evidence and perform investigations. The general field of forensic science has been dealing with the licensing issue for many years for a variety of jobs ranging from fingerprint experts to pathologists to fraud accountant examiners. The debate and analysis regarding this topic is both ongoing and occasionally heated.

Most states requires digital forensics 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 (Kessler & Assoc., 2008). There is little reciprocity among states regarding licenses, and care must be taken to ensure separate licenses are not necessary for the state where evidence is to be collected and investigated. Examiners would be wise to perform thorough research ahead of any forensics investigation, as these rules are constantly changing. This issue recently has been brought to a point with the American Bar Association's open letter to all states requesting that the licensing requirements for electronic discovery and digital forensics personnel be removed (ABA, 2005).

Each state's laws are unique and subject to interpretation both by the persons applying for a license to handle digital information and the administrators of such licensure. However, most states have private investigator statutes that specifically handle investigations performed for profit. For example, investigating a computer in the state of Oklahoma requires a private investigator license as interpreted by Title 59 Section 1759.1 (State of Okla. Statutes, 2007). To both collect and investigate a computer in Arkansas requires an Arkansas private investigator license as interpreted by Class A licenses (Ark. Private Investigators Act and Private Security Agencies Act). To hire someone to collect and investigate a computer in Texas requires that the individual has a license as interpreted in the Chapter 1702 Texas Occupations Code; otherwise, the employer may be fined (Tex. Dept. of Public Safety, 2007).

California's enforcement manager of the agency responsible for licenses explicitly stated that "if a person or entity performing a computer forensic investigation within California obtains information that will be used, or results in [anything described in the PI licensing scheme] . . . a private investigator license is required" (Rasch, 2006). Likewise, Delaware Attorney General Ralph Durstein was quoted as saying, ". . . the conduct of a computer forensic specialist is no different from that of a more traditional private investigator or detective, namely seeking information for a client about another person" (Rasch, 2006). Thus, there are states with clear and definitive positions on the matter (at least for the time being), but others are not so precise.

Clearly, these rules exist in multiple different places in the laws of each state. As a general rule, the licensure of private investigators is controlled by an entity within the government: In Oklahoma, it is managed by the Council of Law Enforcement and Training; in Arkansas, by the State Police; and in Texas, by the Department of Public Safety. The common thread among these application processes is a fee and a required federal background check. Some states also require in-state testing, college courses, or private investigator experience.

Unfortunately, there is no single source of information regarding licensing in each state. This is in contrast to organizations such as the American Medical Association, which explains the requirements of each state as well as the proper method of license transfers. However, Kessler International has compiled information on digital forensic investigation licensing by sending letters to the Attorney Generals of all 50 states asking if fraud or computer investigations within the

state required a license. The results have been published on their website, which also contains a map with licensing information by state and updates are given on the changing laws (Kessler & Assoc., 2008). Although this is a good resource, investigators should always study each particular state's laws before commencing investigatory work.

There are several exceptions to licensing requirements in the majority of states. Most states consider practicing law enforcement officers performing criminal investigations as a part of their duties to be exempt. However, if a law enforcement officer is performing an investigation as a consultant for any additional work, they may need to obtain a private investigator license. Persons licensed by another board in the state performing duties related to that license do not require an additional certification, for example, a medical doctor performing a medical forensic examination. The exception that could be most pertinent to security professionals relates to internal investigators working on cases within their own company. Generally, states require that the person investigating must be an employee, not a contractor or consultant. If a company outsources their information technology services and those individuals are handling digital evidence, they will most likely need a private investigator license. 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 is no license to practice law, medicine, or private investigations in the entirety of the United States, only within a certain state. Although private investigator licensing within each state may be cumbersome due to costs, timeframes, and availability of licenses, it is not an unreasonable system compared with those in other professions that require licenses.

International laws regarding licensure are even less clear. There is no overriding international standard license for digital forensics or e-discovery professionals. Depending on the type of work being performed, such licensing could be covered under other regulations or fields of work, such as bounty hunting, private investigators, detective licenses, or private security licenses.

Most licensing organizations impose both penalties and fines if examiners do not follow the proper evidentiary handling rules. The specific injunctions vary by state but typically include both financial sanctions and the revocation of licenses. Such activity can also carry sanctions, fines, or worse, inadmissible evidence. Less calculable consequences exist for operating without the proper licensure, including the loss of professional reputation and the inability to provide expert testimony.

FORENSICS INVESTIGATOR CERTIFICATIONS

The development of a standard certification for digital forensics professionals has been in the making for a number of years, but nothing has come to fruition. More recently, degrees, vendor certifications, and trade school certifications have become widely available due to the popularity of this industry; unfortunately, these disparate awards do not provide a cohesive certification. The American College of Forensics Examiners Institute, a national organization, offers certifications for forensics consultants in general, but specific certifications have yet to be established (American College of Forensic Examiners, 2008). There are a few opportunities for international digital forensics certifications, such as those offered by the International Society of Computer Forensic Examiners (Int. Society of Computer Forensic Examiners, 2009).

Given that this is a relatively new field, it is likely that a national certification for U.S. and international digital forensics examiners is on the horizon. It should be noted that this standard would apply to a certification and not necessarily licensing. Many efforts for national certification in the digital forensics 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 forensics professional is a combination of experience and certifications from forensics vendors, the computer industry, and academia. This is particularly the case since the federal rule 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. Careful consideration should be taken when information must be retrieved from across country and continental borders,

as the specific rules and requirements will need to be taken into account.

The best recommendation for digital forensics professionals is to carefully research the laws in a particular state or country and stay up to date on changes in legislation that could affect those requirements. Security professionals should be aware of these circumstances in order to most effectively utilize their own personnel relating to training or certification or to recognize the parameters necessary to hire an outside vendor to handle digital evidence.

PRESERVATION AND PRODUCTION OF ELECTRONIC EVIDENCE

The changed federal rules have created significant consequences for attorneys and companies that fail use the proper timing and methods of preserving and producing digital evidence (Fed. Rules of Civil Proc., 2007; U.S. House Jud. Comm., 2006). In fact, a Fulbright Survey of corporate counsel indicates that the number one problem in current litigation is the preservation and production of digital evidence (Fulbright and Jaworski LLP, 2006). In a 2004 survey, 21% of employers were ordered to produce digital evidence as part of legal proceedings, a number that has increased significantly as digital devices become more pervasive in the workplace (Flynn, 2004).

The course of a typical business email provides an example of the vast digital trail that a single document can traverse, highlighting the complexities of digital evidence production. An email simply sent from one employee to another produces a minimum of three digital copies – one in the sent folder, one on the personal computer hard drive, one on the email server, and potentially a fourth if the email is sent to a personal digital assistant (PDA). Word documents can reside in a larger number of places, particularly if it is transmitted to multiple people for edits: a performance evaluation, for example, is generally drafted by a supervisor, edited by the supervisor's superior, edited by human resources, comments sent through email, and then finalized. The digital footprint of such a document is very large given the number of computers containing drafts, edits, and emailed versions.

A large number of companies are finding themselves on the losing ends of battles regarding preservation and production of this type of digital evidence. *Zubulake v. UBS Warburg*, a landmark digital forensics case, involved employment-related sexual discrimination and retaliation (*Zubalake v. UBS Warburg*, 2002). After a lengthy litigation process that has provided guidelines for the management of digital forensics in modern litigation, it was determined that UBS failed to preserve critical emails, and sanctions were levied: the jury awarded the plaintiff $9 million in pay and $20 million in punitive damages. This verdict may have been significantly different had UBS been able to produce the emails in question.

Spoliation of evidence is defined as the "intentional or negligent destruction or alteration of evidence or the failure to preserve property for use as evidence in pending or future litigation" (Gorelick, Marzen, & Solum, 2001). The duty to preserve is not just limited to evidence that may be admissible but also to anything that appears likely to lead to the discovery of admissible evidence.

The issue of when the preservation process begins is a thorny one. As defined by *Zubulake v Warburg*, preservation should begin "when you knew or should've known the evidence was potentially relevant to future litigation" (*Zubalake v. UBS Warburg*, 2002). In the instance of the *Zubulake* case, UBS would have been compliant if it had begun preservation when the employee filed a charge with the Equal Opportunity Employment Commission (EEOC). However, the company would have benefitted from preserving evidence when the employee's manager feared a lawsuit four months prior to the official charge. Other companies can learn from this situation by anticipating lawsuits from internal complaints, grievances, whistleblowers, and disciplinary actions. This means that the lines of communication among human resources, information technology, and internal counsel must be open and frequently utilized in order to best adhere to the court's preservation requirements.

Another issue involves which information a company should keep. It is good practice to preserve what is relevant to possible claims and defenses, what is reasonably calculated to lead to admissible evidence, and what is reasonably likely to be requested during discovery. Clearly, these rules provide substantial room for interpretation, and case law continues to be developed on this issue.

The applications of sanctions in the failure to preserve are based on the degree of culpability and the degree of prejudice. A 2004 study determined that sanctions are granted 65% of the time for all written

opinions, where defendants are sanctioned four times more often than plaintiffs (Scheindlin & Wangkeo, 2004). Sanctions can be based on willfulness or bad faith, prejudice, and negligence of the violator. These sanctions can range from paying the cost of e-discovery or attorneys fees, adverse inference jury instructions, evidence or witness preclusion, attorney fees and costs, to default judgment (Scheindlin & Wangkeo, 2004).

In a prominent case involving sanctions, Prudential Insurance was fined $1 million after having been found to have negligently destroyed documents (Prudential Ins. Co. Litigation, 1997). All employees were notified of the litigation, and Prudential was ordered to promulgate a document retention policy. A major case against Morgan Stanley involved a securities fraud claim, where the company was found to have knowingly failed to preserve and produced digital evidence: the verdict was for $1.4 billion (*Coleman Holdings Inc. v. Morgan Stanley,* 2005). 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 preservation and production order.

In addition, Morgan Stanley was found to have relied on flawed software written by its in-house information technology staff while searching electronic evidence, including the use of a flawed date range to search for emails and a failure to capture email attachments. Although some of the monetary compensation for this case has since been reversed by the court, the decisions related to spoliation have not been rescinded. The amount of money awarded in all of these verdicts and each company's missteps highlight the problems faced by all companies with regard to the preservation and production of electronic information.

Preservation and production for international cases is further complicated by the varying treatment of such data in each country. Of note, the European Union's Privacy Directive dictates that electronic information cannot be transmitted across borders without consent, which clearly includes the production of such information for discovery purposes (Berkowitz, 2009). Article 12 of the United Nations Declaration of Human Rights states the right to privacy for all people, which could be interpreted to cover their associated digital information being requested or seized in relation to legal proceedings (United Nations, 1948).

In addition to these two largely scoped rules, many countries have "blocking statutes" which specifically target the nondisclosure of certain types of electronic information (Cook, 2009). The right to privacy is a major concern in many European countries, so much that those attempting to comply with discovery orders can be heavily fined for producing private information (Cook, 2009): this includes the UK's Data Protection Act in 1998 (UK Info. Comm. Office, 2007). Australia, New Zealand, and Hong Kong are all amidst reviews of their privacy and confidentiality laws, with changes expected soon (OECD, 2008). New Zealand's proposed changes to its Privacy Act of 1993 are noteworthy because it takes away a residence requirement to submit a privacy request and requires that any information passing through the country is subject to the privacy law (New Zealand Parliament Bills Digests, 2008).

Some metadata may be considered private and therefore would not be subject to discovery under the laws of France, in particular (Devy, 2008). This creates significant issues particularly for large corporations whose offices, information, and data storage facilities span the globe. In addition, there may be substantial jurisdictional issues relating to electronic document discovery that crosses borders.

Whether information resides locally or internationally, the development of a plan to properly preserve evidence is key to avoiding sanctions. When litigation is reasonably anticipated, counsel should be engaged to help design, implement, and monitor a "litigation hold." This should be "periodically reissued so that new employees are aware of it, and so that it is fresh in the minds of all employees" (Gorelick, Marzen, & Solum, 2001). Corporate counsel should speak directly to those company employees likely to have relevant information about the litigation hold.

At the least, companies should suspend their document destruction practices and consider adopting a record management policy to guard against spoliation torts. Counsel may request unadulterated electronic copies of all relevant active files from key players, including security personnel, and make sure that all back-up media containing this information is identified and safe. It may behoove those participating in multicountry litigation to consult with local counsel to ensure that the discovery process proceeds as smoothly and effectively as possible.

EVIDENTIARY ADMISSIBILITY

Many legal issues in digital forensics stem from the "cleanliness" of the information being extracted. Both the court system and alternative dispute resolution venues require high standards for the collection and analysis of digital evidence. Digital evidence is subject to the same standards as to any other scientific evidence produced in court, termed the "Daubert" rules: ". . . to even reach the point where specific competency questions are answered, digital evidence must survive the threshold test posed by Daubert of its competency as a class of evidence" (*Daubert v. Merrell Dow Pharmaceuticals*, 1993). In addition, the court has consistently upheld Rule 702 of the Federal Rules of Evidence, suggesting that the following factors be considered when admitting scientific evidence:

- Whether the theories and techniques employed by the scientific 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, and
- Whether the theories and techniques employed by the expert enjoy widespread acceptance.

The list above is neither inclusive nor definitive, and testimony may still be admissible if one or more of the factors are unsatisfied. Also, 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" (*Daubert v. Merrell Dow Pharmaceuticals*, 1993). In their article titled "Legal Aspects of Digital Forensics," D. Ryan and G. Shpantzer state that "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'" (Ryan & Shpantzer, 2002). Producing parties may be asked to use acceptable standards and subjective judgment to limit the amount of evidence produced based on factors such as relevancy, date, author, or location.

In 2006, changes were made to the Federal Rules of Civil Procedure that indicate the court system recognized the crucial importance of electronic information in the process of investigation and litigation (Fed. Rules of Civil Proc., 2007). It is now a requirement to discuss digital information and preservation before the court's scheduling conference and at discovery-planning conferences. In particular, these Rules assign the same weight and status to electronic documents as paper documents.

These rule changes underscore the fundamental shift of modern litigation towards the inclusion of electronic information in the legal process. Although the implications of these changes will not be clear until they are tested in the courts, demand has already increased for properly performed data collection and digital forensics investigations.

PRIVILEGED DOCUMENTS AND CLAWBACK AGREEMENTS

During the discovery portion of court proceedings, it is necessary to produce information to opposing counsel, some of which may contain privileged information. In general, a lawyer's work on a case is protected by the work-product privilege as are attorney-client communications. The work-product privilege means that any documents prepared in anticipation of litigation or for trial by a party's representative enjoy a qualified immunity from discovery. Other such privileges include doctor/patient, priest/penitent, and husband/wife. To prove to the court that information is privileged, the party claiming privilege must show that the communication: (1) was made with an expectation of confidentiality, (2) is essential to a socially approved relationship or purpose, and (3) has not been waived by disclosure of the contents of the communications to persons outside of the relationship.

The initial stage of any evidence collection is the discovery phase. For civil cases, this often involves a variety of conferences between attorneys, sometimes involving the judge, to determine what exactly will be collected. When documents containing privilege are contained on a device to be collected, the scope of information to be investigated is typically restricted. In civil cases, it is common for consent to be given to collect a digital device.

Traditionally, the documents produced in response to discovery are presented in paper form. The privileged

information is removed, or "redacted," using two methods: "blackout" or physical removal. The blackout method involves using a black marker to conceal portions of a document that are considered privileged. The physical removal method involves selecting documents from a group of papers and removing them from the set. Depending on the court's requirements, this may necessitate marking the exact location from which the document was removed.

The same set of concerns exists for privileged information on electronic storage devices, but no standard method of digital redaction has been adopted by the legal community. Computerized methods that mimic the blackout process exist, as do those for mimicking the physical removal method (NSA, 2006; NIST, 2005). The latter typically involves collecting all readable documents from a computer and selecting the items to redact. While electronic blackout and removal methods can sanitize a document or set of documents on an electronic device, they do nothing to redact logical copies or copied fragments of the document that remain (Manes et al., 2007; Manes, Watson, Barclay, Greer, & Hale, 2007). It is increasingly necessary to produce the entire contents of computer disks and other electronic storage devices as evidence, and the redaction of entire files from such a production introduces an entirely separate set of privilege issues.

Due to the extensive scope of privilege reviews on electronically stored information, some parties are entering into "clawback" agreements. Such 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 penalty. Generally, such agreements must include a third party to ensure maximum effectiveness; this is an important distinction for corporate technical personnel to heed. Much like current redaction methods, this is a temporary solution to the general problem of removal of privileged documents from electronic production for which there is no clear solution at this time. Digital forensics specialists may be key players in clawback agreements in order to facilitate reviews and exchanges.

CONCLUSION

The amount of knowledge necessary to thoroughly perform the duties of a security professional are expanding and now encompass many of the basic tenants of digital forensics. As such, information security personnel must be versed in the handling of digital information as if it were evidence, since the majority of commercial lawsuits involve such data. The broadening scope of information retained in a corporate setting as well as the complex storage and use of such data complicate the preservation and production of digital data. The court's requirements continue to shift as case law refines the process of electronic discovery. However, familiarity with the legal and technical components of digital evidence as well as the applicable national and international laws can help security and information technology personnel effectively handle situations where this information must be preserved and produced.

REFERENCES

American Bar Association. (2005). ABA Digital Evidence Project Survey on Electronic Discovery Trends and Proposed Amendments to the Federal Rules of Civil Procedure, Preliminary Report.

American College of Forensic Examiners. (2008). "Forensic Certification Programs." Available from: http://www.acfei.com/forensic_certifications/

Arkansas Private Investigators and Private Security Agencies Act ACA §17-40-101 – 107.

Berkowitz, P. (2009). "International E-Discovery: A Clash of Cultures and Law." The Discovery Standard Discovery News, Lexis-Nexis. Available from: http://law.lexisnexis.com/litigation-news/articles/article.aspx?article= Dr9lQl1LhoY=

Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc., 2005 WL 679071 (Fla. Cir. Ct. March 1, 2005).

Cook, B. (2009). "Why Cross Border Litigation is a Compliance Concern." Available from: http://www.s-ox.com/dsp_getFeaturesDetails.cfm?CID=2509

Daubert v. Merrell Dow Pharmaceuticals (92–102), 509 U.S. 579 (1993).

Devey, C. (2008). Electronic discovery/disclosure: From litigation to international commercial arbitration. The International Journal of Arbitration, Mediation and Dispute Management, 74(4), 375.

Federal Rules of Civil Procedure. (December 2007).

Flynn, N. (2004). "2004 Workplace E-Mail and Instant Messaging Survey." Available from: http://www.epolicyinstitute.com/survey/index.asp

Fulbright and Jaworski LLP. (2006). "Third Annual Litigation Trends Survey Findings." Available from: http://www.fulbright.com/mediaroom/files/2006/FulbrightsThirdAnnualLitigationTrendsSurveyFindings.pdf

Gorelick, J., Marzen, S., and Solum, L. (2001). Destruction of evidence. New York: Aspen Law & Business Publishers.

International Society of Computer Forensic Examiners. (2009). "Certified Computer Examiner." Available from: http://www.isfce.com

Manes, G., Watson, L., Downing, E., Barclay, A., Greer, D., and Hale, J. (2007). Proceedings from the 8th Annual IEEE SMC Information Assurance Workshop '07: A Framework for Redacting Digital Information from Electronic Devices, West Point, New York.

Manes, G., Watson, L., Barclay, A., Greer, D., and Hale, J. (2007), Proceedings from the ADFSL Conference on Digital Forensics '07: Towards Redaction of Digital Information from Electronic Devices, Arlington, Virginia.

Michael G. Kessler and Associates. (2008). "Computer Forensics and Forensic Accounting Licensing Survey Results." Available from: http://www.investigation.com/surveymap/surveymap.html

National Institute of Standards and Technology. (2005). "Computer Forensics Tool Testing (CFTT)." Available from: http://cftt.nist.gov
National Security Agency. (2006). "Redacting with Confidence: How to Safely Publish Sanitized Reports Converted From Word to PDF." Available from: http://www.nsa.gov
New Zealand Parliament Bills Digests. (2008, July). "Privacy (Cross-border Information) Amendment Bill." Available from: http://www.parliament.nz/en-NZ/PubRes/Research/BillsDigests/a/e/a/48PLLawBD16301-Privacy-Cross-border-Information-Amendment-Bill-2008.htm
Organisation for Economic Co-Operation and Development. (2008). "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data." Available from: http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
Prudential Insurance Co. of America Sales Practices Litigation. (N.J.D. 1997) 169 F.R.D. 598,604, 615.
Rasch, M. (2006). "Forensic Felonies." Available from: http://www.securityfocus.com/columnists/399
Ryan, D. and Shpantzer, G. (2002). Legal aspects of digital forensics. Washington, DC: The George Washington University.
Scheindlin, S. and Wangkeo, K. (2004). "Electronic Discovery Sanctions in the Twenty-First Century." Available from: http://www.mttlr.org/voleleven/scheindlin.pdf
Texas Department of Public Safety. (2007). TXDFP Private Security Bureau: Administrative Rules.
The State of Oklahoma Statutes. (2007). Title 59, Section 1759.1.
UK Information Commissioner's Office. (2007, December). "Data Protection Powers and Penalties: The Case for Amending the Data Protection Act 1998." Available from: http://www.ico.gov.uk/upload/documents/library/corporate/detailed_specialist_guides/data_protection_powers_penalties_v1_dec07.pdf
United Nations. (1948). "The Universal Declaration of Human Rights." Available from: http://www.un.org/Overview/rights.html
U.S. House Judiciary Committee. (2006). Federal Rules of Evidence, Article VII, Rule 702. Washington, DC: U.S. Government Printing Office.
Zubulake v. UBS Warburg (S.D.N.Y. 2002–2005).

BIOGRAPHIES

Gavin W. Manes, Ph.D., is the president and CEO at Avansic. His technical interests include information security, digital forensics, and telecommunications security. Manes has a Ph.D. in Computer Science from the University of Tulsa.

Elizabeth Downing is the technical writer at Avansic. She has been widely published in the fields of digital forensics and information assurance in journals, conference proceedings, book chapters, and magazines.