Proceedings of the 14th Colloquium for Information Systems Security Education
Baltimore Marriott Inner Harbor
Baltimore, Maryland June 7 - 9, 2010

Harsh Realities 101- Augmenting Information Assurance with Legal Curricula

Alan Katerinsky, H. Raghav Rao, PhD, and Shambhu Upadhyaya, PhD., *State University of New York at Buffalo*

Abstract – Interdisciplinary collaborations are transforming the way we learn and the way we teach. This article is about expanding the congruent and often overlapping domains of Information Assurance and the Law. While IA curricula pay some heed to the effect of legal matters on security procedure and outcome, the curriculum has been heavily focused on computer science and management information systems. Through greater co-operation we feel that IA curricula may gain tremendous enrichment and increased understanding, not only of the Law, but of issues central to IA.

Index terms – E-discovery, E-disclosure, ESI, Spoliation, Chain of custody, Information Assurance curriculum

I. Introduction

A. Issues and Domains

Information Assurance curricula have, to this point, been an extension of technical training in either Computer Science or Management Information Systems. Introductory curricula offered at SANS Institute, for example, and many management schools have concentrated on preparing students for the Certified Information Systems Security Professional (CISSP) exam, though this is often not the case with Computer Science curricula. Much of the subject matter of subsequent coursework seems geared to this goal.

The CISSP is generally accepted to be the "gold standard" certification in the field of Information Assurance and its contents are regulated by the not-for-profit International Information Systems Security Certification Consortium, commonly known as (ISC) ². It is therefore natural to concentrate on its requirements as the core of the basis for a course of study. The (ISC) ² enumerates their 10 Domains for the CISSP as:

- Access Control Systems & Methodology
- Applications & Systems Development
- Business Continuity & Disaster Recovery Planning
- Cryptography
- Law, Investigation & Ethics
- Operations Security (Computer)
- Physical Security
- Security Architecture & Models
- Security Management Practices
- Telecommunications & Network Security [1]

From this listing we can see that legal matters have not been ignored, and it is easy to understand where one domain might not have its due emphasis among so many others. It is, however, important to realize that legal matters are pervasive in dealing with any and all of the other domains and thus deserves special attention in the construction of the IA curriculum.

Many aspects of Information Assurance rely on legal underpinning, and have legal consequences that intersect with both technical and management concerns. Access control management, for example, depends on the ability of an organization to create and enforce acceptable use policies, and to notify users of their rights under that policy through warning banners upon logging in to the system. Physical security may involve the Fourth Amendment rights of a trespasser against unreasonable search and seizure. Due the interconnectedness of the worldwide communications, the field of Network Security may involve international law and jurisdictional disputes, as a network attack may originate from any country in the world with telephone service.

It is to one area we will devote particular attention in this paper, that of Investigation. We are most concerned with one of the consequences of technology as it has influenced the practice of law, that of Digital Forensics particularly in the civil realm. Digital forensics involves obtaining and analyzing digital information as evidence in civil, criminal, or administrative cases [2]. Many IA curricula offer a Digital Forensics course and some offer an entire course of study.

To refine the scope of inquiry more narrowly we can say that Computer Forensics is concerned with data that can

Alan Katerinsky is a recipient of the prestigious Scholarship for Service grant from the National Science Foundation. Dr. Rao is the Director of the Information Assurance program at UB's School of Management. Dr. Upadhyaya is the director of the Center of Excellence in Information Systems Assurance Research and Education

be retrieved from a computer's hard disk or other storage media. This often entails specifically recovering data that users have hidden or deleted and using it as evidence [3]. It is this evidence that is most often required in the civil realm as part of electronic discovery, or e-discovery.

II. The Problem at hand

One of the first concerns of any computer forensic investigation is the fragility of the evidence. Digital evidence is the most easily compromised of any evidence type. In criminal cases these investigations are usually done by law enforcement professionals, specially trained for the task. Any IA curriculum that trains those outside of law enforcement needs to impart a high level of legal awareness, in order to safeguard their work in the civil realm as well.

Modern operating systems perform hidden record keeping in the background every time a computer is started, with dates at a minimum being changed every time. Special equipment must be used to prevent a suspect's drive from being altered, and a special copy is made to work from. The original drive is then isolated in an evidence bag and stored in a locked facility. As with physical evidence it is vital to maintain records of the chain of custody. All investigations in a criminal investigation are performed on a forensic copy of the suspect's drive, identical down to the bit level, to preserve the integrity of the original.

The fragility of the evidence is vital in civil cases as well, but unfortunately often the investigator is a junior legal counsel, who does not understand that merely by accessing files, they are altered. Applications also perform record keeping on files, with the minimum change being the last modified date. Penalties for mishandling this kind of evidence are staggeringly large as we will see later on.

A. What is E-discovery?

Civil litigation in the United States is based on the idea that the parties should not be subject to surprises at trial [4]. Discovery is the pre-trial process during which each party can request documents and other evidence from other parties. It is part of the Federal Rules of Civil Procedure amended in 2006 to include provisions for electronic discovery [5].

Electronic discovery is the identification, preservation, collection, processing, review and distribution of Electronically Stored Information (ESI) associated with legal and government proceedings [6]. It differs from traditional means of discovery chiefly because of its intangible form, volume, transience and persistence. ESI is also accompanied by metadata, information about the file itself. Some experts will say that in cases of suspected spoliation, the metadata is more important than the data that was lost. Metadata is not present in paper documents, but paper can be scanned in and the resulting image file would contain metadata [7].

Most e-discovery events (criminal, civil and regulatory) target email and electronic documents and require massive amounts of time to find, index, manage, review and produce information [8]. The scope of the issue can be expected to increase over time, as a recent report by the research firm Gartner Inc. which estimates that spending on e-discovery software and services is forecast to increase by 21% annually for the next 3 years [9].

ESI for e-discovery can reside on multiple devices. The most familiar locations are desktop and laptop computers, servers, and mainframes, but anything which can hold data is a possible source. USB thumb drives, Personal Digital Assistants (PDAs), CD-ROMs, DVD-ROMs, MP3 players, Blackberries, smart cell phones, backup tapes, flash memory cards, other archive media and third-party storage systems are all potential repositories of ESI.

The sheer volume of data is a factor recognized in other fields [10], but in e-discovery, it is the most salient feature. Information overload increases the complexity of the problem. Organizations do not know what information they have, where it is stored and what electronic objects should be kept or destroyed.

Because of all this, attorneys involved in case litigation may understand the companies they represent, but they seldom understand the policies and practices that are in place in the company's IT department [11]. The legal processes to halt a company's document destruction policy (called a legal hold) are not obeyed, potentially costing the company huge fines and possibly judgment against them in a court of law.

We believe that IA curricula should therefore express the severity of legal requirement, and enumerate the intricacies of the procedure, so that IT graduates don't catastrophically undermine their own organization.

Several landmark cases have set the rules by which e-discovery is judged, but due to the interests of editorial space, we will explore three of them.

B. Zubulake v. UBS Warburg LLC [12]

In 2003 United States District Court Judge Shira A. Scheindlin issued five groundbreaking opinions in this case, and assessed Warburg $20 million in punitive

damages. This decision helped establish a baseline for e-discovery practices in litigation. Most notable among these is the imposition of sanctions for the spoilation (or destruction) of electronic evidence. This case also expanded the concept of "legal hold." The obligation to suspend an organization's document destruction policy begins once litigation is "reasonably anticipated" and the order to suspend the policy must be issued immediately and periodically reissued. Furthermore, preservation duty must be communicated to "key players" and they must be periodically reminded of the suspension of the organization's normal document disposal policy.

This greatly increases the scope of a party's duty to preserve electronic evidence during the course of litigation, as well as legal counsel's duty to monitor their clients' compliance with electronic data preservation and production.

Also notable in this case are the first data sampling recommendations and guidelines, and the ability for the disclosing party to shift the costs of restoring "inaccessible" backup tapes to the requesting party.

C. Morgan Stanley v. Coleman

In 2005 this case was decided without fully reaching its merits [13], due in large part to the court's view on the relationship between the corporate client and outside counsel.

Morgan Stanley failed to disclose discovery of 1,400 backup tapes and admitted there was an error in its search program. The court found that Morgan Stanley had failed in its duty to preserve the electronic documents, and instructed the jury to draw an adverse inference, that Morgan Stanley deliberately destroyed evidence. The jury awarded US $850 million in punitive damages, which were overturned on appeal for other issues in 2007 [14].

The outcome was costly for the company and for the attorneys involved. The judge revoked Morgan Stanley's counsel's license, noting misrepresentations he made on Morgan Stanley's behalf regarding completeness of e-disclosure (overturned on appeal for separate issues, though this ruling stands), and also disqualified the outside law firm, forcing Morgan Stanley to instruct new counsel two weeks before the trial [15].

New rules in the amended FRCP require technical assistance in preparing initial disclosures and requests for production are aimed at avoiding situations like this in the future. Specifically, the judge was concerned about the backup tapes that were not disclosed in a timely manner, and the fact that attachments were not searched due to script error. Equally disturbing was the selection of data that was missed by the search engine due to "hyper" case sensitivity (i.e., Coleman would not be a hit if the search term was "coleman") [16].

D. Qualcomm Inc. v. Broadcom Corp. [17]

In this case because Qualcomm failed to produce over 46,000 e-mails and committed other discovery misconduct, they were ordered to pay costs of $8,568,633.24 for its "monumental and intentional discovery violation."

The judge said her review led "to the inevitable conclusion that Qualcomm intentionally withheld tens of thousands of decisive documents from its opponent in an effort to win this case and gain a strategic business advantage over Broadcom. Qualcomm could not have achieved this goal without some type of assistance or deliberate ignorance from its retained attorneys." In-house and former outside counsel were ordered to participate in comprehensive "Case Review and Enforcement of Discovery Obligations" (CREDO) program. Six of Qualcomm's outside counsels were referred to the State Bar of California for disciplinary proceedings [18].

The final indignity came when Qualcomm asserted attorney-client privilege over communications with counsel; since privileged communication is not subject to discovery they were at an extreme disadvantage in proving the level of client involvement. In effect, counsel could not defend themselves.

III. SOLUTIONS

A. Implications

The breakdown in communications in each of these cases could be attributed entirely to technical ignorance on the part of legal counsel, but that misses the point. The IT departments involved didn't inform counsel of these potential issues, most likely because they were *equally* ignorant of legal process, and had no understanding of the gravity of the situation, or the severity of consequences.

The stakes are high, and by now the legal profession must perceive themselves as stakeholders. In the afore-mentioned survey by Gartner, 48% of all Law firms were doing some in-house e-discovery function, and 26 % used services of an external firm that specializes in e-discovery [19].

We believe that Information Assurance education could bridge the gap between legal and technical in the workplace, by adding relevant Law courses into the curriculum.

Similarly, legal education could benefit from the introduction of Information Assurance electives, enriching the experience and preparing the student for a career that is becoming increasingly dependent on technology for its basic processes [20].

B. Certification

Most traditional schools (with notable exceptions such as Boston, Norwich and Capella Universities), continue to offer broad degree programs in computer science or information science, and might tend to be less receptive to the idea of offering a new curriculum such as BS or BA in Information Assurance.

What might be more attractive in such situations could be to offer a degree program with an option or concentration in IA. Furthermore, certification can be a viable alternative to launching a separate degree program. Each of these solutions has its attractions and drawbacks. A separate degree program allows academic focus, but might strain the resources of an institution with many prior commitments. The concentration model allows cross-listing with other departments, but might pose serious issues for a faculty concerned with department accreditation, as a possible dilution of their curricula.

At the University at Buffalo, designated as a National Center of Excellence in Information Systems Assurance Research and Education (CEISARE), our solution to the issue of interdisciplinary IA education takes the form of an Advanced Certification program [21].

The IA Certificate is designed to equip our students with a comprehensive understanding of the many facets of Information Assurance and Security. The program provides coursework giving a broad overview of the interdisciplinary aspects of Information Assurance as well as specialized training with respect to a chosen discipline.

This program structure ensures that students receiving this certificate possess the necessary foundation in Information Assurance as well as allows them a certain degree of freedom to tailor the Certificate to their interests. At present, there are four disciplines participating in the program in terms of the applicable courses they offer: Computer Science and Engineering (CSE), School of Management (SOM), Mathematics (MTH), and School of Law (LAW).

The Advanced Certificate is awarded upon completion of 14-15 credit hours of coursework, consisting of:

- 3 credit hours of the required integrative course, Information Assurance (MGS 650).
- 6 credit hours of required coursework defined by the track chosen.
- 5-6 credit hours of elective coursework limited to departmentally approved courses.

Within the Advanced Certificate program, students may elect to follow one of two paths: Technical versus Managerial. The program of study follows from the option chosen. The Technical track is defined by the Computer Science and Engineering department; whereas the Managerial track is defined by the Management Science and Systems department.

In addition to the integrative course - Information Assurance, students must take two from a set of three core courses, based on the track chosen. The 6 credits of coursework fall into two options:

Technical Track:
Introduction to Cryptography;
Applied Cryptography and Computer Security; Computer Security; Wireless Networks Security

Managerial Track:
Network Management; Seminar in E-Commerce

The remaining two or more courses are taken from the list of approved electives to make up the total of 14-15 credit hours:
Fundamentals of Programming Languages; Operating Systems Internals; E-Commerce Technology; Computer Communications; Database Systems; Modern Networking Concepts; Multiagent Systems; Applied Cryptography and Computer Security; Data Mining; Intellectual Property; Legal and Cultural Issues in Cyberspace; Fraud Prevention and Detection; Database Management Systems; System Analysis and Design; Digital Forensics; Intellectual Property; Introduction to the Theory of Numbers I/II; Stream Ciphers

The choice of tracks and number of credits required are chosen with the express intent of enriching, but not impeding a normal degree-granting course of study. It is conceivable that the Certificate may be obtained with a minimum of courses outside the degree major, and students applying for the certification are encouraged to explore subjects outside their discipline. Yet, we feel there is room for growth and greater interaction with the School of Law, adding courses as best fits teaching schedules, and availability of resources. Plans have begun for a third, legal track to accompany the managerial and technical, though the idea is still in the talking stages, and no formal proposals have been submitted. Considering the vital need for IA training in legal practice at large [22], we feel that greater integration may yield spectacular

results in terms of the career capabilities for graduates in the near future.

IV. Lessons learned

A. One student's interdisciplinary experience

Students engaged in the Advanced Certificate program often remark on the enlarged perspective they have obtained. One student in particular used his experience in a course on Intellectual Property to co-ordinate with his class in Digital Forensics. In this he was able to answer real world questions posed by a copyright case celebrated in the news because it involved the President of the United States [23].

Shepard Fairey, controversial graffiti artist who produced the iconic poster for the 2008 Obama campaign is suing the Associated Press for his right to use a photo as the basis for his artwork. In October of 2009 he changed his pleading and was counter-sued by the Associated Press and the case is still pending at the time of this writing.

Leveraging knowledge gained in both, the student produced a presentation that answered common questions, for example:

- One of the oddest facts about the case is that Fairey admits to using a photograph shot by AP photographer Manny Garcia, but denied using the one that AP claimed he did. Why does it make any difference what photo he used?
- What made him change his pleading after eight months of declaring that the AP had it all wrong?
- Why did he sue AP for rights of Fair Use in the first place?

The presentation, prepared for use in the Digital Forensics course, detailed what the student had learned about copyright, the rules of civil procedure, e-discovery and the connection to Forensic software.

After a successful presentation in the Forensics Course, the student realized that the Intellectual property course might like to see this as well, but lacked the technical expertise to appreciate his conclusion. He then added slides to the presentation, giving background that the Law students lacked and in so doing created a general purpose presentation, which could be understood by students in either course, or indeed students who had not taken *either* course.

Entitled *Ghost at the Feast*, the presentation takes its name from Shakespeare's *Macbeth*. Banquo's ghost appears during a banquet at the Forres castle. Earlier in the play Macbeth has had Banquo murdered, and the ghost is a manifestation of Macbeth's guilty conscience. Over the years, the ghost at the feast has become a metaphor for unresolved issues.

The first portion of the student's presentation give some general legal background as to what a civil trial is about; including rules that direct how evidence is accepted into court. The next twelve slides give some background about the field of Digital Forensics and how information is retrieved from copies of hard drives. The next section of the student's presentation details the law of copyright, and the doctrine of fair use.

The doctrine of fair use has developed through a substantial number of court decisions over the years, and has been codified in section 107 of the Copyright Act of 1976 (title 17, U. S. Code) [24].

The distinction between fair use and infringement may be unclear and not easily defined. There is no specific number of words, lines, or notes that may safely be taken without permission [25].

Fairey's case was so compelling that the Fair Use Project of Stanford University offered to represent him.

Section 107 sets out four factors to be considered in determining whether a particular use is fair:

1) The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes,
2) The nature of the copyrighted work,
3) The amount and substantiality of the portion used in relation to the copyrighted work as a whole,
4) The effect of the use upon the potential market for, or value of, the copyrighted work.

The key question in this case appears to be 3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole. Or put another way; is the work derivative or transformative?

A derivative work is an expressive creation that includes major, copyright-protected elements of an original, previously created first work [26]. Transformative works are judged by how much the copied work changes the original? Is it creative enough to qualify for its own copyright [27]? If so the work is transformative and is more likely to be judged a fair use of the copyrighted material.

The concluding section of the student's presentation speaks to the particulars of the case at hand. To answer the question if it makes a difference what photo was used,

we need to look at the photos involved. In the one that Fairey claims was his model, then-Senator Obama was shown as seated at a table with George Clooney. The set of his head, the angle of his face all differ noticeably from the colored poster that Fairey produced for the 2008 campaign. One could make a reasonable claim that the amount of work involved qualified as transformative and therefore fair use. If, on the other hand, it could be shown that Fairey used the photo taken minutes later at the same event, in which the subject looks nearly identical to the image on the poster, then the image is arguably derivative and AP's copyright has been infringed.

The connection between law and technology becomes apparent at the point when Mr. Fairey decided to change his pleading.

In a letter on October 9, 2009, Fairey's attorneys informed AP they wanted to amend their pleadings, and said that they "no longer contend that the Clooney Photograph was used in the creation of the Obama Hope poster" and, in fact, admitted Fairey used the Obama photo AP claimed was used.

They also informed AP that Fairey created new documents claiming use of the Clooney photo after he had filed his original complaint, and that Fairey also attempted to delete key documents about which photo he had used.

Fairey's lawyers concede that the certain documents designed to support Fairey's claim were created by the artist after he filed his suit. The letter went on to tell AP that statements made about the existence of some of Fairey's files addressing the Obama illustration "now appear to have been inaccurate." [28]

So to answer the question; why would he change his pleading, we can conjecture along the following lines. From the admissions of October 9, it becomes clear that Fairey was admitting to tampering with evidence that could easily have been recovered during the e-discovery process and verified by forensic investigation. The change was therefore made in reasonable expectation of being caught obstructing justice, by the spoliation of ESI. It may be bad to admit you're a liar, but it is infinitely worse to have it proven in a court of law.

It was also at this point that Fairey's Lawyers from Stanford's Fair Use Project withdrew from the case, claiming he misled them.

The student's presentation concludes with an update from November 19. The court made clear that it considers spoliation and fabrication of evidence very serious, with Judge Hellerstein saying that in his career he had "never seen anything like this." He ruled that AP may depose not only Mr. Fairey, but also his former counsel and their electronic discovery vendor, regarding the destruction of evidence.

As to why he brought the suit in the first place, the student conjectured that it was a pre-emptive strike to avoid a suit from the AP. From a study of fair use, it might be argued that, had Fairey not tampered with his evidence, he might have won the case on First Amendment grounds. The campaign poster was obviously political free speech, and with the legal talent of a major university behind him, he might have thought he could not lose. These arguments became less compelling when he admitted to spoliation of the ESI. In fact, at this time his suit's chances don't look good at all. The Associated Press website expresses their outrage and intends to vigorously pursue its own countersuit, alleging that Fairey willfully and blatantly violated AP copyright [29].

Because of the IP Law course, this MIS student was able to connect separate courses of study, and provide a coherent narrative that might otherwise have been puzzling without the interdisciplinary experience. How many more puzzles might be solved, once the study of legal issues is even broader and more readily available?

V. Conclusion and Future Direction

A. An IA curriculum needs to bring in issues of law in a major way.

According to National Center for Education Statistics [30] a curriculum search for intuitions that offer "Computer and Information Systems Security" yields a list of 286 total programs, 65 of which offer Certificates, 87 offering Associates, 120 Bachelor and 25 Advanced degrees. Unfortunately these numbers do not tell the whole story. Anecdotally, the experience among educators in Information Assurance is that curricula throughout the nation are overwhelmingly balanced towards education in systems and computer science. Statistics as to how many and which programs offer courses that deal in legal issues are not readily available. Our first conclusion is that detailed data needs to be collected to assess the level of legal education involved in those curricula.

While education in systems is vital for students of IA, the level of demand in the legal profession for IA trained graduates, specifically in the areas of Investigation and e-discovery is potentially enormous. We feel that new courses, targeted at that need, should be composed and offered in the IA curriculum. These courses would need both consultation and cooperation from technical,

managerial and legal components of educational institutions involved.

Since the curriculum must cover so many topics, another option would be to include legal modules to the existing courses, rather than adding more legal courses into the IA certificate. Thus avoiding the question of what to remove, but requiring redesign of the current curriculum to incorporate those topics.

B. The IA legal curriculum should draw inspiration from established industry expectations.

In order to align course offerings with the current requirements, we feel that some sort of external framework in industry best practices be the basis for targeted skills and competencies. Two main sources we recommend for those requirements are the Sedona Conference [31] and the Electronic Discovery Reference Model (EDRM) [32].

According to their Mission Statement, The Sedona Conference "exists to allow leading jurists, lawyers, experts, academics and others, at the cutting edge of issues in the area of antitrust law, complex litigation, and intellectual property rights, to come together - in an effort to move the law forward in a reasoned and just way [33]."

The Sedona Guidelines, publications freely available and organized by topic at their website, are a series created by work groups on specific issues, such as "Best Practice Guidelines & Commentary for Managing Information & Records in the Electronic Age [34]". The site is a wealth of information, and has the advantage of being easily accessible to students at no cost.

Similarly, the Electronic Discovery Reference Model website states that: "EDRM's core objective is to improve the electronic discovery process for everyone involved. EDRM seeks to achieve this objective by establishing guidelines, setting standards, and delivering resources [35]." EDRM also publishes guidelines, standards, whitepapers, research materials, Webinars, news, data sheets and other items. These materials are free for download from their website as well [36].

Some authors caution readers to remember that these organizations were originally formed to produce guidelines. Their publications, such as the EDRM frameworks, have unfortunately become regarded as strict manuals. The problem with that approach is that guidelines adapted to manuals often don't fit many practitioners' specific work processes, and lose credibility over time [37]. However, because both of these resources are composed of working groups, they can be responsive to industry feedback and update the information they provide as technology and other requirements change.

Forrester Research predicts the e-discovery industry, will reach $5 billion by 2011, and is changing at a rapid rate that shows no signs of slowing [38]. It is possible, even likely, that IA graduates will seek positions in the IT departments of specialized firms and eventually average law firms, as the demand for e-discovery trickles down to smaller and smaller cases. More software choices, cloud computing rapid advancement and social networking will likely drive demand for trained professionals to new levels. The IA curricula should be ready to meet that demand with graduates trained in legal issues, or we are doing those graduates an enormous disservice.

VI. Acknowledgments

This research has been supported in part by National Science Foundation Grant No. DUE-0830814. The usual disclaimers apply.

VII. References

[1] "*CISSP Education & Certification*". (ISC)². 2009. https://www.isc2.org/cissp/default.aspx. Retrieved March10, 2009.

[2] Nelson, Phillips, Enfinger, Steuart, *Guide to Computer Forensics and Investigations*, Course Technology, 2008

[3] Ibid.

[4] Wikipedia, *Federal Rules of Civil Procedure*, http://en.wikipedia.org/wiki/Federal_Rules_of_Civil_Procedure, Retrieved March 11, 2010

[5] Cornell University Law School- *Federal Rules of Civil Procedure, Depositions and Discovery> Rule 26* http://www.law.cornell.edu/rules/frcp/Rule26.htm Retrieved March 11, 2010

[6] Mack, Mary, ESQ. (2008), *A Process Of Illumination: The Practical Guide To Electronic Discovery*, p.11 Fios Inc

[7] Wikipedia, *Electronic Discovery*, http://en.wikipedia.org/wiki/Electronic_Discovery Retrieved March 11, 2010

[8] Moerdler Mark, *The True Cost of E-Discovery*, Information Management Newsletters, February 18, 2010 http://www.information-management.com/newsletters/the_true_cost_of_e-discovery-10017179-1.html

[9] Langenkamp, Julie; *Snapshot on E-Discovery*, Information Management Newsletters, February 18, 2010 http://www.information-management.com/newsletters/e-discovery_matures-10017175-1.html

[10] "*How Much Information*", 2003. Retrieved from http://www.sims.berkeley.edu/how-much-info-2003 on march12, 2010.

[11] Wikipedia, *Electronic Discovery*, http://en.wikipedia.org/wiki/Electronic_Discovery Retrieved March 11, 2010

[12] Zubulake vs. UBS Warburg LLC, No. 02 Civ. 1243, 2003 WL 21087884 (S.D.N.Y. May 13, 2003)

[13] Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005) ("Morgan Stanley I"), rev'd on other grounds, Morgan Stanley & Co.Inc. v. Coleman (Parent) Holdings Inc., 955 So.2d 1124 (Fla. Dist. Ct. App. 2007)

[14] Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., No. CA 03-5045 AI, 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005) ("Morgan Stanley II").

[15] Walwyn, Frank E. (2008), *Electronic Disclosure-The Coming Challenges* (given as part of the International Commercial Litigation Training Programme), Judicial Education Institute Tortola, B.V.I.

[16] Mack, Mary, ESQ. (2008), *A Process Of Illumination: The Practical Guide To Electronic Discovery*, p.72 Fios Inc

[17] Qualcomm Inc. v. Broadcom Corp., 2008 WL 66932 (S.D. Cal. Jan. 7, 2008)

[18] Walwyn, Frank E. (2008), *Electronic Disclosure-The Coming Challenges*

[19] Langenkamp, Julie; *Snapshot on E-Discovery*, Information Management Newsletters, February 18, 2010 http://www.information-management.com/newsletters/e-discovery_matures-10017175-1.html

[20] Talley, Ursula, *Successful E-Discovery Starts with a Strong Foundation*, Information Management Newsletters, January 19, 2010 http://www.information-management.com/newsletters/metadata_search_ediscovery-10016891-1.html

[21] Details available at the University at Buffalo website: http://www.cse.buffalo.edu/caeiae/advanced_certificate_program.htm).

[22] Sloan, Karen, *Firms Slow to Awaken to Cybersecurity Threat,* The National Law Journal, March 09, 2010 http://www.law.com/jsp/lawtechnologynews/PubArticleLTN.jsp?id=1202445899467&Firms_Slow_to_Awaken_to_Cybersecurity_Threat

[23] AP: *The Shepard Fairey Case*, Retrieved March 12, 2010. http://www.ap.org/iprights/fairey.html.

[24] http://www.copyright.gov/title17/

[25] http://www.copyright.gov/fls/fl102.html

[26] Kalem Company v. Harper Brothers, 222 U.S. 55 S Ct. 20, 56 L.Ed. 92

27 Cleanflicks of Colorado, LLC v. Soderbergh, USDC 433 F. Supp 2nd 1236 (2006) and Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994)

[28] AP: *The Shepard Fairey Case*, Retrieved March 12, 2010. http://www.ap.org/iprights/fairey.html.

[29] Ibid.

[30] National Center for Education Statistics, http://nces.ed.gov. Data retrieved March 12, 2010

[31] The Sedona Conference, http://www.thesedonaconference.org/. Retrieved 3/11/2010

[32] EDRM – the Electronic Discovery Reference Model http://edrm.net/joining-edrm/frequently-asked-questions

[33] The Sedona Conference, *Mission Statement*, http://www.thesedonaconference.org/content/tsc_mission/show_page_html. Retrieved 3/11/2010.

[34] The Sedona Conference, *Publications,* http://www.thesedonaconference.org/content/miscFiles/publications_html?grp=. Retrieved 3/11/2010.

[35] EDRM – the Electronic Discovery Reference Model http://edrm.net/joining-edrm/frequently-asked-questions

[36] EDRM – the Electronic Discovery Reference Model, Resources, http://edrm.net/resources. Retrieved 3/12/2010.

[37] Balachandran, Bobby, *E-Discovery's Call to Action*, Information Management Newsletters, February 18, 2010 http://www.information-management.com/newsletters/e-discoverys_call_to_action-10017178-1.html. Retrieved 3/12/2010.

[38] Ibid.