The Rules of Digital Evidence and AccessData Technology

A White Paper from AccessData Group

AccessData®

Contents

Authors

Tim Leehealey *CEO of AccessData.*
Esther Lee *General Counsel of AccessData Group.*
Will Fountain *Associate General Counsel of AccessData Group*

Editors

Devin Krugly
VP of Marketing and Business Development, AccessData Group

Caitlin Murphy
Director of Legal Marketing, AccessData Group

Introduction

This document is for users of AccessData software who wish to understand the technology and case law that supports the introduction of electronically stored evidence ("ESI") that is seized/discovered and analyzed with our products in a court of law. This document is not intended as a legal reference. Consequently, we will spend a limited amount of time detailing the basic background information relevant to the general topic of digital evidence and computer forensics.

For the sake of simplicity, one can arrange the rules relevant to ESI into two basic groups. The first, and arguably more foundational group, is the Federal Rules of Evidence ("FRE") and more specifically the way they have been interpreted by courts to accommodate digital evidence. The second group consists of the much more recent and specific amendments to the Federal Rules of Civil Procedure ("FRCP"), which significantly impact every large U.S. and multinational company.

The Federal Rules of Evidence

Digital Evidence presented significant challenges when it first began to appear in courts. Digital evidence presents problems since it is fundamentally different from physical evidence, around which the FRE were predicated. Specifically, the challenges presented by digital evidence are due to following differences:

Degradation

In the world of physical evidence there is some basic acceptance that if a gun is found at the scene of a crime and is handled correctly, that will be the same gun at the point of trial. To the extent that physical evidence does change with time, it is generally accepted by the courts that those changes are immaterial to the relevance of the evidence. The same cannot be said in general about digital evidence. Digital evidence is by its very nature volatile. It is not uncommon for a single bit within a large file to get altered over time, and the resulting effect on the entire document can actually be fairly large (Note: degradation applies to the storage media itself).

Ownership

It is quite difficult to determine ownership of a digital document. While it may be possible to determine on which physical machine a document was found, given the current technical realities associated with shared computer resources, networked computers, and virtual machines, knowing which machine on which a document was placed is not always sufficient to prove who authored the document.

Original Documents

It is nearly impossible to distinguish an original document from copies of it. At the most basic level, all digital documents are simply a series of zeros and ones that are interpreted by the computer. Two documents containing the exact same string of zeros and ones are in every sense identical, and there is no way to determine which was created first or who created it without additional information.

These three crucial differences, as well as the subtleties associated with them, served as the impetus for the courts to essentially re-interpret the FRE in order to more clearly accommodate digital evidence. At a fundamental level, this re-interpretation required dealing with two basic evidentiary issues, Authenticity and the Best Evidence Rule.

Authenticity

For any computer record or other evidence to be admissible against a defendant, the proponent must show that the offered evidence is authentic by producing evidence sufficient to support a finding that the record is what the proponent claims it is.[1] The standard for determining the authenticity of a computer record is no different than authenticating any other record. However, the disparity lies in the inherent qualities of a computer record where the courts have stated that

1 FRE 901

"the complex nature of computer storage calls for a more comprehensive foundation."[2] The need for a more comprehensive foundation has given rise to a number of challenges to the admissibility of digital evidence over the last two decades that fall into three basic categories:

1) The computer-generated or computer-stored records were altered, manipulated, or damaged after they were created;
2) The reliability of the computer program that generated the computer record; and
3) The reliability of the identity of the author.

Fortunately, countless cases over the last two decades have provided significant precedent regarding each of these basic challenges. There is a now-classic opinion detailing the authentication process of ESI, namely Chief Magistrate Judge Paul W. Grimm's 102 page opinion in *Lorraine v. Markel Am. Ins. Co*.[3] Of the several points made in the opinion, the court ruled out ESI as hearsay, extra-judicial statements made by a declarant offered to prove the truth of what the matter asserts if anything, which are inadmissible in court unless it falls into the hearsay exceptions. Conceptually, one could argue ESI as hearsay, since it is not a statement made in court and is offered for the purposes mentioned above. However, hearsay must be a statement made by a person and therefore the court found that it does not fall under the hearsay definition. The Lorraine opinion struck lighting on both sides for respective counsel's lack of foundation and preparation for admitting ESI and is recommended reading for all attorneys who must admit ESI into evidence.

Data Alteration

In regard to challenges based on the premise that the data was altered, the courts offer extensive guidance. First, absent specific evidence that tampering occurred, the mere possibility of tampering does not affect the authenticity of a computer record. A challenge that the offered evidence was tampered with or altered requires evidence to show that it was tampered with or altered. Merely showing that a better method is available is insufficient.[4]

In addition to the question of alteration, the court has also addressed questions surrounding evidence acquisitions. Specifically, the court has generally found that if an investigator can testify to the process used to acquire digital evidence and show that it is in keeping with current best practices, then the evidence is admissible. This exact question was addressed in *Bone v. State*[5], and the court found that the investigator's testimony regarding how he had acquired the evidence, the steps he took to protect the validity of the evidence, and the process he had used to analyze the evidence was sufficient to establish the authenticity of that evidence.

Reliability of the Program

Secondly, FRE 901(b)(9) requires that "matters created according to a process or system can be authenticated with "evidence describing a process or system used...and showing that the process

2 *United States v. Scholle*, 553 F.2d 11¬¬09, 1125 (8th Cir. 1977).
3 *Lorraine v. Markel Am. Ins. Co.*, 241 FRD 534 (D. Md. 2007).
4 See, e.g., *United States v. Glasser*, 773 F.2d 1553,1559 (11th Cir. 1985) (the "fact that it is possible to alter data contained in a computer is plainly insufficient to establish untrustworthiness.")
5 *Bone v. State*, 771 N.E.2d 710, 716 (Ind. Ct. App. 2002) (reviewing whether data from defendant's computer was sufficiently authenticated).

or system produces an accurate result." The authenticity of the computer record is balanced by the reliability and accuracy of the computer program that created the record. The burden of proof is on the party introducing the evidence. As long as that party provides "sufficient facts to warrant a finding that the records are trustworthy and the opposing party is afforded an opportunity to inquire into the accuracy thereof and how the records were maintained and produced, a proper foundation has been established."[6] Reliability can be established by showing that the program is used on a regular basis, such as in the ordinary course of business. Showing that the computer record is one that is normally retrieved, kept, or made in the routine of business operations shows a higher degree of trustworthiness.

Challenges based on reliability can occur when the evidence submitted is retrieved from complex accounting or order processing systems. For example, an employee who is embezzling money by altering a few numbers on an invoicing system might attempt to get the digital evidence thrown out by arguing that the evidence was created by an unreliable process, namely the accounting system. In essence, he could argue it was a system glitch that caused the error, as opposed to a prolonged and systematic scheme. In this case, the courts have generally agreed that if the prosecution can show the reliability of the system in terms of its ability to correctly process millions of other transactions, then the system is considered reliable and the evidence is therefore admissible.

The Reliability of the Identity of the Author

A third common challenge against the admissibility of computer records pertains to whether the purported author is indeed the author stated on the computer record or the one alleged to have made the record. Proving authorship and authenticity of such a computer record is shown either though testimony or through circumstantial evidence. When testimony regarding authorship is available, even in complex situations, it is generally sufficient to prove authorship. One of the best examples of testimony supporting authorship is the case of *United States v. Tank*[7]. At question in Tank, a child pornography case, was the authorship of Internet chat messages by defendant, the authorship of which is intuitively difficult because these messages are identified only through a self-defined username. In considering the authorship issue, the appellate court noted that in the context of FRE 901(a), the court can admit evidence if "sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity."[8] In addition, there needs to be a sufficient link shown between "the proffered evidence and the defendant."[9] To satisfy these requirements the government offered the testimony of other chat room participants and the computer server administrator. In Tank, the court accepted the testimony to serve as adequate foundational showing that the chat room printouts were authentic, stating it was "sufficient to allow a reasonable juror to find that the chat room log printouts were authenticated."[10] Courts considering the admissibility of electronic evidence frequently use this method.[11] It is necessary,

6 *United States v. Briscoe, 896 F.2d 1476, 1494 (7th Cir.1990) (citing United States v. Croft, 750 F.2d 1354, 1365 (7th Cir.1984) at n. 7)*
7 *United States v. Tank*, 200 F. 3d 627 (9th Cir. 2000).
8 *Id*. at 630.
9 *Id.*
10 *Id.* citing United States v. Catabran, 836 F.2d 453, 458 (9th Cir. 1988) ("Any question as to the accuracy of the printouts ... would have affected only the weight of the printouts, not their admissibility.").
11 See, e.g., *United States v. Kassimu*, 188 Fed. Appx. 264, 2006 WL 1880335 (5th Cir. 2006) (computer records authenticated by witness with

however, that the authenticating witness provide factual specificity about the process by which the ESI was "created, obtained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so, as opposed to boilerplate, conclusory statements that simply parrot the elements of the business record exception to the hearsay rule, Rule 803(6), or public record exception, Rule 803(8).[12]

FRE 901(b)(3) and (b)(4) also provide other methods to authenticate ESI. For example, FRE 901(b)(3) permits authentication by "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics, taken in conjunction with circumstances." FRE 901(b)(4) allows authentication through "circumstantial evidence."[13] Other methods include the following:

1) Showing that the document was obtained from a machine utilized either primarily or entirely by the author of the relevant document;
2) Showing that the file was surrounded by other files or emails also created by the author;
3) Detailing the author's other activities on the relevant machine when the relevant file was created; or
4) Showing that the file was in a restricted area accessible only by the author, such as an email in-box or password protected machine.

Certain identifying marks or data contained within or associated with the ESI may also enable identification. Two common examples are "hash values" and "metadata." A hash value is a unique numerical identifier that can be assigned to a file, a group of files, or a portion of a file. Hash values can be inserted into original electronic documents when they are created to provide them with distinctive characteristics that will permit their authentication under FRE 901(b)(4).[14] Metadata is another distinctive characteristic of ESI that can be used to authenticate under FRE 901(b)(4). It provides information about a particular data set by describing how, when, and by whom it was collected, created, accessed, or modified.

There is, of course, a multitude of additional ways to authenticate ESI, including reliance upon any "self-authenticating" characteristics of the ESI itself. In Lorraine, Judge Grimm noted that counsel must be "creative in identifying methods of authenticating electronic evidence when the facts support a conclusion that the evidence is reliable, accurate, and authentic, regardless of whether there is a particular example in Rules 901 and 902 that neatly fits."[15] In short, lawyers must be able to authenticate the ESI that they intend to use at trial. The standards of ESI authentication vary widely by venue. However Judge Grimm believes with time, all courts will adopt a more demanding approach.

Generally, it is only when dealing with purely Internet-based evidence provided by an Internet service provider ("ISP") that authorship can be truly difficult to prove. This is often the case when attempting to prove hacking and Internet theft activity. In those instances, there is usually

---

personal knowledge).

12 *Lorraine*, 241 FRD at 557.

13 See, e.g., *United States v. Siddiqui*, 235 F.3d 1318, 1322-23 (11th Cir. 2000) (authentication of email by circumstantial evidence such as the presence of defendant's work email address and use of the defendant's nickname in the e-mail).

14 *Lorraine*, 241 FRD at 557. See also United States District Court for the District of Maryland, Suggested Protocol for Discovery of Electronically Stored Information , available at http://www.mdd.uscourts.gov/news/news/ES I Protocol. pdf (encouraging parties to discuss hash values when producing electronic records in discovery to facilitate later authentication).

15 *Lorraine*, supra, note 2.

extensive additional circumstantial evidence, proof of facts offered as evidence from which other facts can be inferred, to prove authorship.

Best Evidence Rule

The second major issue digital evidence presents is that it violates the Best Evidence Rule. The Best Evidence Rule, also "referred to as the 'Original Writing Rule,' does not mandate introduction of the 'best' evidence to prove the contents of a writing, recording or photograph, rather it requires such proof by an 'original,' 'duplicate' or, in certain instances, by 'secondary evidence-any evidence that is something other than an original or duplicate (such as testimony, or a draft of a writing to prove the final version, if no original or duplicate is available."FRE 1002 states, "to prove the content of a writing, recording or photograph, the original writing, recording, or photograph is required, except as otherwise provided in these rules or by Act of Congress." Within the context of computer-generated data, FRE 1001(3) expressly states that data stored on a computer or similar device should be considered an "original." Conclusively, an "accurate" printout would be considered an original and therefore satisfy the Best Evidence Rule.

However the key word is "accurate." The Rule assumes that the printout has all the relevant data to conclude its information is complete and within its original context.[16] In *Armstrong v. EOP*[17], the court concluded the hard copy paper printout of an electronic document did not include all the information in the computer memory and that it failed to be a complete understanding of what actually happened. Computer forensics is a branch of forensic science pertaining to legal evidence found in computers and digital storage mediums, and the most important role is to ensure accurate and complete data acquisition. This scientific approach to ensuring the accuracy of digital evidence is critical to the issues surrounding its admissibility.

Daubert & Frye

The courts have provided two critical bodies of law (based upon *Frye v. United States*[18] and *Daubert v. Merrill Dow Pharmaceuticals*[19]) that are relevant to computer forensics. For decades, courts have applied the "general acceptance" test to all scientific evidence and testimony. In particular, Frye set the standard that: if the scientific community in that particular field, which was well recognized in scientific principle or discovery, "generally accepted" the practice, then it could be admitted in court. These principles were then updated in 2000 by FRE 702 and its amendment, which state that if there is scientific, technical, or specialized knowledge needed to understand the evidence, sufficient foundation must be laid where 1) the testimony must be based on sufficient facts or data, 2) the testimony is the product of reliable principles and methods, and 3) the witness has to have applied the principles and methods reliably to the facts of the case.

Seventy years after Frye,[20] the United States Supreme Court provided four specific criteria for scientific evidence in the case of Daubert.[21] In this case the Court threw out Frye's standards and drew up a whole new set of criteria to determine the reliability, relevancy, and admissibility of the

16 See, *Armstrong v. Executive Office of the President*, 810 F. Supp. 335, at 342 (D.D.C. 1993).
17 *Id.*
18 *Frye v. United States*, 54 App. D.C. 46, 293 F. 1013 (D.C. Cir. 1923) (affirming a lower court's sustaining of an objection to the introduction of expert witness testimony affirmed).
19 *Daubert v. Merrell Down Pharmaceuticals, Inc.*, 509 U.S. 579 (1993).
20 *Id.*
21 *Daubert*, supra, note 21.

evidence. It also gave the courts discretion on whether to accept the scientific evidence based on those criteria. Daubert [22] held that for any scientific evidence to be admitted:

1) The theory or technique utilized must have been tested and that test must be replicable.
2) The theory or technique must have been subject to peer review and publication.
3) The error rate associated with the technique must be known.
4) The theory or technique must enjoy general acceptance within the scientific community.

Court Citation of AccessData Forensic Technology

As we stated initially, this document is not meant to serve as a legal reference and is instead intended for customers of AccessData who wish to understand the legal foundation on which our products stand. As such, we will move now from discussing the basic laws of digital evidence and directly examine the relevant technology and case law associated with our products.

Notably it is worth taking a quick look at the two primary pieces of AccessData's technology that come into play when determining the admissibility of digital evidence:

Data Acquisition

AccessData's solutions utilize widely accepted forensic techniques for acquiring data without affecting, or minimally affecting, the target machine. Depending on the version of the product utilized, either an agent on the target machine or a hardware write blocker enables our solutions to acquire an exact bit stream copy of the target machine. All data can be acquired or selected by individual files. In either case the acquired data is complete, unaffected, and captured in its entirety, including all relevant metadata (a critical factor for compliance with the Federal Rules of Civil Procedure).

Evidence Storage

In addition to the methodology utilized to acquire the data, the storage format associated with the acquired data is also often relevant. Here again our solutions utilize widely accepted file formats for the storage of digital evidence. In addition to our own proprietary format (AD1), we offer users the option to store the data in other popular formats, such as DD or Export Witness E01. What is common among these formats is the utilization of hashing and checksum algorithms to ensure that any changes in the preserved data occurring after seizure or during analysis are detectable. Depending on the format used, the way the forensic imaging technologies work is they take a digital fingerprint (hash) of the entire collected dataset. Some formats, such as the Expert Witness format E01, calculate checksums at pre-determined increments. Those checksums and hashes are then saved with the forensic bit stream image of the acquired evidence. When the data is reviewed at a later point, the hashes can be re-calculated and compared to the originals to identify if any changes to the data have occurred.

AccessData's Technology and Case Law

The case of *Gutman v. Klein*[23] established the validity of AccessData's Forensic Toolkit®("FTK®")

22 *Id.*
23 *Gutman v. Klein*, 2008 U.S. Dist. LEXIS 92398, 2008 WL 4682208 (E.D.N.Y. Oct. 15, 2008).

technology for both data acquisition and evidence storage. In Gutman, the computer forensics examiner, Douglass Vitale ("Vitale") forensically copied, or "imaged" defendant's laptop hard drive using FTK® version 2.2 and testified that it was an "accepted tool under industry standards, to perform the imaging and create a forensic duplicate of the hard drive." Additionally, due to a likely battery malfunction on Vitale's computer, the forensic image was recorded as having occurred on January 1,2000, rather than the real date, December 8, 2005.[24] However, the hash value, or unique "digital fingerprint" of the imaged data, verified as accurate and thereby demonstrated that the image was accurate and complete.[25]

After Vitale imaged the hard drive, another examiner, Stroz Friedberg (See Stroz Report P 10-11),[26] took possession of the forensic image on November 14, 2006. The defense argued that the inconsistency in the imaging dates indicated the examiner had failed to authenticate the ownership of the evidence and therefore the evidence was inadmissible. The court, however, found that the hashes used by FTK to authenticate the image and establish a chain of custody were sufficient to "establish the usage and ownership history." The case explicitly established FTK as an acceptable industry standard for collecting digital evidence.

Meeting the Daubert Standards

In addition to the acceptance of the underlying AccessData technologies utilized, AccessData's solutions have been upheld countless times in court as meeting the standards set forth by the *Daubert*[27] case discussed above. Application of the Daubert standards to FTK generates the following questions:

-Has FTK® Technology Been Reliably Tested?
-Has FTK Technology Been Given Peer Review?
-What is the error rate?
-Has FTK Been Generally Accepted by the Computer Forensics Community?

Has FTK® Technology Been Reliably Tested?

AccessData's technology has been extensively tested, both by AccessData's development team and by the community at large. Probably the most widely accepted testing body is the National Institute of Standards and Technology (NIST), a department under the U.S. Department of Commerce. NIST conducts periodic tests of commercially available digital investigation solutions. NIST's Office of Law Enforcement Standards and Information Technology Laboratory formed a joint project with the National Institute of Justice (NIJ) called the Computer Forensic Tool Testing Project ("CFTT"). In 2008, the CFTT conducted a thorough examination of AccessData's Forensic Toolkit® (FTK®) technology for the purposes of disk imaging. The results of those tests are available in a National Institute of Justice Special Report, which can be downloaded at http://www.cftt.nist.gov/disk imaging.htm.

In addition to NIST and the CFTT Project, AccessData's digital investigation technologies are

24 *Id.* at 12.
25 *Id.*
26 *Id.*
27 *Daubert*, supra, note 11.

frequently evaluated by federal agencies, state agencies, and law enforcement organizations. AccessData continues to maintain collaborative relationships with these entities to optimize development efforts and stay ahead of the demands of digital investigations.

Has FTK® Technology Been Given Peer Review?

AccessData's solutions are utilized by more than 60,000 investigators, and AccessData has allowed its solutions to be scrutinized by countless industry experts, federal agencies, and publications, including but not limited to the following:

- Gartner
- Stroz Friedberg
- SC Magazine
- NIST
- Department of Defense Cyber Crime Center
- Department of Justice

What Are the Error Rates?

Error rates are not generally a relevant category within the field of computer forensics, because there are essentially no errors in data acquisitions. There is no replicable error rate. If something does happen to the acquired data, it is fully revealed by the hashing and checksum techniques, which we discussed above. That said, what is more relevant within the field of digital evidence is the concept of supported platforms. AccessData widely publishes all the platforms and file systems supported by its products.[28]

Has FTK Been Generally Accepted by the Computer Forensics Community?

AccessData's solutions have been widely accepted throughout the forensics community in the United States and around the world. Not only are there more than 60,000 copies of our software in use, but our solutions are utilized by the largest law enforcement agencies in the world, including the SEC, FBI, USSS, UK Met Police, IRS, ICE, and countless others. In addition to our extensive user base, AccessData hosts a message board with more than 7,300 active members, trains more than 6,000 people annually, and hosts one of the largest computer forensics conferences in the United States.

Finally, our forensic technology is referenced in specific case law validating its acceptance by the forensics community. In the case of *United States v. Gaynor*,[29] the court explicitly acknowledged FTK® (AccessData's flagship technology) as one of the two most commonly used forensic tools used by forensic examiners for computer investigations.

---

28 At the end of 2008, the file systems supported were FAT16, FAT32, NTFS, CDfs, HFS, HFS+, Ext2FS, Ext3FS, Reiser, UFS1, UFS2, EFS, JFS, LVM, SafeBoot, Utimaco, Credant, VMware, LVM2, every possible CD/DVD format [VCD, SVCD, SACD, CD-ROM, CD-ROM XA, CD-R, CD-RW, CD-MRW, DVD-ROM, DVCD, DVD-RAM, DVD-R, DVD-RW, DVD+R,DVD+RW, DVD+MRW, DVD+R Dual Layer, DVD-R Dual Layer, DVD+RW Dual Layer, DVD+VR, DVD+VRW, DVD-VR, DVD-VRW, DVD-VM, DVD-VFR, BD-ROM, BD-R, BD-R DL, BD-RE, BD-RE DL, BD-R SRM, BD-R RRM, BD-R SRM+POW, BD-R SRM-POW, BDAV, BDMV HD DVD-ROM, HD DVD-R, HD DVD-R DL, HD DVD-RW, HD DVD-RW DL, HD DVD-RAM, and HD DVD.

29 *United States v. Gaynor*, 2008 WL 113653

The New Federal Rules of Civil Procedure

The second group of rules relevant to digital evidence is the much more recent and more specific amendments to the Federal Rules of Civil Procedure ("FRCP"). In April of 2006, the U.S. Supreme Court approved a significant amendment to the FRCP illustrating discovery rules for electronically stored information. The new rules promulgated as early as 1996 stemmed from the first issues of computer based discovery, originated with the Advisory Committee, and finally became effective in December 2006. While the changes were extensive and nuanced, there were five key rules that provided significant guidance for companies facing litigation:

- Definition of e-Discovery: The amendment addressed the process of electronic discovery, ("e-Discovery or e-discovery") as any process in which electronic data is sought, located, secured, and searched with the intent of using it as evidence in a civil or criminal legal case.[30] This broad definition is meant to include present and future computer based information through ever changing technology beyond the desktop computer such as smartphones and tablets.
- Scope of Discovery: The scope of the discovery demands an exhaustive search for all electronically stored information that is "in the possession, custody, or control of the party."[31] Under FRCP 26(b)(2) the scope of the production of ESI is distinguished between those that are easily accessible and those that are not due to undue burden or cost. In such instance, the requesting party must move to compel discovery of the information and the responding party must show evidence that production would result in undue burden or cost. It is upon the court's discretion to grant the motion to compel for good cause. Even when data is "identified as not reasonably accessible because of undue burden or cost," its location and description must be disclosed.[32] These changes have been interpreted to mean a thorough search of all active or stored data, as opposed to all available data, which would include the recovery of deleted documents.
- Early Review and Production: The new rules also require immediate review and extremely quick production of electronic evidence. Specifically, the new rules require ESI to a party's initial disclosures and that a comprehensive search of electronic data be done prior to the first pre-trial conference.[33] Discovered data must be disclosed "without awaiting a discovery request" with the only exception being privileged data.[34]
- Format of Production: FRCP 26(f)(3) and FRCP 34(b) addresses the parties initial meeting in which they discuss the format of any electronic discovery to be produced. The rules don't mandate a specific format but mandates for the producing party to disclose which format they plan to produce their ESI. While the rules don't require ESI to be produced in any specific format, significant case law indicates a requirement for native production in certain circumstances, including the Williams[35] case, in which the Court ruled that the electronic spreadsheets kept in the ordinary course of business, were to be produced "in native format ... with their metadata intact."

30 *Id.* at 10.
31 *Id.* at 12.
32 FRCP 26(b)(2)(B)
33 FRCP Rule (16)(b)
34 FRCP RULE 26(a)(1).
35 *Williams v. Sprint/United Mgmt. Co.*, 230 F.R.D. 640, 2005 U.S. Dist. LEXIS 21966 (D. Kan. Sept. 29, 2005)

- Sanctions: Finally, the new rules provide for significant sanctions in the event that data is not produced in a timely manner or deleted:
- Data Is not Produced: When data is not produced, sanctions can be significant, such as the monetary fines awarded in *Todd v. Guidance Software*.[36] In addition, the court can appoint external experts to retrieve the data from the company if the company is unable to produce the data itself.
- Data Is Produced Late: When data is produced late the fines are typically monetary as in the case of *Serra Chevrolet, Inc. v. General Motors*[37] where a sanction of $50,000 per day was awarded until the data was produced.
- Data Is Deleted: When data is deleted, the new rules apply a "routine, good-faith operation" standard to determine whether the data was deleted as part of normal procedures or if it was knowingly deleted to hide evidence. If the data was deleted as part of a normal process, Rule 37(f) safe harbor protects the company from sanctions. However, if it was deleted for other reasons, sanctions can range from fines to entry of default judgment, as awarded in *Arista v. Usenet.com*.[38] Moreover, a good faith defense can be closely scrutinized depending on what kind of preservation operation is in place, "A party cannot exploit the routine operation of an information system to evade discovery obligations by failing to prevent destruction of stored information that is required to preserve."[39]

Proper Collection and Good Faith Effort are Critical

When dealing with discovery matters, the courts have confirmed that ESI collected by FTK® technology and produced in the form of FTK®-generated reports have been sufficient to satisfy discovery requirements.[40] These findings provide assurance that using the software with proper methods would satisfy discovery requirements, save time in collection, and thereby reduce costs.

While computer forensic technology, such as FTK®, can ease the burden of collection, this technology also makes it easier to prove a party is not disclosing everything requested. Using this type of technology, a forensic expert is able to track collection efforts and timeline ESI production to illustrate a party's good faith effort or a party's failure to comply. Even more than before, it is critical for an organization to legitimately and appropriately produce ESI requested through discovery motions. Failure to produce ESI in strict compliance with the Federal Rules has resulted in the United States District Court sanctioning parties, ordering the compensation of the opposing party's attorney and expert witness fees in gathering the undisclosed ESI, and even going as far as considering dismissal of a case when destruction of ESI has been proven.

In *In re Atlantic*,[41] the court held defendant's corporate counsel failed to cooperate in discovery which led the court to award compensation of plaintiff's attorney fees and costs incurred in pursuing discovery. Defendant made contradictory statements regarding several issues. One of the

36 *Todd v. Guidance Software, Inc.*, No. 8:08-CV-01354, (C.D. Cal. filed Dec. 16, 2008)
37 *Serra Chevrolet, Inc. v. General Motors Corp.*, 446 F.3d 1137 (11th Cir. 2006).
38 *Arista Records, LLC v. Usenet.com, Inc.*, 2009 WL 1873589 (S.D.N.Y. June 30, 2009).
39 *Williams v. Sprint/United Mgmt. Co*., 230 F.R.D. 640, 2005 U.S. Dist. LEXIS 21966 (D. Kan. Sept. 29,2005).
40 See "AccessData in Court," The Rules of Digital Evidence and AccessData Technology, AccessData Corp. 2009. Available at http://www.accessdata.com/
41 In *re Atlantic Intern'l Mortg. Co.*, 352 B.R. 503, 509 (Bankr. M.D. Fla. 2006).

issues was regarding whether FTK® was used for document recovery and, in response, defendant's technology manager testified that no such program was used to search and recover any documents. Meanwhile, a court-appointed computer expert testified that he found evidence that proved FTK® had been used but that the documents had just not been turned over to Plaintiff. Not only did the court accept the data searched for and produced by FTK®, but relayed repercussions of what happens when parties do not cooperate in good discovery practice. The United States District Court easily found bad faith discovery methods with the assistance of a court-appointed expert, utilizing computer forensic methodology.

Not only is it beneficial to use an expert and the proper accepted software in ESI production, but it is mandatory under the FRCP 26(a)(2)(c). The rule mandates that a "party must make [expert] disclosures at the times and in sequence that the court orders."[42] In making the good faith effort of showing cooperation of discovery disclosures, it would be beneficial to the party to use software that has been acknowledged as an acceptable method of production of ESI, such as FTK®. In 2008, the court in *Rivera-Cruz*[43] held that, even though the expert failed to apply his forensic methods correctly to the facts of the case, the proper methods and software, FTK®, was used as it was the same product used by the United States General Services Administration. Using the proper tools from the beginning can diminish further doubt by opposing parties and prevent opposing parties from bringing in motions against proper discovery methods and further delaying litigation, which can cause more expenses and, more importantly, bad faith presumption on a party's case.

Duty to Preserve - Litigation Holds

Once a person or company has a reason to believe they may be a party to a litigation action, they have a duty to preserve relevant discovery. To fulfill this duty, the legal counsel for the proposed party must put on a legal hold. A legal hold is a process which an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated.[44] The legal hold is a notice by the legal counsel sent to all possible and relevant persons who have or may have information regarding the anticipated litigation at hand and notifies these persons ("Custodians") that they must preserve all relevant materials. Litigation holds are also to be sent to information technology employees of the company that controls any document retention policies or business procedures which automatically delete ESI, otherwise the employee could just as well be compared to an employee shredding documents in the backroom. In *UBS v. Zubulake*,[45] where former UBS equities trader Laura Zubulake won a $29 million award in a federal gender discrimination suit, the judge penalized UBS for failing to recognize that missing emails would end up being relevant to future litigation, stating "the obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation."[46] An organization's choice of technology to fulfill this obligation is critical to avoid court sanctions and embarrassing court losses.

42 *Id.*
43 *Rivera-Cruz. v. Latimer, Miaggi, Rachid & Godreau, LLP,* 2008 WL 2446331 (D. Puerto Rico 2008).
44 Wikipedia, August 1, 2012, http://en.wikipedia.org/wiki/Legal_hold
45 In *re Atlantic Intern'l Mortg. Co*., 352 B.R. 503, 509 (Bankr. M.D. Fla. 2006).
46 *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212, 216 (S.D.N.Y.2003) ("Zubulake IV').

Litigation Hold Notification

The litigation hold itself should contain all the information a Custodian would need to know in order to comply with his or her preservation obligations. A record of receipt with the Custodian's confirmation should also be maintained to ensure that the right Custodian is on notice. It is recommended that a reminder be sent to Custodians throughout the investigation or possible threatened litigation period and into the actual litigation, if any.

The litigation hold process required by the FRCP 2006 amendment can be arduous, especially for a good sized organization. All of this, however, can be an automated process using AccessData's Early Case Assessment or e-Discovery tool. From the moment the company counsel learns of a possible threat of litigation or investigation, the counsel can log into the system using AccessData's software and initiate a case file. From there, counsel can choose the Custodians from a list generated of the organization's employee file and draft a specific legal notice to send out to the selected Custodians. Counsel can also set a reminder notice to all the Custodians for that certain case file. A reminder will be sent to the Custodians so they do not forget their obligation to preserve any potentially relevant or relevant documents. After counsel sends out the legal hold, the Custodians will receive a message via email where they will be asked to click a link so as to confirm the receipt of the litigation hold. This confirmation is sent to the case file, where counsel can manage and be on notice of which Custodians have confirmed receipt.

The Collection Process and Reducing Risk

Documents and other information are central to every legal matter, even for those matters that don't involve litigation. For matters involving litigation, even potential litigation, an extra duty of preservation is imposed upon the party.[47] Spoliation of evidence, when there is a duty to preserve it, can prompt a court to impose sanctions on an organization and/or its counsel. Sanctions are often monetary[48] but can include: the striking of pleadings,[49] default judgment,[50] dismissal of the case[51], or an adverse inference.[52]

The duty to preserve implies two subsequent actions, namely the identification of the relevant information, and the collection of that information for review and possible production/ presentation. Thus, for each case the attorney must find the relevant information and decide how to preserve it.

---

47 "The duty to preserve evidence 'arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.'" *Acorn v. City of Nassau*, 2009 WL 605859 at 2 (E.D.N.Y. March 9, 2009) citing *Zubulake v. UBS Warburg LLC* ("Zubulake IV'), 220 F.R.D. 212, 216 (S.D.N.Y.2003) (which quoted *Fujitsu Ltd. v. Federal Express Corp.*, 247 F.3d 423, 436 (2d Cir.2001). "Once the duty to preserve arises, a litigant is expected, at the very least, to 'suspend its routine document and retention/destruction policy and to put in place a litigation hold.'" *Id.*, citing *Zubulake IV*, 220 F.R.D. at 218; and also *Doe v. Norwalk Cmty. Coll.*, 2007 U.S. Dist LEXIS 51084, at *14 (D. Conn. July 16, 2007) (a party needs to take affirmative acts to prevent its system from routinely destroying information).

48 See, e.g., *Kipperman v. Onex Corp.*, 2009 WL 1473708 (N.D. Ga. May 27, 2009) ($1,022,700 in monetary sanctions levied against the defendant for "a textbook case of discovery abuse.")

49 FRCP Rule 37(b)(2)(iii): "striking pleadings in whole or in part". See, e.g., *Channel Components, Inc. v. Am. II Electronics, Inc.*, 915 So. 2d 1278 (Fla. Dist. Ct. App. 2005) (striking of pleading considered, but not imposed by the Court).

50 FRCP Rule 37(b)(2)(vi): "rendering a default judgment against the disobedient party". See, e.g., *Gutman v. Klein*, 2008 WL 4682208 (E.D.N.Y. Oct 15, 2008) (Magistrate Judge recommended default judgment in favor of plaintiff, plus attorneys' fees); *Atlantic Recording Corp. v. Howell*, 2008 WL 4080008 (D. Ariz. Aug. 29, 2008) (default judgment warranted after "brazen destruction of evidence").

51 FRCP Rule 37(b)(2)(v): "dismissing the action or proceeding in whole or in part". See, e.g., *Kvitka v. Puffin Co., LLC*, 2009 WL 385582 (M.D. Pa. Feb. 13, 2009) (all of plaintiffs claims were dismissed, and an adverse inference instruction awarded to defendant's cross-claims after plaintiff intentionally discarded her laptop in spite of a duty to preserve it).

52 See, e.g., *Smith v. Slifer Smith & FramptonNail Assocs. Real Estate, LLC*, 2009 WL 482603 (D. Colo. Feb. 25, 2009) (Despite lack of evidence of a "smoking gun," the Court awarded an adverse inference against the defendant because documents were destroyed well after the litigation hold notice was put in place.)

The preservation of the information, however, can be affected by how the information is collected. Consequently, a sanction-averse attorney would do well to acquaint him/herself with their collection options.

There are many "right" and some "wrong" ways to collect and to preserve potentially relevant evidence. No matter what, however, the attorney and/or client will need to take some action, which will likely entail some software application in order to take advantage of any safe harbor provisions.[53] What constitutes a right or a wrong collection process can be subjective, with the last word belonging to a judge. From the attorney's standpoint, there are only two main varieties of collection procedures: copy/sequester and in-place hold (also referred to as hold in place). Each procedure has benefits and shortcomings. More importantly, each procedure has a different potential for sanctions by a court.

Attorneys prefer the copy/sequester method because it mirrors sound forensic guidelines promulgated by many law enforcement agencies, such as the U.S. Department of Justice.[54] The copy/sequester method doesn't make a single copy of the original document. Instead, two copies are typically made. Experts utilize the second copy (called a "working copy") for analysis. The first copy is left undisturbed and can be used to obtain working copies of the document if the review/examination process corrupts the original working copy.

If there is a question regarding the integrity of the document, the question can be resolved by reference to the first copy in a manner easily defensible to a court.[55] The copy/sequestration method, if done with a competent forensic software application, can make an exact copy of the document itself and the associated metadata while leaving the original document in place for further use by the client. Remember, if not done correctly, the process of copying can result in spoliation of the evidence. In the past, some attorneys were concerned whether the copied electronic files adhered to the Best Evidence Rule.[56] This isn't a problem in today's computerized legal environment. Recall that the Best Evidence Rule was promulgated in the 19th century, when it was difficult to make copies of a document at all, let alone precisely. However in the 21st century, making precisely identical copies of an electronic document is trivial and reliable with the right software. Because precisely identical copies of electronic documents and their associated metadata can be readily made, creating authenticable copies of ESI, if done properly, does not subject the attorney to a sanctions motion for spoliation of evidence.

---

53 The safe harbor provisions are identified in FRCP Rule 37(e). See, e.g., *Gippetti v. UPS, Inc.*, 2008 WL 3264483 (N.D. Cal. Aug. 6, 2008) (Plaintiff's motion for sanctions were denied in view of a safe harbor provision because the documents that were destroyed were done so in accordance with the company's document retention policy and there was no apparent relevancy of those documents to the case given the Plaintiffs cause of action).

54 See, e.g., "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," Computer Crime and Intellectual Property Section, Criminal Division, United States Department of Justice, July 2002 at p. 53, available at http://www.usdoj.gov/criminal/cybercrime/s&s-manual2002.pdf. Judge Scheindlin in *Zubulake V* arguably endorsed elements of the copy/sequestration method when she set fourth three factors that counsel should take in conjunction with the litigation hold, one of which was: "Finally, counsel should instruct all employees to produce electronic copies of their relevant active files. Counsel must also make sure that all backup media which the party is required to retain is identified and stored in a safe place." *Zubulake v. UBS Warburg*, 229 F.R.D. at 422, 434 (S.D.N.Y. July 20, 2004) (emphasis added).

55 The integrity of the copy can be verified by comparison to "hash values" using a cryptographic function, such as the Message-Digest algorithm "MD5". See, e.g., *Xpel Techs. Corp. v. Am. Filter Film Distribs.*, 2008 WL 744837 (W.D. Tex. Mar. 17, 2008) ("all images and copies of images shall be authenticated by generating an MD5 hash value verification for comparison to the original hard drive."); *Bro-Tech Corp. v. Thermax, Inc.*, 2008 WL 724627 (E.D. Pa. Mar. 17, 2008); *Creative Sci. Sys., Inc. v. Forex Capital Mkts., LLC*, 2006 WL 870973 (N.D. Cal. Apr. 4, 2006) (Unpublished).

56 The Best Evidence Rule is also "referred to as the 'Original Writing Rule' because it does not mandate introduction of the 'best' evidence to prove the contents of a writing, recording or photograph, but merely requires such proof by an 'original,' 'duplicate' or, in certain instances, by 'secondary evidence'-any evidence that is something other than an original or duplicate (such as testimony, or a draft of a writing to prove the final version, if no original or duplicate is available." *Lorainne v. supra*, note 2 citing FED. R. EvID. 1001 advisory committee's note. Article X of the Federal Rules of Evidence codified the common law Best Evidence Rule, terming it instead the 'original writing rule.'" *Id.*

While copying electronic documents and their associated metadata can be readily accomplished, the attorney needs to ensure that the copying is done properly. Simply making copies by burning CD's, copying files to thumb drives or "ghosting" may seem adequate, but unless attorneys are very careful, they will likely alter (irreparably) some of the metadata associated with the original file, thus tampering with the evidence.[57] In some cases, the altering of such metadata has resulted in sanctions.[58] It is always better to use a forensics tool that is designed to preserve all of the evidence when making a copy using default settings.

Sequestration of the copied evidence is the obvious second step in the method. Sequestration can take many forms, such as locking the hard drives containing the copies of the evidence in a secure locker in the legal department or storing the information at an offsite location. There is no objective standard for the sequestration step, although attorneys should exercise reasonable judgment. The key is separating the first (archive) copy of the information from both the original copy and the working copy used by attorneys and experts, and maintaining the security of the various copies. This ensures that there is a source where, if all else fails, a precise copy of the original evidence is available to remedy problems.

As the name suggests, in-place hold allows the original electronic documents to remain in where they are. The benefits are obvious. The attorney doesn't have to disrupt access to his or her client's data during a copying process. However, in order to adhere to litigation hold notices or other preservation considerations, the attorney must impose some safeguards so that the original electronic documents are not disturbed. This can be accomplished by forcing the client to save new/updated documents to another location. Unfortunately, not only does the "copy new/updated files to a new place" method disrupt the client's normal business operations, that method also requires strict cooperation by the client and their employees. Moreover, to avoid frustration, some employees may not adhere to the terms of the litigation hold and destroy the evidence.[59] Circumvention of the in-place hold methodologies, particularly those employing agent-less software applications, rely upon features[60] of the underlying operating system.[61] However, employees using tools readily available on the Internet can modify the privilege levels of relevant files and thus tamper with the evidence.[62] Furthermore, even after software guards have been put in place, some custodians have been known to destroy the machine containing the evidence.[63]

While the Federal Rules don't preclude the in-place hold methodologies, "[c]ourts may consider

57 See, e.g., Craig Ball, "Don't Mess With System Metadata" Law Technology News, April 23, 2009, available at http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202430116124.

58 See, e.g., *Krumwiede v. Brighton Assocs., L.L.C.*, 2006 WL 1308629 (N.D. III. May 8, 2006) (a plaintiff who destroyed metadata in the process of copying files was subject to a default judgment on the first four claims and ordered to pay costs--including expert fees and attorney fees—associated with the sanctions motion).

59 In re Hawaiian Airlines, 2007 WL 3172642 (Bkrtcy. D. Hawaii, Oct. 30, 2007) (company sanctioned when its CFO wiped files from his laptop computers after he was informed of a litigation hold notice).

60 All operating systems utilize mass storage devices (such as hard disks or flash drives) that are formatted with a file system. File systems typically have a system of allocating privileges for reading, modifying, or otherwise utilizing files contained within the file system. For example, normal users are typically not allowed to modify files associated with the core software applications required for standard operation of the machine.

61 *United States v. Briscoe*, 896 F.2d 1476, 1494 (7th Cir.1990) (citing *United States v. Croft*, 750 F.2d 1354, 1365 (7th Cir.1984) at n. 7)

62 One such tool is Ophcrack (http://ophcrack.sourceforge.net/), which is a Linux LiveCD that can be used to find the passwords associated with the Windows machine, including the administrator's password. Ophcrack is free and works on any flavor of Windows, including Vista. Another popular tool is "ntpasswd"
which is freely available at: http://home.eunet.no/pnordahl/ntpasswd/. Ntpasswd can reset the administrator's password to whatever the employee desires. Note, the tools mentioned previously are commonly used by system administrators to fix problems encountered during the normal operation of PC's. In other words, these tools are not aberrant or illegal hacker software, but instead have legitimate uses.

63 *Kvitka*, supra, n. 51, is a case where the plaintiff destroyed her laptop after being apprised that she was under an obligation to preserve it, and did not reveal the loss of the laptop to the Court when a judge asked her about the state of some of the contents of the laptop.

the actions taken by counsel to ensure compliance with a party's preservation obligation."[64] Indeed, the court in *Hawaiian Airlines* noted that the defendant had alternatives to the in-place hold scheme that they had adopted, and sanctions were appropriate because the collection/sequestration option was not taken.[65] The Sedona Conference has recently noted the need for quality assurance as part of the attorney's duty.[66] Indeed, the trend is to impose a duty on the attorney to require a certain level of quality assurance for the operations performed under his or her direction.[67]

Finally, one may question whether storing new/updated copies of the original documents in a different location is any less trouble than the copy/sequester method because, in both cases, there are two sets of documents in two locations. Wouldn't it have been simpler to make a copy of the original set of documents and allow clients to continue using their machines in the normal fashion?

If the "in-place hold" method fails for some reason, the requesting party can file a motion under Rule 34(a)[68] asking the court to require the responding party to provide access to its system to the requesting party's forensic expert or to a court-appointed special master.[69] If there is evidence of spoliation, sanctions could be imposed on the producing party and their attorneys.[70]

Under the copy/sequester method, virtually the only thing that can go wrong is the mechanical failure of the device containing the sequestered data. Such failures do happen.[71] However, no court has ever held that against an attorney or party for such a mechanical failure outside the control of the attorney or his or her client.

Because employing the copy/sequester method reduces the potential for sanctions against the attorney and the client, most attorneys when faced with a choice will avoid the "in-place hold" method for preserving electronically stored information.

The Federal Rules and Technology

Since the change in the Federal Rules, there have been many cases that have further defined and provided insight into the interpretation of these rules. There has also been a large amount of practical experience

64 "The Sedona Conference on Legal Holds: The Trigger & The Process" (August 2007 Public Comment Version) by the Sedona Working Group at 12, citing *Zubulake V*. The paper is available at http://www.thesedonaconference.org/dItForm?did=Legal_holds.pdf

65 "Mesa could have taken reasonable steps that would have prevented, or mitigated the consequences of, Mr. Murnane's destruction of evidence. For example, Mesa could have made a backup of Mr. Murnane's H drive and the hard drives of Laptop 1 and Laptop 2 promptly after HA filed suit. Doing so would not have been costly, burdensome, or unduly disruptive of Mesa's business. Instead, Mesa simply told Mr. Murnane to preserve all evidence and trusted him to comply. Even though Mr. Murnane was a valued, trusted, high level employee of the company, Mesa could and should have taken reasonable steps to prevent all of its employees from doing wrongful and foolish things, like destroying evidence, under the pressure of litigation. Because Mesa failed to take such steps, Mesa facilitated Mr. Murnane's misconduct." In *re Hawaiian Airlines, Inc.*, Debtor; *Hawaiian Airlines, Inc. v. Mesa Air Group, Inc.*, 2007 WL 3172642 at *6 (Bkrtcy. D. Hawaii, Oct. 30, 2007).

66 The Sedona Conference, "Commentary on Achieving Quality in the E-Discovery Process" (May 2009 Public Comment Version) available at: http://www.thesedonaconference.org/content/ miscFiles/publications_html?grp=wgs110

67 See, e.g., *Wingnut Films v. Katja Motino Pictures Corp.*, 2007 WL 2758571, at *5 (C.D. Cal. Sept. 18, 2007) (a producing party must make a "reasonably diligent search for e-mails and other electronic documents").

68 "(a) Scope. Any party may serve on any other party a request (1) to produce and permit the party making the request, or someone acting on the requestor's behalf, to inspect, copy, test, or sample any designated documents or electronically stored information - including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations stored in any medium from which information can be obtained, translated, if necessary, by the respondent into reasonably usable form, or to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served; or (2) to permit entry upon designated land or other property in the possession or control of the party upon whom the request is served for the purpose of inspection and measuring, surveying, photographing, testing, or sampling the property or any designated object or operation thereon, within the scope of Rule 26(b)." FRCP 34(a).

69 See, e.g., White v. Graceland Coll. Ctr. for Prof'I Dev. & Lifelong Learning, Inc., 2009 WL 722056 (D. Kan. Mar. 18, 2009) (although intrusive, "request for inspection for forensic or mirror imaging of computers [are] neither routine nor extraordinary.") citing G.D. v. Monarch Plastic Surgery, P.A., 239 F.R.D. 641 (D.Kan. 2007); Balboa Threadworks, Inc. v. Stucky, No. 05-1157-JTM-DWB, 2006 WL 763668 (D.Kan. Mar. 24, 2006); Jacobson v. Starbucks Coffee Co., No. 05-1338-JTM, 2006 WL 3146349 (D.Kan. Oct. 31, 2006).

70 See, e.g., *Kipperman*, supra note 48 (court imposed $1,022,700 sanction for discovery abuse); *Oz Optics, Ltd. v. Hakimoglu*, 2009 WL 1017042 (Cal. App. Apr. 15, 2009) (appellate court upholds $90,000 sanction); *Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co.*, 2009 WL 546429 (M.D. Fla. Mar. 4, 2009) (court imposed sanctions on plaintiff and counsel).

71 Hard disks do fail, more often after a few years of non-use, which is well within the time period of lawsuits. Many vendors who store data know this and offer to "spin up" the hard disk periodically to ensure operation over extended periods of time.

gained as companies have attempted to comply with the rules, as well as test their boundaries. While none of this experience directly references any particular products, the last few years have made it clear that there are a few technological requirements that corporations should focus on when purchasing an e-discovery solution:

1) Metadata - How Important Is It?

The importance of metadata is growing as more and more judges require its production. That said, the issue is actually fairly nuanced. The most accurate statement regarding metadata is that it is as important as the prosecution wants it to be. If the prosecution asks for the production of metadata in the initial Meet and Confer (26(f) meeting), or prior to a significant amount of data being produced, then the courts have almost universally required its production.

> "There is a clear pattern in the case law concerning motions to compel the production of metadata. Courts generally have ordered the production of metadata when it is sought in the initial document request and the producing party has not yet produced the documents in any form. See Payment Card, 2007 WL 121426, at *4 (directing production of metadata for any documents not yet produced); Hagenbuch, 2006 WL 665005, at *4 (granting motion to compel production in native form); In re Priceline.com, 233 F.R.D. at 91 (production ordered in TIFF format with corresponding searchable metadata databases)." [72]

Even when the data has been produced, if the evidentiary value of the metadata is clear or at least should have been clear, the court has required its production in native form, as in the case of *Williams*,[73] when the court "ordered production of Excel spreadsheets with metadata even though no request had been made initially because producing party should reasonably have known that metadata was relevant."[74]

If, however, the request for production comes well after documents have already been produced and the evidentiary value of the metadata is not immediately clear, then the courts have been more reluctant to require its production:

> "See *Mich. First Credit Union*, 2007 WL 4098213, at *2 (court denied production despite timely request for metadata because it was not relevant and production would be unduly burdensome). On the other hand, if metadata is not sought in the initial document request, and particularly if the producing party already has produced the documents in another form, courts tend to deny later requests, often concluding that the metadata is not relevant. See *Autotech Techs.*, 248 F.R.D. at 559-60 (court refused to compel production of metadata not sought in initial request); *D'Onofrio v. SFX Sports Group, Inc.*, 247 F.R.D. 43, 48 (D.D.C.2008) (same); Payment Card, 2007 WL 121426, at *4 (denying motion to compel metadata for documents already produced in TIFF format because another production would be unduly burdensome); *Ky. Speedway*, 2006 WL 5097354, at *8 (motion to compel production of metadata denied when request first came seven months after production); *Wyeth*, 248 F.R.D. at *171 (documents produced in TIFF format were sufficient since

72 *Aguilar v. Immigration and Customs Enforcement Div. of U.S. Dept. of Homeland Sec.*, 2008 WL 5062700 (S.D.N.Y. Nov.21, 2008).
73 *Williams*, supra, note 38, 230 F.R.D. at 654.
74 *Id.*

parties never agreed on form of production).[75]

Despite the nuanced nature of the law, the point here for any company looking to implement an e-discovery solution is that attorneys absolutely must have a solution that can collect and produce relevant metadata.

2) Timely Production and Scope of Discovery

The speed and scope of production are very important issues when considering which e-discovery solution to implement and have also been an area of interest in case law. Case law and the new Federal Rules are fairly clear that if a machine is on the network it is within scope. In fact over the past several years the courts have become extremely unforgiving regarding "undue burden" arguments attempted by defense. One particularly compelling case regarding these issues is *Todd v. Guidance Software*.[76] In this wrongful termination case, Todd requested production from Guidance Software ("GSI") of all documents related to her and discussions regarding her performance and employment. The case is important because of the way GSI responded to the request and the resulting conclusions formed by the court.

- Filter: The investigator at GSI tasked with the discovery apparently filtered data that was reactive to the agreed upon search terms based on his perception of relevance. In the words of the judge: "The problem that I see immediately [is that] he acted like a filter. That's not his job. That's not what discovery is all about ……It's inexcusable."
- Data Corruption: GSI ultimately claimed that the inability to produce data stemmed from the corruption of its Exchange server shortly after the departure of Todd. In reaction to this admission in combination with the slow data production, the judge concluded: "Was there hiding the ball going on? Circumstantial evidence, but it is very, very persuasive that this was being done." The arbitrator went on to say that the behavior of Guidance Software "and the naiveté that they thought they could get away with boggles the mind."[77]
- Time and Scope: In addition to the above issues, the case takes a very interesting look at the issues of both time and scope. On May 9, 2008 the Court entered a sanction order requiring GSI to execute a board search and return the resulting data immediately. GSI reacted by saying it was "unable to comply……. Because of the scope and breadth of the searches proposed and the number of custodians designated by plaintiff were overboard. Instead, GSI indicated that the search would require 12-14 days to complete." In response plaintiff offered expert testimony that "the search terms and number of custodians was reasonable... and that it was possible to conduct the search within 24 hours." In reaction to the two respective arguments, the judge ruled that "GSI has not fulfilled its obligations to produce all discoverable documents."[78]
- Court Reaction: The court reacted in three distinct ways to the incomplete and improper production. First and foremost, Guidance Software was sanctioned and required to pay expert fees to evaluate its collection. Secondly, the judge concluded that relevant data had been withheld

75 *Aguilar*, supra, note 72.
76 *Todd v. Guidance Software, Inc.*, supra, note 39.
77 *Id.*
78 *Id.*

or destroyed and allowed Todd to stipulate the existence of several incriminating emails without objection. Finally, the judge ultimately found in favor of the plaintiff.[79]

The *Todd* case is compelling for companies to consider when looking at an e-discovery solution, as it speaks not only to scope but also to time considerations. It is clear from this case and many others that the courts are less receptive to delays or claims of undue burden then before, when fewer solutions were available. As a result, companies need to implement solutions that can quickly respond to relatively large-scale discovery requests. In short, the solution needs to be truly distributed and automated.

3) Deleted Data

In most cases, deleted data has generally been considered beyond the scope of most discovery requests. However, that is not always the case and it is important for companies to realize that they can be compelled to produce deleted documents. This is particularly true for governmental organizations, as it was in the case of *State ex rel. Toledo Blade Co. v. Seneca County Bd. of Comm'rs*.[80] In this case, the Ohio Supreme Court ruled in a 7-0 decision that "the Seneca County Board of Commissioners had to make reasonable efforts to recover and provide the Toledo Blade newspaper with emails that had been deleted in violation of the County's records retention policy and disposition schedule. The fact that these emails had been deleted did not relieve the County from its obligation to produce this information since deleted computer files are still discoverable."

It is no surprise that destruction of evidence by either party whether it is material or not can become a huge issue during litigation. A party's failure to preserve discovery in the light of litigation could considerably prejudice the other party's ability to litigate their claims and therefore such findings by the court that a party fail to preserve discovery and go further as to delete such discovery can result in heavy sanctions and even adverse jury instructions. More important than sanctions, an adverse instruction to the jury at trial may be permitted if destruction of evidence is illustrated. The opposing party must show with sufficient evidence which a "reasonable trier of fact could infer that the destroyed evidence would have been the nature alleged by the party affected by its destruction."[81] However, if there is a showing of bad faith on the party that destroys evidence, through sufficient circumstantial evidence, the jury could conclude that the missing evidence was unfavorable to that party. In other words, the jury may be given instructions that a party found to have destroyed evidence in bad faith had caused spoliation of evidence and therefore, when making the final decision, the jury must infer that the evidence that was deleted or spoiled would have worked against the party that had deleted the data and was favorable to the other party at trial. Obviously, any such inference could be destructive, which goes to show that proper electronic discovery methods must be used.

While the party seeking discovery has the burden of proving that any such destruction of evidence has occurred, it has become all too easy for a party to find wrongdoing through court-ordered

79 *Id.*
80 *State ex rel. Toledo Blade Co. v. Seneca County Bd. of Comm'rs, 899 N.E.2d 961, 2008 WL 5157133, (Ohio 2008).*
81 *Id.*

forensic experts. *In Smith v. Slifer Smith & Frampton/Vail Associates Real Estate LLC and W. Seibert*,[82] the court granted the plaintiff's motion for sanctions for spoliation of evidence and inference of adverse and granted attorneys' costs due to findings and expert testimony of plaintiff's forensic expert that data was manually deleted off the defendant's hard drive. Plaintiff's forensic expert testified that using e-discovery software, he could confirm that deletions on the defendant's hard drive took place during specific times and that though some were automated deletions, others were deleted manually by defendant. The court accepted the expert testimony and granted plaintiff's request for sanctions and attorneys' costs as well as instructing the jury to receive adverse inference instructions because the court concluded the deletion of data was done in "bad faith and intended to prevent disclosure of relevant evidence."[83]

Attorneys' fees and expert fees can become uncontrollable if an organization must compensate the opposing party's fees due to failure to use good discovery practice. The court in Smith found plaintiff's ability to litigate their claims were substantially prejudiced by defendant's failure to preserve potentially relevant information and therefore found that Defendant's failure to preserve ESI had forced the plaintiffs to incur considerable discovery expenses.[84] The court therefore ordered plaintiffs an award of their attorney fees and costs for the motion of additional discovery expenses. Litigation is always expensive and having to compensate the other party for additional costs such as these stresses the importance of practicing good discovery through good faith and proper court-approved methods.

4) Limits of Litigation Hold Technologies

The last area we are going to examine here is the limitation of litigation hold technologies. These technologies are absolutely critical for virtually every company subject to U.S. law because of the prominent place litigation hold notices take in case law. Despite the importance of these solutions, it is critical for companies to understand that they do not represent a complete solution, nor do they reduce the company's obligation to produce evidence subject to the litigation hold notice. This issue is made crystal clear in the case of *In re Hawaiian Airlines, Inc.*,[85] in which defendant Mesa Air relied on litigation hold notices to ensure that key data was preserved. Unfortunately, upon receiving the litigation hold notice, Mesa's CFO downloaded and executed wiping tools designed to eliminate all relevant data from his computer. In this case, Mesa Air argued that because the CFO had acted alone in direct conflict to the litigation hold notice that had been sent, Mesa should not be subject to sanctions or summary judgment. In his ruling, the judge disagreed with the arguments put forth by Mesa Air and concluded that "Mesa should also be responsible for the intentional destruction by one of its highest ranking officers of evidence."[86] To justify his decision, the judge pointed to the fact that "Mesa could have prevented Mr. Murnane from destroying evidence, or at least limited his ability to destroy evidence, by taking reasonable, inexpensive, and non-burdensome steps. Mesa failed to do so and is responsible for the consequences of that failure."[87] To remedy the prejudice resulting from the destruction of data, the judge entered a finding of fact that Mesa Air not only had destroyed

82 *Smith v. Slifer Smith & Frampton/Vail Associates Real Estate LLC and W. Seibert*, 2009 WL 482603 (D. Colo. Feb. 25, 2009).
83 2009 WL 482603 (D.Colo.)
84 *Id.*
85 *Hawaiian Airlines*, supra, note 59.
86 *Id.*
87 *Id.*

critical evidence but that the evidence validated Hawaiian Airlines claims. In addition he held open the possibility that Hawaiian Airlines "may also be entitled to costs and reasonable attorneys' fees as a further sanction."[88]

The important point raised by the case of *In re Hawaiian Airlines*[89] is that so-called "hold in place" technologies do not protect a company from claims of spoliation, especially if that spoliation is perpetrated by an employee who is even moderately skilled technically. As a result, companies need to ensure they not only have litigation hold capabilities, but that they also have an e-discovery solution with the following two key capabilities:

- Integration with Litigation Hold: Companies should work to ensure that whatever technology they select for their e-discovery solution offers some degree of integration with their litigation hold technology. At a minimum, companies need the ability to specify employees who might be critical to a given case and execute a proactive collection against prior or in conjunction with the sending of litigation hold notices.
- Automated Forensic Collection: Companies need a solution that automates both the identification of data relevant to a given case, as well as the collection and preservation of that data. In addition, the solution should be able to execute a complete disk image of particularly critical resources (the computer of the Mesa CFO comes to mind).

Pension Comm. Of Univ. of Montreal Pension Plan v. Bank of Am. Secs., LLC

In the case of *Pension Comm. Of Univ. of Montreal Pension Plan v. Bank of Am. Secs., LLC*, Judge Shira Scheindlein gave an extensive opinion in regards to the preservation obligations of litigating parties and "revisited" Zubulake from 2004. In the final 2004 Zubulake opinion, it was established that once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and place a "litigation hold", ordering all relevant documents to be preserved. Six years later, in this case, the court eliminates any room for excuses or defenses for a party's failure to preserve evidence once the duty to preserve arises and thus identifies the standard of care that must be used to avoid sanctions, at the least.

The court makes an unequivocal statement in its introduction on what Zubulake means now: "By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records--paper or electronic--and to search in the right places for those records, will inevitably result in the spoliation of evidence."[90]

First the court identifies the standard of care. Without going into the details of the case itself, the issue between the parties was not the egregious or willful destruction of property, nor acting out of bad faith, but rather a matter of carelessness and indifference involved in the collection efforts after the duty to preserve was apparent. Nonetheless, the court found that even in situations in which there is an absence of bad faith, there can still be a finding of gross negligence or willfulness, depending on the circumstances. At a minimum, there can be a finding of negligence where two things happen: 1) duty to preserve arises, and 2) party fails to preserve evidence. Furthermore, the court found that the

88 *Id.*
89 *Id.*
90 *Id.*

failure to "take all appropriate measures to preserve ESI [electronically stored information] likely falls in the category of negligence."[91]

The duty arises when a party "reasonably anticipates litigation." The court states, however, that there is no bright line as to when this is, but that each case is circumstantial on its own facts. The court states that this in fact can be well before litigation has begun, since the timing of litigation can be controlled. Again, when this duty arises, a party must suspend its routine document retention/destruction policy and initiate a "litigation hold" to ensure the relevant documents are preserved and not destroyed. Should a party not adhere to these standards of care, sanctions may and most likely will ensue and such sanctions depending on the category of negligence could be huge.

The court concludes with another element of consideration for future litigating parties, in addition to the final opinion of Zubulake's 2004 decision:

"While litigants are not required to execute document productions with absolute precision, at a minimum they must act diligently and search thoroughly at the time they reasonably anticipate litigation." Also that, "Parties need to anticipate and undertake document preservation with the most serious and thorough care, if for no other reason than to avoid the detour of sanctions,"[92] which she later describes as a process [sanction motions] that is "very, very time consuming, distracting and expensive for the parties and the courts."[93]

This decision clearly brings into question the validity of litigation hold solutions that depend heavily on the custodians to preserve their own documents. Using these types of litigation hold products, an organization issues hold notifications to all relevant custodians within the organization, informing them that they must cease the destruction of documents and preserve all ESI related to a particular matter. This approach to litigation hold hardly qualifies as "preservation with the most serious and thorough care," given that there are technologies available that allow an organization to easily preserve ESI without relying on the individual custodians.

When litigation is anticipated, the only way to effectively and promptly preserve all relevant ESI is to collect that data remotely, in an automated, forensically sound manner. This requires an enterprise-class technology, such as AccessData eDiscovery. While AccessData eDiscovery is not the only enterprise-class e-discovery solution on the market, it is the only "end-to-end" e-discovery solution with built-in litigation hold and final review capabilities. Furthermore, it is the only solution of its kind that enables the forensic collection of both structured data and unstructured data, which means

91 *Id.*
92 *Id.*
93 *Id.*

an organization is able to promptly preserve ESI anywhere it is located across the enterprise, from custodian computers, network shares, email servers, and structured repositories, such as Enterprise Vault or SharePoint and cloud based email.

Using AccessData eDiscovery, an organization is able to issue and manage litigation holds, forensically preserve relevant ESI, process that data, analyze it, and produce it. By addressing each phase of the electronic discovery process, with a single solution, including litigation hold and final attorney organizations greatly reduce the risk of spoliation, since they will not be migrating ESI from one tool to the next.

Furthermore, the same is true with regard to preservation, as AccessData eDiscovery enables forensic collection of both structured and unstructured data, so the organization will not have to employ two or more collection tools to preserve ESI. Only through the use of a technology this comprehensive is an organization able to meet the standards of care set forth in the Pension Committee opinion, as well as ensure the most seamless and prudent approach to the e-discovery process as a whole.

Search Issues and AccessData Technology

The issue of search scope is unusually relevant in the field of digital evidence and digital forensics. Warrants and scope of search rules were all crafted around the simple realties of the physical world. The idea behind this is that a warrant sets down the scope of the allowable investigations and any evidence found by searching outside of the permitted scope is not admissible. In the physical world these rules are easy to understand and easy to comply with. However, in the digital world, they are not nearly as transparent.

The question investigators often face when they have a warrant to search a computer related to a specific matter is:

What am I allowed to do before I step outside the rights granted by the warrant?

While there is no blanket answer to this question, the case of *United States v. Mann*[94] sheds some light on the issue. In this case, Mann was charged with possession of child pornography. The pornography was found on Mann's computer subsequent to a search of his computer equipment under a search warrant. In the course of the investigation, the investigating officer utilized FTK®, which was described as "software commonly used by many forensic computer examiners,"[95] to image and analyze four items of the suspect's digital media. The investigator did not limit his

94 *United States v. Mann*, 2008 WL 1701743 (N.D. Ind., April 8, 2008)
95 *Id.* at *2.

search by file timestamp, file name, file location, or by any other criteria. Indeed, the investigator utilized the known file filter (KFF) technology provided by FTK® to remove standard system files from his search, as well as detect any known instances of child porn. When the investigator found files known to be child pornography, he looked at them "without obtaining another search warrant."[96]

The defense challenged the admissibility of the evidence, because the warrant was granted pursuant to an issue of voyeurism and not pornography and therefore, "the search exceeded the scope of the warrant."[97] Specifically, the defense argued that the specific language of the search warrant authorized officers to search for "video tapes, CDs or other digital media, computers, and the contents of said computers, tapes or other electronic media to search for images of women in locker rooms or other private areas"[98] as opposed to child pornography. However, Mann argued "that upon suspecting child pornography, the police officers were required to obtain a separate warrant."[99]

The court ruled that "[t]he search was executed within the scope of its authorization, with limited exceptions" and that the evidence should therefore be admitted. The court provided the following reasoning for allowing the evidence:[100]

1) "The warrant did not, by its terms, restrict the police officers from viewing files that might have been downloaded to Mann's computer. The warrant did not restrict the officers from decrypting files or viewing files that had been erased. The warrant did not restrict the police officers from viewing files related to Mann's internet activities, newsgroup participation, computer files, e-mail, papers and business records, jacks, adaptor cords.[101]

2) "A police officer may properly seize evidence of a crime without a warrant if: (a) a law-enforcement officer is lawfully present, (b) an item not named in the warrant (or, likewise, outside the scope of consent) is in the plain view of the officer, and (c) the incriminating nature of the item is immediately apparent (i.e., the government can show probable cause to believe the item is linked to criminal activity).[102]

The plain view doctrine cited is of particular importance in computer forensics, both to law enforcement and to corporate practitioners. Not only is it well tested within U.S. courts,[103] but many corporate customers have utilized the plain view doctrine when conducting network-based forensic investigations to ensure that evidence found in the course of a search is admissible.

United States v. Graziano

In *United States v. Graziano*,[104] the court provided even stronger language supporting the broad interpretation of warrants relative to digital evidence. In this case, FTK® was again used to search and analyze a computer and again the defense challenged the admissibility of the data on the

96 *Id.* at *3.
97 *Id.* at *1.
98 *Id.* at *5.
99 *Id.*
100 *Id.*
101 *Id.*
102 *Id.* citing *United States v. Raney*, 342 F.3d 551, 558-59 (7th Cir. 2003); *United States v. Bruce*, 109 F.3d 323, 328-29 (7th Cir. 1997).
103 See, e.g., *United States v Wong*, 334 F.3d 831 (9th Cir. 2002); United States v. Gray, 484 F.2d 352 (6thCir. 1973).
104 *United States v. Graziano*, 558 F.Supp.2d 304, 75 Fed. R. Evid. Serv. 1220 (E.D.N.Y. Mar 20, 2008). But see, *United States v. Hamilton*, 579 F.Supp.2d 637, 77 Fed. R. Evid. Serv. 874 (D.N.J. Sep 28, 2008).

grounds that "the warrant is facially overbroad and invalid because it did not require a certain search methodology or limit the search of computers to certain keywords or terms." In this case the court explicitly addresses the issue of search terms and found the following:

> "[T]here is nothing in the language of the Fourth Amendment, or in the jurisprudence of the Supreme Court or the Second Circuit, that requires such a rule in the context of a search of computers. See *Dalia v. United States*.[105] ("Nothing in the language of the Constitution or in this Court's decisions interpreting that language suggests that...search warrants also must include a specification of the precise manner in which they are to be executed.")[106]

In fact, the Supreme Court has noted that, as a general matter, "it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search authorized by warrant."[107] The reason for not imposing a protocol requirement on law enforcement in conjunction with search warrant applications for computer searches is obvious—in most instances, there is no way for law enforcement or the courts to know in advance how a criminal may label or code his computer files and/or documents which contain evidence of criminal activities. In other words, to require courts in advance to restrict the computer search in every case to certain methodologies or terms would give criminals the ability to evade law enforcement scrutiny simply by utilizing coded terms in their files or documents, or placing such documents in areas of the computer that would not normally contain such files/documents. In today's technological age, a computer should not be a safe-haven for criminals to hide evidence of their criminal activities by unnecessarily limiting law enforcement's ability to search only certain files/documents on a computer with a certain name or term, or located in a certain area of the computer hard drive. Therefore, although the Second Circuit has not decided this precise issue, this court declines to adopt a rule that would invalidate search warrants which did not contain a specific methodology explaining how the computers would be searched."[108]

While neither case enables a blanket statement to be made regarding the admissibility of digital evidence obtained as part of a warrant-based search, the case law is fairly robust in its support of the plain view doctrine and the open-ended searching of digital media when the warrant doesn't explicitly limit the scope.

---

105 *Dalia v. United States*, 441 U.S. 238, 257, 99 S.Ct. 1682, 60 L.Ed.2d 177 (1979).
106 *Id.*
107 *Dalia*, 441 U.S. at 257, 99 S Ct. at 1682.
108 *Id.*

Mobile Phone Search and Seizure Issues

Reconciling advancements in technology, like the advent of mobile devices such as cellular phones, digital cameras, and tablet computers, with the Fourth Amendment has become a difficult proposition for many courts. And, if Moore's law, or the idea that computing power continuously doubles and will continue to do so for the foreseeable future, is to be any guide the ability to search and seize information found on mobile devices becomes ever more relevant.

While the Fourth Amendment protects against unreasonable search and seizure, the examination of data found on cell phones and similar devices has become increasingly commonplace. Still, the search and seizure of these mobile devices have the same requirements of any other traditional search and are still subject to the same exceptions, such as a search incident to arrest and exigent circumstances.

Searches of mobile devices need not "necessarily be conducted at the moment of arrest or even after arrest. [The 9th] Circuit has held that a search and seizure may occur before or after the arrest if probable cause has developed for the arrest and the search and seizure are 'substantially' contemporaneous."[109] Furthermore, searches can also be conducted of an arrestee's personal effects.[110] In *United States v. Finley*, police took the defendant's cell phone they had found on his person and conducted a search pursuant to the defendant's arrest. The court found that the search was lawful and that the "reasonable search" was not "constrained to search only for weapons or instruments of escape on the arrestee's person; they may also, without any additional justification, look for evidence of the arrestee's crime on his person in order to preserve it for use at trial."[111]

Numerous courts have attempted to tackle the question of searches of mobile devices incident to an arrest. For example, in *People v. Diaz*, 165 Cal. App. 4th 732, 81 Cal. Rptr.3d 215 (2d Dist. 2008), the defendant's cell phone was seized from his person incident to his arrest, but the cell phone itself was searched 90 minutes later. The court, upholding the validity of the search, noted that "courts have upheld delayed warrantless searches of wallets (see, e.g., *United States v. Passaro*, 624 F.2d 938, 944 (9th Cir. 1980)) purses (*People v. Decker*, 176 Cal.App.3d 1247, 1252 (1986), 222 Cal. Rptr. 689), and pagers (*United States v. Chan*, 830 F.Supp. 531, 536 (N.D.Cal 1993)).[112] A number of other courts have relied on the exigent circumstances exception to the warrant requirement to justify the search of cell phones.[113]

Still, the decisions continue to be mixed. Courts in cases like *United States v. Edwards*,[114]

109 *Schlossberg v. Solesbee*, --- F.Supp.2d ---- (2012), 2012 WL 141741, quoting U.S. v. Smith, 389 F.3d 944, 952 (9th Cir.2004) ("A search incident to arrest need not be delayed until the arrest is effected. Rather, when an arrest follows 'quickly on the heels' of the search, it is not particularly important that the search preceded the arrest rather than vice versa.")

110 *U.S. v. Robinson*, 414 U.S. 218, 236, 94 S.Ct. 467, 38 L.Ed.2d 427 (1973).

111 *United States v. Finley*, 477F.3d 250 (5th Cir. 2007).

112 In their opinion, the Diaz Court addressed both *Finley* and *Edwards*, as well as *United States v. Chadwick,* 433 U.S. 1 (1977).

113 See, e.g., *United States v. Ortiz*, 84 F.3d 977 (7th Cir.1996) (warrantless search of pager to preserve electronic evidence); *United States v. Zamora*, 2006 WL 418390, *4, 2006 U.S. Dist. LEXIS 8196, *31-32 (N.D.Ga. Feb. 21, 2006) ("In this case the phones were reasonably believed by the investigating agents to be dynamic, subject to change without warning by a call simply being made to the instrument. With each call is the risk that a number stored would be deleted…."); *United States v. Mercado-Nava*, 486 F.Supp.2d 1271 (D.Kan.2007) (interest in preserving destruction of evidence justified warrantless search incident to arrest of cell phone information); *United States v. Parada*, 289 F.Supp.2d 1291 (D.Kan.2003) (because stored telephone number data on cell phone was easily lost warrantless search of cell phone incident to arrest valid).

114 *United States v. Edwards,* 415 U.S. 800 (1974).

United States v. Park,[115] *State v. Smith*,[116] and *Schlossberg v. Solesbee*[117] have found that while the information found or stored on a cell phone may be similar to that found in an arrestee's wallet, the sheer volume of information that can be stored on a cell phone affords the holder thereof a greater expectation of privacy to the data stored therein, and makes them subject to a Fourth Amendment analysis. The Northern District of California, on the other hand, found in *United States v. Hill*, that the amount of information that may or may not be found on a cell phone is irrelevant, and as such, the cell phones could be subject to search as long as the arrest itself was lawful.[118]

Indeed, mobile devices today can contain vast amounts of data which may be relevant to an arrest, and knowing what to look for and how to look for it can prove challenging.

AccessData software allows investigators to acquire and analyze evidence from more than 3,500 mobile devices incident to an arrest.

Options are incorporated into the software to allow the investigator to examine only specific areas of the device, such as call history or SMS, or preserve everything. Officers can even create customized reports at the scene of the device seizure.

United States v. Gomez

Perhaps Judge Ursula Ungaro said it best, by describing the current status of the topic in *U.S. v. Gomez*, 807 F.Supp.2d 1134, 1153 (2011) (holding that evidence obtained from Defendant's cell phone was properly obtained), stating that "[a]s many courts have already opined, the scope of a cell phone search incident to arrest is presently in flux and, with every increasing advance to cell phone technology and memory capacity (not to mention the advent of new portable devices such as iPads), the question on how to deal with them will become increasingly important."

Voice over Internet Protocol (VoIP) Interception & Analysis

While Forensic Toolkit® is used to analyze mobile phone data, another AccessData technology, SilentRunner, can be used to intercept, analyze, and preserve Voice over Internet Protocol data. Voice over Internet Protocol (VoIP) refers to voice traffic over an Internet Protocol (IP) based broadband network. There are three types of VoIP services: computer to computer, telephone to computer, and telephone to telephone. The main distinction to the landline telephonic communication is not how the communication is given or received, but rather in the data conversion that occurs during VoIP transactions. VoIP converts ordinary audio telephone

115 *U.S. v. Park*, 2007 WL 1521573, at *8-9.
116 *State v. Smith*, 920 N.E.3d 949
117 *Schlossberg v. Solesbee*, --- F.Supp.2d ---- (2012), 2012 WL 141741.
118 *U.S. v. Hill*, 2011 WL 90130 at *8.

signals into data packets that are sent over the Internet using Internet Protocol.[119] Because of the conversion into data packets, the VoIP transaction is not treated as telecommunications services but as information services.

Southwestern v. Mo. PSC

In *Southwestern v. Mo. PSC*,[120] the court followed the Federal Communications Commission ("FCC") interpretation of VoIP classification:
that it is a hybrid service, which has both telecommunications and information components and that because of its "capabilities for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information," VoIP falls "exclusively within the information service category if the telecommunications and information services are sufficiently intertwined." Furthermore, the court in *Vonage v. Minn. PUC*[121] interpreted the Communications Act of 1996 and concluded that the VoIP service provided by Vonage "constituted an information service, because it offers the 'capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications.'" The distinct categorization of VoIP transactions as information services weakens the argument that these communications are protected from wiretapping, as were the old landline telecommunications.

The Fourth Amendment and the Federal Wiretap Act of 1968 are the two bodies of law that grant wiretapping protection. In *Katz v. United States*,[122] the U.S. Supreme Court interpreted the Fourth Amendment and stated the two part test of when a person's telephone calls are protected:
1) a person must have a "reasonable expectation of privacy" and 2) the expectation must be one that society is prepared to recognize as reasonable. Katz only applies when the government is an actor or a private party is acting on behalf of the government. The Federal Wiretap Act, however, protects parties against third-party interception of telecommunications and information services, although there is a reduced protection when it is deemed information services. Incidentally, courts have permitted the interception of Internet data under the Act, since most of the time the data is stored on the third party's computers.[123]

The distinguishing features between the two are that third-party interception of landline phone calls requires tapping physically into the telephone line and listening in real time, whereas VoIP transactions store data and interception only requires a personal computer and some enabling software. The FCC went on record to state that "it does not matter that there is a `voice' at both ends of an IP-PSTN call [computer to phone VoIP]. The same is true of voicemail, which the FCC has long recognized is an information service."[124]

On the issue of VoIP interception in the workplace, privacy protection would be addressed in the same way as it would with data traversing the network. The very relationship as employee and employer would subject the data to some level of monitoring by the employer-the exceptions

119 Bick, Jonathan, Calculating Hidden VoIP Costs, N.J. L.J. (Nov. 07, 2007), a copy of which is available at: http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=900005495393
120 *Southwestern Bell Tel., L.P. v. Mo. PSC*, 461 F.Supp. 2d 1055, 2006 U.S. Dist. LEXIS 65536 (E.D. No., 2006), affm'd. *Southwestern Bell Tel., L.P. v. Mo. PSC*, 530 F.3d 676; 2008 U.S. App. LEXIS 13062; 45 Comm. Reg. (P & F) 540 (8th Cir. 2008).
121 *Vonage Holdings Corp. v. Minn. PUC*, 290 F.Supp. 2d 993 (D. Minn. 2003).
122 *Katz v. United States*, 389 U.S. 347 (1967).
123 Calculating, supra, note 112.
124 In *re Schools and Libraries Service Support Mechanisms*, 18 F.C.C.R. 9202, P29 n. 49 (2003).

being the telephone and any mail through the U.S. Post Office.[125] Once again the categorization of VoIP as an information transmission and also the existence of the employee-employer relationship would sum up the protection level of VoIP transmissions to a reduced level of protection. Most companies have a policy statement explaining the scope of their monitoring and monitor such communications in the ordinary course of business, which allows for a lesser degree of privacy protection for the employee. Interception of personal matters or non-consensual interception by companies are highly discouraged and, in fact, is protected against by the Electronic Communications Privacy Act.[126]

While the same information can be transmitted through landline or VoIP, the two different platforms of sending the message can change who is allowed and not allowed to listen in on the call. VoIP transmission technology is growing rapidly, because of its low cost and bandwidth efficiency. Therefore, it is an issue to be tracked closely until a definite answer is given on what can and cannot be intercepted.

RAM Analysis: Be Prepared

Everyone in the forensics industry knew it was inevitable, but just the same, everyone dreaded the day the courts woke up to the true relevance of information contained in random access memory ("RAM"). Nonetheless, that day has come and we now have several key court decisions, such as *Columbia Pictures Industries Inc. v. Bunnell*,[127] in which the preservation of data contained in RAM was deemed both discoverable and relevant. Similar cases have found that information contained in similar areas is also subject to discovery. In *Victor Stanley, Inc. v. Creative Pipe, Inc.*, the court found "[t]he general duty to preserve may also include deleted data, data in slack spaces, backup tapes, legacy systems, and metadata."[128] This was also discussed in Zubulake, where the court found that discovery obligations apply not only to "electronic documents that are currently in use, but also documents that may have been deleted and now reside only on backup disks."[129] While the actual instances are still rare, that dynamic is clearly set to change as the amount of RAM available on a standard computer continues to rise exponentially, and particularly with the widespread use of so-called "virtual machines."

One should expect that, in the near future, seizure of RAM by law enforcement agencies will become standard best practice. AccessData's users are particularly well positioned when this shift occurs, because all of our products contain the ability to both acquire and analyze RAM. In fact, there is no difference from the perspective of the user between the acquisition and analysis of RAM and that of more traditional memory.

125 See, e.g., *United States v. Kassimu*, 188 Fed. Appx. 264, 2006 WL 1880335 (5th Cir. 2006) (computer records authenticated by witness with personal knowledge).
126 Electronic Communications Privacy Act of 1986, 18 U.S.C. §2510 et. seq.
127 *Columbia Pictures Indus. v. Bunnell*, 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. June 19, 2007), motion for rehearing den'd, 2007 U.S. Dist. LEXIS 63620 (C.D. Cal. Aug. 24, 2007).
128 *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 524 (D.Md.2010).
129 *Zubulake v. UBS Warburg, LLC*, 217 F.R.D. 309, 316 (S.D.N.Y.2003)

Predictive Coding

The idea of having to review a large set of documents to find those that are relevant to a case is nothing new in the legal field. Typically, this meant that a team of attorneys would be tasked with reviewing each of these documents, one by one, searching for key words which would help separate the relevant documents from the irrelevant. Such a process could take months and cost an exorbitant amount in legal fees.

Predictive coding technology has changed this. By taking a seed set of sample documents, AccessData's software can be trained to recognize what sort of document qualifies as relevant. Once trained, the software can conduct the search on its own, potentially saving a great deal of time and a massive amount in legal fees.

While some may believe that human review is superior to that done by a computer, Grossman and Cormack found in their article on the topic that this idea "is strongly refuted. Technology-assisted review can (and does) yield more accurate results than exhaustive manual review, with much lower effort."[130] Furthermore, in addition to producing more effective results, Grossman and Cormack found that electronic review through the use of predictive coding "require[s], on average, human review of only 1.9% of the documents, a fifty-fold savings over exhaustive manual review."[131]

Finally, lawyers can now feel comfortable using predictive coding technologies in the discovery process, thanks to a landmark decision by U.S. Magistrate Judge Andrew J. Peck. In *Moore v. Publicis Groupe*,[132] Judge Peck said in his February 24, 2012 decision that "computer-assisted review is an available tool and should be seriously considered for use in large-data-volume cases where it may save the producing party (or both parties) significant amounts of legal fees in document review." *Moore v. Publicis Groupe*,[133] Peck also ruled that the use of electronic search does not violate Federal Rule of Evidence 702 or Daubert, since Rule 702 and Daubert are used to ensure reliable expert testimony at trial, not the methods by which documents are searched for during discovery. Id. Finally, while attorneys may have been cautious about using the technology in the past, "[c]ounsel no longer have to worry about being the 'first' or 'guinea pig' for judicial acceptance of computer-assisted review."[134]

While labor-intensive manual review may still have its place in legal discovery, it is clear that the use of predictive coding can not only have strong benefits over the traditional methods, it can surpass them in many respects. It has not only been proven through independent research, but has been approved for use in federal court. The benefits offered by AccessData's predictive coding software should be seriously considered by any team faced with large-data-volume cases.

130 *Maura R. Grossman & Gordon V. Cormack, Technolgy-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review*, Rich. J.L. & Tech., Spring 2011, at 48.
131 *Id.* at 43.
132 Case No. 11-CV-1279
133 11 CIV. 1279 ALC AJP, 2012 WL 607412 (S.D.N.Y. Feb. 24, 2012)
134 *Id.*

Social Media and E-Discovery

Social media has become a mainstay of many people's lives. Two-thirds of the Internet community is logged onto some social media site[135] where they can post nearly anything about themselves and communicate with hundreds of people at the stroke of a computer key. Social media is defined as a form of electronic communication (as Web sites for social networking and microblogging) through which users create online communities to share information, ideas, personal messages, and other content (as videos).[136] While social media sites such as Facebook®, Twitter® and LinkedIn® may bring ease into everyday communications, it becomes a huge hurdle for corporate attorneys and organizations from a legal perspective. As technology introduces more and more avenues of communication, counsel must also be informed of these changes and know how to tackle the hurdles since the American Bar Association ("ABA") Model Rules mandate counsel be competent to represent its clients and be abreast of technology.[137] Furthering this rule and applying it to the present day, the *Griffin*[138] court stated that "it should now be a matter of professional competence for attorneys to take the time to investigate social media sites."

With the voluminous number of postings people place daily on their social media sites, certain posts are bound to become controversial or subject to being part of some investigation or litigation. The type of claims brought against people on social media sites can vary from criminal, employment, insurance claims, and family to trademark infringement cases. The difficulty comes from various areas. This includes the fact that social media sites are on a third party site behind an organization's firewall, which leads to the question of retrieval. Remember, attorneys have an obligation to preserve through legal holds. However, how much does a counsel have to review in terms of social media sites and how does the counsel tackle privacy issues related to social media sites? The model legal hold, attorney's ethics, admissibility and authentication, and retrieval all become issues derived from social media sites.

Unfortunately the courts have not given a thorough and precise way for counsel to tackle issues involving social media in e-discovery. However there have been some cases that could give guidance on how counsel should approach the issues. In *Guest v. Leis*[139] the court stated that when there are privacy settings available for the user of the social media site and the user has not applied any privacy settings, then those materials available to the public are discoverable. The same held for the case *EEOC v Simply Storage Management*[140], where the court compelled production of relevant content from social media and stated that "an expectation of privacy is not a basis of shredding discovery" and stated that information that is already shared has less privacy expectations. However, not all courts have allowed discovery of social media sites. In *Crispin v. Audigier*, the court allowed the defendant's

135 Neilsen report
136 Merriam-Webster's Dictionary
137 ABA Model Rules 1.1
138 *Griffin v. Maryland*
139 *Guest v. Leis*, 255 F.3d 325 (6th cir 2001).
140 *EEOC v. Simply Storage Management.*

discovery material to be protected under the Stored Communications Act,[141] and stated that the messages on Facebook® and MySpace® were not public and therefore could not be compelled to produce. Though this case prevented the exchange of information on a social media site, it aligns with the standard of privacy expectations where messages intended to be private were found less discoverable than those that are viewable by the public or were once public. Moreover, Facebook® and MySpace® sites have policies that state there is no expectation of privacy.[142]

Once admissibility has been determined, counsel would most likely think about authentication of what is being requested or produced. Authentication has not been a difficult hurdle to overcome once the court has compelled production of the information on social media sites. In *Treat*,[143] the court allowed printed copies with time stamps of the social media sites to be admissible. In *Lorraine*,[144] circumstantial evidence produced would authenticate the discovery using metadata and hash tags.

The rules of litigation holds apply in every aspect to counsel regarding social media e-discovery. Once a litigation hold is in place, the duty to preserve is greater, and counsel cannot rely on self-preservation by the custodians. The obligation to collect and ensure data is not being destroyed remains very much the case. Spoilation after a legal hold is in effect makes the sanctions that much greater as well. In the case of *Lester v. Allied Concrete Co*,[145] the defendant's attorney placed a litigation hold then advised its employees to "clean up" all incriminating Facebook photos. The court sanctioned this attorney $522,000 for his spoliation of evidence. Once a litigation hold is in place everyone, especially the counsel, should be on notice that no evidence, whether it is on a computer on a physical document or even on a social media site, can be destroyed.

Conclusion

While it is true that neither the current case law nor the Federal Rules of Civil Procedure directly specify technology, it is equally true that together they provide companies with some very clear key requirements. AccessData's eDiscovery solution is the only solution on the market that matches all of these requirements in full. The enterprise-class architecture allows an organization to not only search thousands of computers in a matter of days, but delivers the most comprehensive data access capabilities available. AccessData eDiscovery can search and collect from every widely accepted operating system, every major email type, and search and collect from more than 30 of the most common data repositories, including Oracle URM, Documentum, OpenText, FileNet, SharePoint, and Symantec's Enterprise Vault. The technology supports a number of data collection options, including capturing complete forensic images or forensic acquisition of individual files that support native file production with metadata preservation. All collections performed using AccessData technology can be made in a forensically sound manner, meaning

141 *EEOC v. Simply Storage Management, LLC*, 270 F.R.D. 430, 434 (S.D. Ind. 2010).
142 *Crispin v. Audigier*
143 *Treat v Tom Kelly Buick Pontiac*
144 *Lorraine v. Markel Am Insurance Company*
145 *Lorraine v. Markel Am. Ins. Co.*, 241 FRD 534 (D. Md. 2007).

that the collected data is not altered and that all relevant metadata is preserved. Finally, the solution has built-in litigation hold capabilities and integrates with other market-leading litigation hold products for those organizations that have already implemented a litigation hold technology. As the most comprehensive e-discovery technology on the market, AccessData eDiscovery is the soundest choice for an organization looking to reduce the risks and costs associated with electronic discovery.

AccessData in Court

AccessData's FTK® is the standard computer forensic product used by the U.S. Federal Bureau of Investigation. As such, FTK® is constantly being recognized by courts as an effective tool to extract and analyze electronically stored information. In addition to the cases mentioned in the main body of this document, here are a few more representative cases:

United States v. Mann, 592 F.3d 779 (7th Cir. 2010) cert. denied, 130 S. Ct. 3525, 177 L. Ed. 2d 1106 (U.S. 2010).

In this child pornography case, a laptop and external hard drive were seized into evidence and examined using FTK®. After his motion to suppress evidence was denied, 2008 WL 1701743, the defendant entered a conditional guilty plea and then appealed. Here, the court found that "there is no reason to believe that [the detective] exceeded the scope of the warrant by employing the FTK® software without more". In the motion to dismiss, the court indicated that FTK® is a "software commonly used by many forensic computer examiners." FTK® had been used for various purposes of the computer investigation, including by not limited to KFF alerts (known file filter) and uncovering websites that the defendant had visited.

United States v. Haymond, 2009 WL 3029592 (N.D. Okla, Aug 28, 2009)

In the case of Haymond, where the defendant was charged with possession of child pornography, the government made a mirror image of defendant's hard drive, on which it allegedly found images of child pornography. Defendant's expert, David Penrod, at the Regional Computer Forensic Laboratory ("RCFL") in Denver, CO, failed to find ANY pornographic images on the mirrored hard drive using EnCase Software, owned by Guidance Software. In response, defendant made a motion to compel, requesting access to the evidence against him. The court then directed Penrod to try again to access the images. The second time, Penrod used AccessData's Forensic Toolkit® (FTK®) and was successful in finding 78 images containing child pornography. In making an appeal, *United States v. Haymond*, 672 F.3d 948 (10th Cir. 2012), the defendant did not dispute the evidence discovered through the use of FTK®, but rather other various procedural aspects of his charges, and the conviction was affirmed.

United States v. Moreland, 665 F.3d 137 (5th Cir. 2011).

In this child pornography case, the defendant had previously been convicted of child pornography charges and sentenced to 51 months imprisonment and five years of

supervision after release. At trial, the prosecution had relied on evidence gathered from the defendant's home computers, which he shared with other various members of his family. In examining the computers, Columbus, MS, police had used Forensic Toolkit® (FTK®) to recover thousands of images, 112 of which were identified as being potentially pornographic. The prosecution also relied on usage patterns and browser history in presenting its case. In analyzing the Defendant's appeal, the court eventually ruled that the joint custody and use of the computers by other members of the defendant's family created enough reasonable doubt to overturn the conviction. The existence of the 112 images discovered through use of FTK® was never disputed, however.

United States v. Perocier, 269 F.R.D. 103 (D.P.R. 2009)

Here, multiple defendants had been charged with conspiracy to commit mail fraud. The defendants moved to exclude the testimony of an expert enlisted by the government. At a Daubert hearing, the expert testified that he had used Forensic Toolkit® (FTK®), and in particular, FTK Imager. He testified that the program "is the industry standard, used by 'virtually every' federal agency", and that in his view, "FTK Imager is 'absolutely reliable' and he has never heard of any problem or inaccuracy arising with the program". Perocier at 110. The defendants did not object to the expert's status as an expert, and the motion to exclude the testimony was denied.

Smith v. Slifer Smith & Frampton/Vail Associates Real Estate, LLC, 2009 WL 482603 (D. Colo. Feb. 25, 2009)

In a hearing related to real estate transactions, the Magistrate found and concluded that defendants had responded to an RFP by submitting the results of a Forensic Toolkit® (FTK®) report.

United States v. Underwood, 2010 WL 5313766 (W.D. Ky. Dec. 20, 2010)

In this memorandum opinion and order relating to child pornography charges, the court noted that Forensic Toolkit® software had been used to retrieve images from the defendant's computer, and that the evidence was validly seized pursuant to the warrant issued. MD5-hash values were used to verify that the evidentiary hard drive was identical to the source drive.

United States v. Tummins, 2011 WL 2078107 (M.D. Tenn. May 26, 2011).

In this Memorandum and Order in response to a defendant's Motion to Compel Discovery in a child pornography case, FTK® was used to discover evidence related to the government's case against the defendant.

United States v. White, 779 F. Supp. 2d 775, (N.D. Ill. 2011)

In this hate crime case, the FBI used FTK® to conduct a forensic analysis on digital media that had been seized by the FBI, "which would enable them to search for specific articles and words." White at 781. The government's expert used FTK® to find particular website posts made by the defendant, and would have had to "scroll through years of entries, comprising thousands of posts, to find … " the evidence in question without using FTK®. Id. at 787, 801.

State v. Howe, 159 N.H. 366 (2009)

In *State v. Howe*, the government was successful in prosecuting defendant of unlawful possession of child pornography with the help of FTK®. Defendant's landlord found printed pornographic images,

some of which depicted children, as well as a CD containing similar images. These items were found amongst the defendant's possessions left behind after he vacated an apartment, from which he had been evicted. In an effort to support the evidence against defendant, Detective Craig used FTK® to analyze a computer belonging to defendant's friend. Defendant had the closest access to this computer. Craig generated a report using FTK®, which revealed that the computer had been used to access child pornography and also confirmed that the images found in defendant's apartment were on the analyzed computer. Since there were no fingerprints found on the CD, the FTK® analysis was successful in proving defendant as the owner of the CD by definitively illustrating the times when these images were searched for and downloaded. The court stated that the combination of the report's information and the testimony of witnesses constituted "clear proof" that defendant was responsible for the child pornography found on the computer.

United States v. Potts, 2008 WL 2051090 (D. Kan. 2008).
In this case, the defendant moved to suppress evidence gathered through an "overly broad" search warrant. Attachment B of the warrant "lists evidence pertaining to images of child pornography, and sexual activity with children." Id. at *5. "The search warrant authorized a search of defendant's residence, including any computers and electronic storage devices found in defendant's residence." Id. The judge noted that the examiner of the computer, Sergeant Owen, "did not engage in an impermissibly broad search for the items listed in the warrant." Id. at *22. Because, "[w]hile the warrant allowed Sergeant Owen to open every file and look at the first few pages, he did not need to do so because such a broad search is unnecessary with modern forensic software." Id. at *21. The court specifically identified "forensic software, including Forensic Toolkit"® (FTK®). Id. at *10.

Tauck v. Tauck, 2007 Conn. Super. LEXIS 2618 (Conn. Super. Ct., Sept. 21, 2007).
In a bitter divorce case, which cost more than $13 million in legal fees for both sides, computer forensics was used to determine whether allegations made by Nancy Tauck against her husband, Peter Tauck, were valid. Nancy Tauck accused her husband of possessing child pornography, and Peter Tauck's old Toshiba laptop was one of the materials seized and examined. An expert from Global CompuSearch LLC, a computer forensics service provider, examined the laptop for the husband and served as his expert witness, testifying at the trial. After forensic analysis, Marcus Lawson, president of Global CompuSearch LLC, refuted the claims made by Nancy Tauck. Global CompuSearch was given six hard drives to examine in which there were found numerous "suspect" images. However, it was also discovered that 148 of those images were downloaded on May 5, 2005, which was the date Peter Tauck's passport verified that he was in Tahiti. The question then became: "From what location were the images downloaded?" Global CompuSearch found an Internet Protocol ("IP") address that led them to conclude the download took place from within the state of Connecticut, where the wife was at the time. The forensic expert further stated that he found no evidence that anyone had altered the system date on the computer.

Furthermore, Global CompuSearch found that a substantial number of files on other computers had been deleted from the Internet cache folders. With this information, they were able to illustrate that some deliberate action was taken to eliminate information on that computer so there would be no Internet browsing history to show which sites were visited. The Court found that the evidence did not corroborate Nancy Tauck's allegations and that it was clear that the download of the suspected photographs took place when Peter Tauck was half way across the globe. The Court concluded from the forensic evidence that Nancy Tauck, or other unknown persons, planted the images onto the computer while Peter Tauck was away.

Commonwealth v. Koehler, 914 A.2d 427 (Pa. Super. 2006).
In this criminal case, the Court found that there was reasonable suspicion to conduct a warrantless property search of a parolee's residence and computer. The search resulted in a computer forensic analysis that uncovered sufficient evidence that Mr. Koehler possessed child pornography. The computer forensic examination of Koehler's computer hard drive was performed by Erie County Detective Jessica Lynn, who used FTK® to analyze the images on Koehler's computer. Detective Lynn discovered 235 video clips depicting children and more than 300 items that were suspect as child pornography. Detective Lynn's findings against appellant resulted in 19 charges filed against him, which lead to Koehler being sentenced to 12 to 24 months of incarceration for each of his fourteen counts.

United States v. Calimlim, 2005 WL 2922193 (E.D. Wis., November 4, 2005).
The government's examiner used FTK® to search data and unallocated space, which included emails, the Internet, typed documents, and deleted items. The examiner conducted the forensic examinations using the keyword and scanning methodologies available in FTK®.

United States v. Fumo, 2007 WL 3232112 (E.D. Pa, October 30, 2007).
In this case, the government had used FTK® to examine Fumo's computer system. The defendant moved the court to compel the government to disclose the search protocol and keyword terms under Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure in order to determine whether the search and seizure violated his Fourth Amendment rights. The Court concluded that the "requested information [was] not material to application of the exclusionary rule" and denied the motion.

United States v. Luken, 515 F.Supp.2d 1020 (D.S.D, August 21, 2007).
In this opinion, the Magistrate Judge recommended that the defendant's motion to dismiss be denied. The Magistrate determined that the defendant had consented to the search of his laptop, and the evidence of child pornography found using FTK® by the agent was admissible.

United States v. Richardson, 583 F.Supp.2d 694 (W.D. Pa. October 31, 2008).
Agents used FTK® to search the defendant's laptops, where child pornography was found.

Gutman v. Klein, 2008 WL 4682208 (E.D.N.Y., October 15, 2008).
In this civil action, the defendant was suspected of accessing the website www.ntfs.com and deleting

files from a laptop before handing over the device for discovery. The plaintiff's examiner used FTK® to image the hard drive of the laptop. The court-appointed forensic expert, Stroz Friedberg, referenced in his report that FTK® version 2.2 is an "accepted tool under industry standards, to perform the imaging and create a forensic duplicate of the hard drive."

State v. Voorhees, 2008 WL 2579709 (Ohio App. 3 Dist., June 30, 2008).
In a child rape case, the state's forensic examiner used FTK® to find more than 1,700 images of child pornography and videos on the defendant's computer and under which account they existed and/or were accessed.

United States v. Graziano, 558 F.Supp.2d 304, 75 Fed. R. Evid. Serv. 1220 (E.D.N.Y., March 20,2008).
In an arson case, the defendant moved to suppress fruits of the search of his home and computer. "In terms of the procedure employed during the search of the computer, [the examiner] used a software package called Forensic Tool Kit ("FTK"), which searches through the entire file system..." Id. 558 F.Supp.2d at 313. "In the instant case, when the files were sorted by FTK, [the examiner] recognized that there was a significant amount of evidence found in the internet history files." Id. at 314. Further utilizing FTK®, the examiner was able to identify a file "search [3].htm" that contained evidence of "an AOL search using the terms 'arson rico laws' at one time in the search box." Id. The court concluded that "the examiner's search of the computer and discovery of that evidence was executed in a manner that was within the scope of the warrant and was reasonable under the Fourth Amendment." Id. at 317.

United States v. Sage, 2007 WL 4592074 (W.D.Mo., December 27, 2007).
In this statutory rape case, a motion to suppress the computer evidence was denied. The forensic examiner used FTK® to examine the defendant's computer and used FTK® to organize the materials and retrieve the evidence that linked the defendant to the under-aged victim and other younger males.

United States v. Gaynor, 2008 WL 113653 (D.Conn., January 4, 2008).
This opinion focused on a motion to provide copies of ESI to defendants who were charged with possession of child pornography. The Adam Walsh Act prohibited the defendants from obtaining copies of child pornography (even as evidence) limited its exposure to the defendants by requiring any viewing to be done at a government facility. The Court acknowledged FTK® and EnCase as the most commonly used forensic tools used by forensic examiners for computer investigations. The government offered to provide defendant's examiner with a computer that met the minimum system requirements for both FTK® and EnCase so that an examination could be conducted.

United States v. Flinn, 521 F.Supp.2d 1097 (E.D. Cal., October 16, 2007).
In Flinn, the defendant was charged with receiving and possessing child pornography. The government seized the defendant's computer where he had allegedly received and stored the child pornography. Due to the Adam Walsh Act, the government could not release any copies or

duplicative material since the material contained child pornography. Rather, under 18 U.S.C.A. § 3509(m)(2)(B), the government was required to provide the defendant "ample opportunity for inspection, viewing, and examination at a government facility." The Court recognized this statute to mean that the government can supply "reasonably up to date hardware and software tools and facilities such that a defendant can construct a reasonable, available forensic defense." The facility used was the former McClellan Air Force Base, where computers were available with all of the relevant materials to perform a forensic analysis. The software implemented and made available for use was FTK-1 which the Court recognized as a "standard." The court found that the available hardware and software provided was sufficient to uphold the defendant's discovery rights and thereby denied the defendant's motion to use its own facilities to examine mirror images of the evidence on their own computer.

United States v. Eberle, 2006 WL 1705143 (W.D. Pa, June 15, 2006).
In Eberle, the question was whether certain ESI was on a particular computer. The question was resolved using FTK®, whereby "Detective Lynn performed a more targeted search known as a 'hash value check,' whereby she searched for a specific identifier, known as an MD5 hash, that is particular to an internet image, much like a fingerprint. This hash check similarly failed to uncover any of the images that had been uploaded onto the Yahoo! Server in 2001." Id. at *2.

United States v. Aldeen, 2006 WL 752821 (March 22, 2006).
Defendant Ahmed Aldeen moved the Court to order the government to provide him with a mirror image of his computer hard drive allegedly containing images of child pornography. This case was prosecuted prior to the Adam Walsh Act that enables the government to prevent release of any material or copies of materials seized that involve child pornography. At the time however, the court did find the defense argument so convincing that it allowed the defendant's computer experts to utilize their own personal computers so that they could run two computer programs, one being FTK®, to examine the videos.

In re Atlantic Intern. Mortg. Co., 352 B.R. 503, 509 (Bankr. M.D. Fla. 2006).
In this bankruptcy proceeding, attorneys for the debtor hired a forensic examiner to conduct an investigation of certain electronic documents, and the examiner used FTK® to perform the examination.

Sanders v. State, 191 S.W.3d 272 (Tex.App. - Waco, March 8, 2006).
In this case, the examiner, who was trained and well versed in FTK®, discovered multiple instances of child pornography on the defendant's computer. The Appellate Ccourt refused to overturn the lower court's acceptance of the expert's testimony.

United States v. Butts, 2006 WL 3613364 (D. Ariz., December 6, 2006).
In this Adams Walsh Act issue, the government moved the court to limit defendant's access to the electronic evidence. Since the Adams Walsh Act was effective after the filing of the present case, the court had the option of denying the government's motion for reconsideration. However, the court granted the government's motion and limited the defendant's ability to review the evidence. FTK® was used by the defendant's expert to examine the evidence.

Notes:

Notes:

AccessData Group has pioneered digital investigations and litigation support for more than twenty years and is the maker of the industry-standard computer forensics technology, FTK, as well as the leading legal review technology, Summation. AccessData provides a broad spectrum of stand-alone and enterprise-class solutions that enable digital investigations of any kind, including computer forensics, incident response, e-discovery, legal review, IP theft, compliance auditing and information assurance. More than 130,000 users in law enforcement, government agencies, corporations, consultancies, and law firms around the world rely on AccessData software solutions, as well as our premier hosted review and digital investigations services. AccessData Group is also a leading provider of digital forensics and litigation support training and certification, with our much sought after AccessData Certified Examiner® (ACE®) program and Summation certification program.

Come learn why our e-discovery solutions are consistently ranked among the leaders in analysts coverage of the market space, by visiting AccessData.com.

AccessData Group
384 South 400 West Suite 200
Lindon, UT 84042 USA
801.377.5410