EDDE JOURNAL

A Publication of the E-Discovery and Digital Evidence Committee
ABA Section of Science & Technology Law

SUMMER 2011 VOLUME 2 ISSUE 3

The Collection and Use in a French Courtroom of Digital Evidence Stored in an Employee's Computer and Evidentiary Use of Written Exchanges Made via Social Media

By Mathilde Houet-Weil

France, where individual freedom is highly prized, is a bastion of workplace privacy. French rule of law finds support in Article 8 of the European Convention on Human Rights, which provides a right to respect for one's private life, family life, home and correspondence, subject only to restrictions deemed strictly necessary in a democratic society. In addition, Article 9 of the French Civil Code provides that everyone has the right to respect for his private life. Both of these provisions apply to employees in the workplace and during working time. The employee's right to privacy extends to conversations and communications that take place at work or within work systems. *Read more*

Rule 1 and Information Governance – The Bookends of Cost-Effective e-Discovery

By Phillip Favro

The Decree from Rule 1 to Discover Efficiently and Cost Effectively
The e-Discovery frenzy that has gripped the American legal system over the past decade has become increasingly expensive. Particularly costly are inquiries into an organization's data management practices and production efforts. These investigations are lengthy and often disruptive to business operations. Just as troubling, they increase the expense and duration of litigation. Given these cost and delay issues, it is no wonder that jurists are looking for alternative methods to rein in "promiscuous discovery." *Read more*

The Legality of Digital Image Copies of Paper Records (Part 2)

By Robert F. Williams and Hon. Ronald J. Hedges

5. Technical and Conceptual Issues Relating to Digital Image Copies
This section addresses three technical issues associated with digital image copies and concludes that digital image copies are as acceptable as the original paper records in any legal proceeding. **5.1 The Role of Digital Image Formats** The conversion of paper and icrographic records to digital image copies is accomplished using a digital scanner. The scanner divides every page into a very detailed grid of literally millions of picture elements ("pixels"). The reflectivity value of these pixels then is automatically measured by the scanner *Read more*

Virginia Becomes First Jurisdiction to Authorize Online Notarization

By Timothy Reiniger and Dr. Richard Hansberger

On March 26, 2011, Virginia enacted a law that authorizes online notarization by means of internet video/audio conference technology. Using these provisions, the signer does not need to appear physically in front of a notary but may elect to appear before the notary online. The law becomes effective July 1, 2012. Following years of discussion and speculation about the future of "cyber notaries" at the ABA, this marks the first time that remote notarization has been authorized in the United States. *Read more*

The Collection and Use in a French Courtroom of Digital Evidence Stored in an Employee's Computer and Evidentiary Use of Written Exchanges Made via Social Media

By Mathilde Houet-Weil

France, where individual freedom is highly prized, is a bastion of workplace privacy. French rule of law finds support in Article 8 of the European Convention on Human Rights, which provides a right to respect for one's private life, family life, home and correspondence, subject only to restrictions deemed strictly necessary in a democratic society. In addition, Article 9 of the French Civil Code provides that everyone has the right to respect for his private life. Both of these provisions apply to employees in the workplace and during working time. The employee's right to privacy extends to conversations and communications that take place at work or within work systems.

The right of the employee to dignity and therefore to a private life has been implemented into strong workplace privacy protections through the French Labour Code. For example, the French Labour Code prohibits the collection of worker information without prior notice and consultation with employee representatives. When the information collected through surveillance and monitoring qualifies as personal, an employer must also notify an employee prior to installation and use of any surveillance or monitoring device[1]. The French Labour Code also establishes that any activity, including surveillance and monitoring, that restricts an employee's rights and freedom must be proportional to, and justified by, its purpose.[2] As a consequence, surveillance in the workplace is inherently viewed as posing a threat to an employee's privacy, and therefore must be transparent, proportional and justified.

With the rise of the digital age, the debate on privacy in the workplace increasingly concerns data stored in an employee's computer used for professional purposes.

Over the past decade, French employment courts have seen an ever-growing range of employment litigation in which digital evidence is key. This typically occurs, for instance, in unfair competition cases where an employee sets up a competing business during work hours, using an employer's assets to poach clients.

When an employee has engaged in such disloyal activity, the critical steps taken by an employer of searching, examining, collecting and preserving evidence found on an employee's computer may likely determine the outcome of any resulting employment litigation. The French courts have provided significant guidance on each of these critical steps as the admission of hard drives, internet files and emails as courtroom evidence in employment disputes has become increasingly common.

---

[1] Article L. 1222-4 of the French Labor Code
[2] Article L. 1121-1 of the French Labor Code

The admissibility of digital evidence is a particularly sensitive issue in French civil procedures where evidence is almost exclusively in a written format. Court testimony is seldom used and instead witness statements are submitted. Witness depositions/examinations and discovery are unheard of in the French system.

Therefore unfair competition cases in an employment context rely heavily on digital evidence available in an employee's computer. Moreover the concept of employment at will does not exist in France and thus failure to prove that an employee's dismissal is well grounded exposes an employer to damages for unfair dismissal. Such damages can reach 2 to 3 years of salary, depending on the seniority at hand. Accordingly, an employer who discovers an employee's disloyal activity and wishes to sack the employee on the spot should take time to elaborate a strategy that will enable it to secure available digital evidence before declaring war on the employee.

Computers placed at the employee's disposal by the employer remain the employer's property and are supposed to contain only limited information related to the employee's private life. However, personal use of the company's computer is allowed provided that such use is reasonable and does not affect the employee's work and the company's activity.

This situation raises the question of ownership of the data stored by an employee on a computer placed at his disposal by his employer and highlights the need to balance the personal dignity of employees with the proprietary interests of employers.

In France, as opposed to the United States, computer data stored on a corporate asset and created using corporate systems does not automatically qualify as company property.

The French Supreme Court, based on the starting point that workers have a right to privacy even in the workplace – although this principle is not cited as such in the French Labour Code - , has developed case law on digital evidence over the past ten years, setting precedents which may disconcert an American observer.

This article addresses the admissibility of employee emails and computer files in the courtroom as well as the use of an employee's browsing history. Particularly noteworthy is a recent court ruling, which, for the first time, rendered a decision on the admissibility of messages posted on the Facebook wall of an employee.

1. The collection and use in a courtroom of digital data created by a disloyal employee

1.1. Employers must respect the privacy of disloyal employees, according to the French Supreme Court

During working hours, sitting in his company office and using the tools put at his disposal by his employer, an employee sets up and operates a competing business, poaches his employer's clients, thereby generating shadow revenues to his benefit. The employer becomes suspicious, searches the

corporate computer and prints out volumes of digital data proving the employee's disloyalty and terminates the employee. In a wrongful termination suit, is this evidence admissible? According to the French Supreme Court in a 2001 decision,[3] the answer was "no." The Court determined that the employer violated the privacy to which an employee is entitled even when working. The fact that a corporate policy forbids any private use of the company computer was irrelevant. The employer was ordered to pay the employee(i) wages for what would have been the notice period prior to cessation of employment,(ii)wages for paid holidays, (iii) a severance indemnity and (iv) damages for non justified loss of employment.

With this ruling, the French Supreme Court established a strong precedent that favoured employee's privacy over the protection of the company's interests and left employers somewhat at a loss.

In a 2005 case, an employer found erotic pictures in an employee's office drawer. The employer then searched the employee's computer and opened a file flagged as "personal." The employee was sacked for gross misbehaviour on the basis of the non-professional data stored in the personal file opened by the employer. According to the French Supreme Court, however, this digital data was deemed inadmissible evidence. The French Supreme Court adopted an analysis used in an earlier case involving the personal locker of an employee. The Court analogized that the same privacy protection applies to personal computer files as it does to a personal locker.[4] The Court further indicated that erotic pictures found in the employee's drawer did not create a particular risk allowing the employer to open personal computer files.

While this decision favoured the employee, the French Supreme Court nevertheless created an exception to its stringent 2001 precedent;[5] the employer can access and use the private files of an employee if the company is facing particular risks.[6]

The French Supreme Court provided further guidance in 2006 when it determined that emails and files stored in an employee's work computer or in the office are presumed to be work-related – and therefore accessible by the employer and admissible in court, except if they are flagged as "personal" or "private"[7]. With this new precedent, the French Supreme Court further softened the effects of its 2001 ruling ,[8] which had been criticized as over-protective of disloyal employees.

As a consequence of the 2005 and 2006 rulings, any email or document that is not labelled "personal" or "private" – either by its name or by the file where it is stored – can be opened and used in court by

---

[3] Cour de cassation (chambre sociale), 2 octobre 2001, n° 99-42.942, JSL n° 88-2
[4] Cour de cassation (chambre sociale), 11 décembre 2001, Juris-Data n° 2001-012121 ; Bull. civ. 2001, V, n° 377
[5] See note 3 above
[6] Cour de cassation (chambre sociale), 17 mai 2005, n° 03-40.017
[7] Cour de cassation (chambre sociale), 18 octobre 2006, n° 04-48.025, F-P+B, Le Fur / SARL Technisoft, Juris-Data n° 2006-035418
[8] See note 3 above

the employer. Moreover, emails and documents that are flagged "personal" or "private" can be opened when the company is facing particular risks.

It should be noted, however, that whether a document label is sufficiently marked as "personal" is decided by the courts on a case-by-case basis. For example, the French Supreme Court held in 2009 that a file named "JM" after an employee's initials (Jean-Marc) was not sufficiently labelled as "personal"; its content was therefore admissible evidence[9]

Opening a private email is a criminal offence known as violation of private correspondence, which is sanctioned by one-year imprisonment and a 45,000 euros fine[10]. Nevertheless, employees seldom seek redress in the criminal court because the employment-law procedure – in which an employee may also seek damages – might be adjourned until the criminal judge renders a final decision.

1.2. Best practice to collect and preserve digital evidence created by a disloyal employee

When an employer collects digital evidence to be used against an employee, the employee may question the authenticity of the collected data and claim that the employer planted evidence in his work computer.

It is therefore advisable to request in court the appointment of a bailiff who will be assigned, with the assistance of an IT expert, to collect all relevant data in the employee's computer. This procedural route was expressly set forth by the French Supreme Court in 2005.[11]

With this procedure, the court will precisely delineate bailiff's assignment, adapting the description requested by the plaintiff in his brief, in order to ensure that an employee's privacy is protected. The bailiff's assignment will be strictly limited to the disloyal activity presumably carried out by the employee and the bailiff will not be able to collect any other private data.

The bailiff will then issue a certified report with a print-out of all relevant data which authenticity is thereby guaranteed.

Once the employer becomes suspicious of an employee's activity and begins to anticipate litigation, it is advisable to immediately remit the computer to the bailiff who will sequester it during the time of the procedure. The procedure further reduces the risk of the employee successfully arguing that evidence was planted in the computer.

Some particular situations may be encountered, jeopardizing the outcome of such procedure:

[9] Cour de cassation (chambre sociale), 18 octobre 2009, n° 05-38.492
[10] Article 226-1 of the French Criminal Code
[11] See note 5 above

- What if the computer is in the hands of the employee, as is commonly the case with a laptop? A summons to appear in court may certainly lead an employee to delete all relevant data from the computer before submitting it to the court-appointed bailiff.

  In that case, the employer can file a "one-sided" motion to the court, that is a motion that is not disclosed to the other party. If the motion is granted and a bailiff is appointed by the court, the bailiff will seize the computer without providing advance notice to the employee. At that time of seizure, the bailiff notifies the employee of the employer's motion and of the court order granting such motion. The employee can then challenge the court order and seek the annulment of the motion and the subsequent seizure. In order to obtain such annulment, the employee will have to prove that the facts presented by the employer in his "one-sided" motion are inaccurate or were not serious enough to justify the seizure of the computer.

- What if the employee works from a home office and the computer is therefore located in the home? Can a court-appointed bailiff enter an employee's home without consent and seize the company computer?

  Yes, when the employee has a dedicated room for a home office and the employer pays an indemnity for the professional use of this room. In that case, the home office space is regarded as a professional space from which the bailiff can seize the computer.

  In such an instance, a court will usually order that the bailiff be assisted by a police officer and a locksmith to ensure that the seizure takes place.

- What if the employee, anticipating that the computer may be searched, deletes all relevant data before the bailiff can seize the computer?

  The employer may hand the computer over to a private IT firm who will be able to restore the data. An employee is likely to dispute the authenticity of any damaging evidence found since the private IT firm is not an independent third party, but is instead hired and paid by the employer in anticipation of litigation.

  This situation can be avoided if an employer asks the court to appoint an independent expert who will restore the data deleted by an employee pertaining to the disloyal activity.

  As mentioned above, digital evidence pertaining to the employee's disloyal activity is key to avoid payment of damages for unfair dismissal. It is also key in an unfair competition claim brought before the commercial court against a competing company established by an employee with the use of a former employer's assets.

2. An employer can use as court evidence the list of websites browsed by his employee

The internet activity of an employee on a company computer can tell a lot about whether the mind of the employee is focused on professional tasks or on personal business.

For this type of evidence, the French Supreme Court has ruled in favour of employers and has found that websites browsed by an employee with a company computer are presumed to have a professional nature. Therefore, an employer can access a history of sites browsed even in the absence of the concerned employee presence.[12]

In one noteworthy case, an employee spent more than 40 hours per month on the internet, visiting websites with content unrelated to work. Following the above mentioned precedent, the French Supreme Court found that the browsing history, including dates and times, was admissible evidence. The employer was therefore able to prove that the employee abused the right to use the internet for personal purposes, laying cause for dismissal.[13]

In another instance, an employee used the company computer during working time to access pornographic websites, store a wide amount of explicit data and exchange many emails with internet-users met on these websites. The employer filed a criminal complaint against the employee for misuse of corporate assets. The French Supreme Court found for the employer and declared that the use of corporate tools for a time-consuming activity unrelated to the employee's professional tasks constituted the criminal offence of misuse of corporate assets.[14]

In cases involving visits to child pornography websites, such activity of an employee is criminal and the employer bears an obligation to report such offence to the Public Prosecutor. Therefore it is the duty of an employer, when he has reasonable suspicion that an employee is engaged in such criminal activity, to investigate and collect digital evidence of said activity.

Generally speaking, it is recommended that a bailiff collect the data pertaining to browsed websites in order to ensure authenticity of such data.

3. Facebook: friends of your friends may not be your friends

A French saying goes "*The friends of my friends are my friends.*" This may not be true on Facebook.

Three employees of the same company carry on a discussion on the Facebook wall of one of them. The discussion takes place on a Saturday night from the employees' respective homes. Two of the employees welcome the third one in a "club", the purpose of which is to "make fun" (in slang language) of their boss all day long without her noticing, and more generally to be a real pain in the

[12] Cour de cassation (chambre sociale), 9 juillet 2008, n° 06-45.800, L. v. Sté Entreprise M., Jurisdata n° 2008-044801
[13] Cour de cassation (chambre sociale), 18 mars 2009, n° 07-44.247, X v. Sté Lauzin
[14] Cour de cassation (chambre criminelle), 19 mai 2004, n° 03-83.953

neck for her. The privacy settings of the employee hosting the conversation enable his friends and his friends' friends to have access to the wall.

One of his friends' friends comes across the conversation, prints it out and hands it over to the employer.

All three employees are dismissed on the spot (a severe measure under French employment law because usually a notice period is granted).

The dismissed employees sought redress in an employment court and claimed that it is the employer who misbehaved when it peeked on the Facebook wall because it "introduced" itself in a private space without being invited. Furthermore, they argued that the conversation was of a humoristic nature, as shown by the slang language used and the "smileys" posted in their messages. The employees asserted that their actions constituted joking, from their homes and in their private time.

The employer replied that it did not peek at the wall but that a print-out of the conversation was handed over to it by someone who had authorized access to the wall, in his capacity as "friend of a friend". The employer also noted that eleven employees had access to the wall and that the reported conversation was detrimental to the company's interests. According to the employer, the three employees abused their freedom of speech and could legitimately be dismissed without notice.

In this case at hand, a 2010 decision of the employment court held that the evidence found on the Facebook wall was admissible.[15] By granting access to his wall to his friends' friends, the employee hosting the conversation made his wall a public space – or rather a semi-public one. Moreover, the court determined that the content of the messages was abusive and therefore not protected under freedom of speech; the dismissals without notice were grounded.

This 2010 decision is the first decision rendered in France on Facebook evidence. The employees have appealed this lower court decision. The decision of the Appellate Court is much anticipated by employment-law practitioners. The Appellate Court may be tempted to reverse the lower court decision which ruling appears to be quite harsh on the employees in the French employment-law environment where employees' rights are carefully protected.

Facebook conversations among colleagues are the virtual equivalent of casual conversations around the coffee machine. Facebook users as well as email users exchange informal comments in writing, typing as quickly as they would speak and without thinking of the consequences. The line between speaking and writing is blurred as one writes instead of speaking. The line between private and professional time is also blurred as emails or Facebook messages carelessly written from home outside working time may under certain prerequisites be admissible as court evidence against the employee.

[15] Conseil de prud'hommes de Boulogne Billancourt, 19th November 2010, Mme S v. Sté Alten Sir, Juris-Data n° 2010-021303

While a conversation at the coffee machine may be overheard by a handful of colleague and soon be forgotten by all, new technologies and social media in contrast turn informal conversations into written evidence that can be brought into the courtroom. Blogs, trivial social interactions, emails and "LOL" moments are preserved indiscriminately and may be examined by a judge outside their context.

After having worked for big Anglo-American law firms, Mathilde Houet-Weil joined WEIL & ASSOCIES in order to develop the labour law department. Mathilde gives advice to heads of personnel departments of big multinational groups in the context of restructurings (company strategy in terms of staff and competences, redundancy programs, closing downs, company transfers, relocation abroad), management of employment and dismissal of executives (expatriation etc). Mathilde also dedicates a part of her work to corporate law and advices the clients of the firm in corporation management (AGM, capital increase...), as well as extraordinary events (commutation, contribution or sale of assets, squeeze out of shareholders etc).

Generally, her double French-American education enables her to represent the interests of Anglo-American groups in a global context. Her knowledge of the German language and culture has made it possible for her to become, since her beginnings in Berlin, a privileged contact person for French-German business relationships. Mathilde graduated from the school for interpreters and translators in Paris in English and in German after four years of studies. She studied law at Paris II (Panthéon-Assas), and has participated at the Erasmus Program at the University of Utrecht, Netherlands. Mathilde has acquired the LL.M of Duke Law University, USA, and is admitted to practice at the New York Bar. Mathilde speaks and writes fluently French, English and German.

Rule 1 and Information Governance – The Bookends of Cost-Effective e-Discovery

By Phillip Favro

The Decree from Rule 1 to Discover Efficiently and Cost Effectively

The e-Discovery frenzy that has gripped the American legal system over the past decade has become increasingly expensive. Particularly costly are inquiries into an organization's data management practices and production efforts. These investigations are lengthy and often disruptive to business operations. Just as troubling, they increase the expense and duration of litigation. Given these cost and delay issues, it is no wonder that jurists are looking for alternative methods to rein in "promiscuous discovery."[1] The latest approach is found in Federal Rule of Civil Procedure 1.

Rule 1 establishes a compelling directive that is tailor made for e-Discovery. More than just a vestigial preamble to the Federal Rules, Rule 1 requires the "just, speedy, and inexpensive determination of every action and proceeding."[2] And courts are recognizing the value of Rule 1's decree to address unreasonable e-Discovery expenses and delays. Indeed, the Tenth Circuit just invoked Rule 1 to affirm dismissal of a lawsuit for discovery abuses that were unreasonably lengthening and delaying that case.[3] Other recent cases have also drawn on this cost-cutting theme to dispose of e-Discovery disputes.[4]

Pursuing Rule 1's Decree by Implementing Effective Information Governance Procedures

Rule 1 thus provides a powerful message to litigants – and their counsel – to discover information efficiently and cost effectively.[5] Organizations that are looking to do so should consider whether they have an effective plan for storing and managing data. Implementing such a plan will typically help a company prepare for litigation. At the same time, it will reduce storage costs, eliminate data stockpiles and minimize litigation risks. With an effective information governance plan, a company will store data that must be kept for business, legal or regulatory purposes – and nothing else.

---

[1] Calcor Space Facility, Inc. v. Superior Court, 53 Cal.App.4th 216, 223 (1997) (urging courts to "aggressively" curb discovery abuses which, "like a cancerous growth, can destroy a meritorious cause or defense").

[2] Fed. R. Civ. P. 1.

[3] Lee v. Max Intern., LLC, --- F.3d --- (10th Cir. 2011) (dismissing plaintiffs' action after they failed to produce relevant documents in response to two court orders).

[4] *See* Surowiec v. Capital Title Agency, Inc., No. 09-cv-2153 (DGC), slip op. at 9 (D. Ariz. May 4, 2011) (reasoning that "judicial efficiency and the prompt resolution of litigation" supported a terminating sanction given defendants' evidence destruction and the resulting delays it caused); Nycomed U.S. Inc. v. Glenmark Generics Ltd., No. 08-CV-5023 (CBA)(RLM), slip op. at 11 (E.D.N.Y. Aug. 11, 2010) (imposing monetary sanctions on defendants for the "undue delay" caused by their discovery failings).

[5] Fed. R. Civ. P. 1, advisory committee's note, 1993 Amendment ("The purpose of this revision . . . is to recognize the affirmative duty of the court . . . to *ensure that civil litigation is resolved* not only fairly, but also *without undue cost or delay*. As officers of the court, *attorneys share this responsibility with the judge* to whom the case is assigned") (emphasis added); Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. SCI. & TECH. L. 1, 3 (2007) (noting that counsel "must adopt new rules of engagement to effectively represent her clients" in the digital age).

In contrast, an informal approach to storing or managing data will frequently leave a company unprepared for litigation. And this, in turn, usually leads to higher litigation fees as outside counsel tries to navigate a labyrinth of unorganized information and procedures to find responsive materials. It may also hamstring a company with increased data storage costs and greater exposure to litigation risks.

To appreciate the importance of information governance, the problems with an informal data management must first be identified and understood. Only then can a discussion of effective information governance procedures make sense.

The Issue with Informal Pre-Litigation Data Management: Employee-Delegated Archiving

So what is the real problem with an informal approach to pre-litigation records management? Without a formal plan, a company unwittingly – or even intentionally – delegates its data management to rank and file employees. This leads to inconsistent retention of company data, which begets further problems.

For example, a company will generally keep more electronic data than it otherwise would. While this will increase storage costs, the effects might be worse. The surplus of data may include information that could be damaging in future litigation.

A company may also fail to retain important documents. This may be due to the programmed operation of computer systems or because employees neglect to keep such information. Employees may also destroy or modify documents in order to cover their mistakes.

e-Discovery history demonstrates that any of these scenarios could very well lead to a litigation disaster. In *Northington v. H & M International*, the court issued an adverse inference jury instruction against a company that destroyed significant emails and other data.[6] The company failed to keep those records because it took no thought to implement pre-litigation information governance procedures. For example, the company neglected to establish a formal document retention policy.[7] Instead, "data retention . . . was evidently handled on an ad hoc, case-by-case basis."[8] This lack of organization eventually led to the loss of key data and the court's sanctions award.[9]

The Issue with Informal Response Protocols: Employee-Led Preservation Effort

The same attitude of carelessness regarding pre-litigation records management is often manifested in the identification, preservation and collection of data required during litigation. Companies leave too much discretion in the hands of operations-level employees to keep what they feel is relevant without oversight from legal counsel. This allows an employee to have the "last word" on preservation

[6] Northington v. H & M International, No. 08-cv-6297, slip op. at 22 (N.D. Ill. Jan. 12, 2011), *aff'd*, (Feb. 14, 2011).
[7] *Id*. at 7-8, 16.
[8] *Id*. at 8.
[9] *Id*. at 16.

regardless of that employee's training, knowledge, level of sophistication or even connection to the alleged claims.[10]

Such a laissez-faire response to litigation is typically disastrous. Documents that should be preserved for production are instead inadvertently (or intentionally) lost. The *Green v. Blitz* case is a quintessential example of the problem with this informal approach.[11]

In *Green*, the company was sanctioned for failing to properly identify, preserve and collect responsive electronic information.[12] The defendant company lost key emails after entrusting a single, lay employee with the identification and collection of discoverable documents.[13] That employee had little if any supervision from counsel. Moreover, the employee – who was in the thick of the alleged wrongdoing – was not technically sophisticated.[14] Nevertheless, he did not involve IT to help identify or collect the electronic data.[15] As a result, entire categories of relevant data were destroyed and the company was sanctioned accordingly.

The *Northington* case is also instructive on this issue. In *Northington*, the company neglected to establish global litigation response procedures.[16] Into this vacuum stepped rank and file employees – some of whom were accused by the plaintiff of harassment – who were tasked with identifying and collecting discoverable emails from their workstations.[17] Predictably, key documents were never found and the court had little choice but to inform the jury that the company destroyed evidence.[18]

Suggested Practices for Implementing Effective Information Governance Procedures

An organization does not have to suffer the same fate as the companies in *Green* and *Northington*. It can take charge of its data – both before and during litigation – through effective information governance. While the specifics will vary from one organization to the next, successful information governance will typically incorporate the following elements.

Cooperation among Records Management Stakeholders

An organization needs to get its key records management stakeholders on the same page regarding what data (especially email) will be kept and for what length of time. This is an important step because a holistic information governance approach cannot be adopted without cooperation by legal, IT,

---

[10] *See* Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, LLC, 685 F.Supp.2d 456, 473 (S.D.N.Y. 2010) (explaining that plaintiffs' litigation hold was insufficient since it relied on lay employees to identify responsive documents without the assistance of counsel).
[11] Green v. Blitz U.S.A., Inc., No. 2:07-CV-372 (TJW), slip op. (E.D. Tex. Mar. 1, 2011).
[12] *Id*. at 7, 9.
[13] *Id*. at 3, 6.
[14] *Id*. at 6.
[15] *Id*. at 6, 8-9.
[16] Northington v. H & M International, No. 08-cv-6297, slip op. at 7-8 (N.D. Ill. Jan. 12, 2011).
[17] *Id*. at 17 ("defendant never tasked anyone other than the custodians themselves to search their computer hard drives, hard copy documents, or other sources for potentially relevant evidence.").
[18] *Id*. at 16-17.

business units and records managers. Should these key players fail to jointly develop an information management strategy, their organization may very well repeat the mistakes that plagued the defendants in *Northington* and *Green*.

Establish a Records Retention Policy

After devising a global data management plan, a company must then establish and observe retention policies that carry out its decisions on data preservation.[19] A document retention policy is essential to ensuring that only pertinent data is retained.[20] The *E.I. du Pont de Nemours v. Kolon Industries* decision from this spring is particularly instructive on this issue.[21]

In *du Pont*, the plaintiff manufacturer defeated a sanctions motion due to its effective information governance procedures.[22] The manufacturer implemented a document retention policy that typically kept emails from former employee accounts for 60 days, after which the emails were overwritten and deleted.[23] The manufacturer also promulgated a course of action whereby the retention policy would be promptly suspended on the occurrence of litigation or other triggering event.[24] This way, email build-up could be reduced until a litigation event required otherwise.[25] Because the manufacturer faithfully observed those procedures, it decreased a stockpile of email and was still protected from court sanctions.[26]

Similarly, in *Viramontes v. U.S. Bancorp*, the defendant bank relied on its data governance protocols to stave off a sanctions motion after overwriting several years of email.[27] Because those emails were destroyed pursuant to a neutral retention policy before a preservation duty attached, the bank was protected from sanctions under the Federal Rule of Civil Procedure 37(e) safe harbor for the destruction of electronic information.[28]

Deploying Archiving Software to Enforce Retention Protocols

Coupling retention policies with archiving software is another crucial step toward taking charge of an organization's data. Archiving software will enable employees to access their stored email and other documents without allowing them to delete or otherwise modify the archived materials. Moreover, such software can be programmed to ensure that electronic data is kept for legal and regulatory purposes, while discarding other materials. Finally, an intelligent archiving solution will also have a

---

[19] Micron Technology, Inc. v. Rambus Inc., --- F.3d --- (Fed. Cir. 2011) (reasoning that organizations may lawfully discard data before a preservation duty is triggered by implementing neutral document retention policies).
[20] See Philip J. Favro, *Sea Change or Status Quo Has the Rule 37(e) Safe Harbor Advanced Best Practices for Records Management?*, 11 MINN. J.L. SCI. & TECH. 317, 342-43 (2010).
[21] E.I. du Pont de Nemours and Co. v. Kolon Industries, Inc., No. 3:09-cv-58, slip op. (E.D. Va. Apr. 27, 2011).
[22] *Id*. at 14, n.9, 16.
[23] *Id*. at 3.
[24] *Id*.
[25] *Id*.
[26] *Id*. at 14, n.9.
[27] Viramontes v. U.S. Bancorp, No. 10 C 761, slip op. at 4-5 (N.D. Ill. Jan. 27, 2011).
[28] *Id*. at 3-5.

litigation hold mechanism which allows an organization to suspend aspects of its retention policies to ensure that data subject to a preservation duty is actually retained.

Deploying archiving software would have saved countless litigants from sanctions. For example, in *Suntrust v. AIG United Guaranty*, several key emails that supported the defendant's arguments were electronically altered by a Suntrust employee to bolster the plaintiff's claims.[29] When the truth eventually came out, Suntrust's credibility – and pocketbook – took a hit.[30] Archiving software could have led to a different result. While the software would have allowed the employee to access her emails, it could be tailored to prevent their contents from being modified. Likewise, in *Northington*, the employees would not have been able to discard the key evidence that brought down sanctions in that case. These and other recent decisions make clear that an archiving solution provides a superior alternative to leaving information governance to rank and file employees.[31]

Preparing a Litigation Response Effort

Last but not least, a company should act like litigation will happen – for in today's economic climate, it almost certainly will. An organization should therefore develop an internal process for how it will address document productions in litigation. This will undoubtedly help once the company is involved in a lawsuit.[32]

Such a process will typically include the designation of company officials who are responsible for:

- Issuing and ensuring compliance with a litigation hold,
- Suspending certain aspects of the company's document retention policies, and
- Overseeing employees as they work with legal counsel to identify, collect and preserve relevant data.

This will help a company keep document identification and collection out of the exclusive control of it employees. For no matter how sophisticated they may be, "[m]ost non-lawyer employees . . . do not

[29] Suntrust Mortg., Inc. v. AIG United Guar. Corp., No. 3:09-cv-529, Slip Op. at 3-4 (E.D. Va. Mar. 29, 2011).
[30] *Id*. at 15-16, 28.
[31] *See*, *e.g.*, Antonio v. Security Services of America, LLC, No. AW-05-2982, at *4 (D. Md. Mar. 29, 2010), *aff'd*, (D. Md. July 19, 2010) (sanctioning defendants for directing their employees to discard electronic documents except those the employees deemed "essential"); Pension Committee of University of Montreal Pension Plan v. Banc of America Securities, LLC, 685 F.Supp.2d 456, 473 (S.D.N.Y. 2010); Phillip M. Adams & Assoc., L.L.C. v. Dell, Inc., 621 F. Supp. 2d 1173, 1193-94 (D. Utah 2009) (holding that defendants inappropriately entrusted their "operations-level employees" with ultimately decision-making authority over "what information is relevant to the enterprise and its data retention needs").
[32] *See* Hannan v. Dusch, 153 S.E. 824, 831 (Va. 1930) ("The law helps those who help themselves, generally aids the vigilant, but rarely the sleeping, and never the acquiescent.").

have enough knowledge of the applicable law to correctly recognize which documents are relevant to a lawsuit and which are not."[33]

Conclusion

Using effective data governance procedures to rein in a company's information will yield court approval. Implementing those procedures will help a party store, manage and discover its information efficiently and cost effectively. They will reduce data proliferation, decrease storage expenses and lessen litigation risks. All of which will ring true with Rule 1's decree since that organization will be facilitating a cost effective approach to e-Discovery.

Philip Favro is a Discovery Attorney for Symantec Corporation in Mountain View, California. Phil brings to Symantec practical expertise in electronic discovery. Phil advised technology companies and other clients regarding complex e-Discovery issues during his eleven-year litigation practice. Phil's expertise has been enhanced by his legal scholarship. His line of research addresses the changes and challenges that electronic data have forcibly introduced into litigation and, in particular, on discovery practice. Phil now works with Symantec customers and company stakeholders on information governance and e-Discovery matters. Phil has been a licensed member of the California State Bar since 1999. He belongs to the American Bar Association and is a member of the ABA's Science & Technology Section. Phil is also a member of the Electronic Document Retention and Production (WG1) Working Group of the Sedona Conference. Phil previously chaired the Santa Clara County Bar Association's High Technology Law Section and was a member of its Board of Trustees. Phil also serves as a Judge Pro Tempore for the Santa Clara County Superior Court.

[33] Northington v. H & M International, No. 08-cv-6297, slip op. at 17 (N.D. Ill. Jan. 12, 2011).

The Legality of Digital Image Copies of paper Records (Part 2)

By Robert F. Williams and Hon. Ronald J. Hedges

5. Technical and Conceptual Issues Relating to Digital Image Copies

This section addresses three technical issues associated with digital image copies and concludes that digital image copies are as acceptable as the original paper records in any legal proceeding.

5.1 The Role of Digital Image Formats

The conversion of paper and micrographic records to digital image copies is accomplished using a digital scanner. The scanner divides every page into a very detailed grid of literally millions of picture elements ("pixels"). The reflectivity value of these pixels then is automatically measured by the scanner resulting in "dots" that then are converted to a stream of bits (zeros and ones) which collectively represent a "bit map," an image manifesting the original paper record. There are instances where color scanning is desirable. Users, however, should recognize that color creates exponentially larger bit map files – an unnecessary added operational cost for black-and-white business records. Black-and-white scanning therefore is overwhelmingly used to convert paper records to digital image copies.

Digital scanners convert paper or micrographic records to one of three widely recognized image formats: TIFF, PDF and JPEG. All of these formats use compression algorithms (such as ITU Group 3 or 4)[1] to reduce the size of the stored image:

- *TIFF (Tagged Image File Format)* – TIFF is the most flexible of the current public domain raster file formats. It is the de facto direct output format for most paper and micrographic scanners. The majority of stored scanned image records are in TIFF format that has been compressed using ITU Group 3 or 4 compressions.
- *PDF Image (Portable Document Format from Adobe)* – Acrobat Capture 3.0 offers four different variants of Adobe PDF for use with paper-based documents:
  - *PDF Image Only,*
  - *PDF Searchable Image Exact,*

[1] ITU Group 3 and 4 is an open, international, lossless compression standard that is used in facsimile communications and as the primary means for reducing the size of TIFF format files for more efficient storage and transmission.

- *PDF Searchable Image Compact, and*
- *PDF Formatted Text and Graphics.*

Because they offer lossless compression and do not provide alterable text, PDF Image Only and PDF Searchable Image Exact are the two formats recommended by Adobe for use with digital image records.

PDF/A provides a file format for long-term preservation of electronic documents, and organizations should consider it to maintain records that may be required as evidence at some point over their life. The PDF/A file format provides a mechanism for representing electronic documents in a manner that preserves their visual appearance over time, independent of the tools and systems used for creating, storing, or tending the files. See ISO 19005-1.

- *JPEG (Joint Photographic Expert Group)* – The JPEG format is typically used for storing photographic images, such as from digital cameras. It supports 8-bit-per-color (red, green, and blue, for 24-bit total) and produces relatively small file sizes. The compression, when not too severe, does not detract noticeably from the image. However, JPEG files can suffer generational degradation when repeatedly edited and saved.

TIFF and PDF image formats are the most frequently utilized output formats, both historically and currently, for digital image copies of scanned paper or micrographic business records.

5.2 The Revolution of Three Conversions

Converting paper to digital image copies is the culmination of the following three paper- to-alternative-media conversions:

- *Microfilming* significantly reduced three of paper's most significant limitations (bulky volume, propensity to deteriorate and difficulty to distribute) by introducing an alternative media that could a) rapidly copy paper, b) cost-effectively duplicate images, c) efficiently store information and d) more effectively preserve and protect information originally recorded on paper.
- *Xerography and fax technologies* then fundamentally changed the long-standing, burdensome geographic limitations of paper by introducing the capability to easily and rapidly copy and distribute paper records.
- *Computers and the Web* then eliminated all of paper's intrinsic media-based limitations by radically reducing the time required to create, capture, process, communicate and access information as well as redefining the media on which information is stored. The resulting

unprecedented productivity gains of this "ultimate revolution" mandated large-scale conversion of paper to digital image copies.

5.3 The Paradigm Sea Change

Converting paper to digital image copies has resulted in major paradigm shifts. For centuries, (paper) records have been managed on a media-centric basis in accordance with the operational model now called "materials management," which is applied to all types of other business assets. Because these paper records were, in essence, a physical commodity, their management was driven largely by need and space. The time period for retaining them was based on need, and the location for storing them was determined by the availability of space.

Accordingly, records were kept where they were readily accessible for as long as space permitted. Over time, they typically were transferred to another location where there was more (and usually less costly) space – where their continued accessibility could be ensured for as long as they were needed. This methodology provided the necessary controls to ensure both the authenticity and availability of the records within its domain.

For as long as records have been created, media-centric records management practices successfully served the needs of government and business.

Now consider the sea change at hand: the transformation of records management – from the paradigm of media-centric records, where management was based on observable physical location controlled by humans, to the age of digital information, content-centric records management, and ESI, where the management process is based on invisible logical locations controlled by computers.

This sea change is grounded in the radically different nature of electronic records and has resulted in exponentially greater complexity in the process of managing records and information through their lifecycle. It also has created extraordinary new capabilities for improving that process, achieving unprecedented levels of control, effectiveness and automation.

Content-centric records management is a revolution in more than just a conceptual context. It is revolutionary in every aspect of how records are managed: from identifying and understanding new types of records. . . to where records are located and how they are accessed. . . to dependence on technology. . . to higher performance standards… to new skill sets required for records and IS/IT managers. . . to the need for a cross-functional records management team. . . and so much more.[2]

5.4 Judge Hedges' Comments

The real-world implementation of the benefits conferred by this revolution in records management capabilities must still be guided by the same basic concepts that governed media-centric paper record

[2] R. Williams and L. Ashley, *Cohasset ARMA AIIM Electronic Records Management Survey - Call for Collaboration* (2007).

keeping: authenticity and accessibility. An effective records management system is one that can utilize the technological improvements addressed in this white paper to create and maintain a streamlined and cost-effective system for storing data in a manner that preserves all important data, while organizing that data according to its usefulness.

While the specifications of an organization's records management system must be tailored to meet the needs of the particular business, the need to develop new management skills and cross-functional records management personnel is essential to every business that creates electronic records.

Capable and knowledgeable records management personnel must have a thorough understanding of the data system's organization, the format of the various types of records being stored, the "destination" on the system of particular types of records, how those records arrive at that destination, and how to retrieve those records when necessary. In the context of litigation or a regulatory investigation, the importance of records management personnel is magnified as the process of preserving and retrieving records becomes almost as important as the records themselves. Having a streamlined records maintenance system and a knowledgeable employee to designate as a 30(b)(6)[3] witness when data retention and production becomes an issue can save a business from engaging in costly discovery disputes.

6. Destruction of "Original" Paper Records Is Acceptable Following Creation of a Digital Image Copy

This section addresses the disposition of "original" paper records that have been converted to digital image copies. Can they be destroyed or must they be retained in addition to the digital image copy?

6.1 The Right to Destroy

There is jurisprudence (case law) acknowledging records shredding to be a valid component of robust records management practices. In *United States v. Arthur Andersen,* the United States Supreme Court ruled that an organization which shreds without an illegal intent has not committed a crime under a particular statute:

[3] Rule 30. Deposition by Oral Examination

(b) Notice of the Deposition; Other Formal Requirements.

(6) Notice or Subpoena Directed to an Organization.

In its notice or subpoena, a party may name as the deponent a public or private corporation, a partnership, an association, a governmental agency, or other entity and must describe with reasonable particularity the matters for examination. The named organization must then designate one or more officers, directors, or managing agents, or designate other persons who consent to testify on its behalf; and it may set out the matters on which each person designated will testify. A subpoena must advise a nonparty organization of its duty to make this designation. The persons designated must testify about information known or reasonably available to the organization. This paragraph (6) does not preclude a deposition by any other procedure allowed by these rules.

A "knowingly. . . corrupt persuader" cannot be someone who persuades others to shred documents under a document retention policy when he does not have in contemplation any particular official proceeding in which those documents might be material.[4]

Additionally, the UPA (see Section 4.3) clearly authorizes the destruction of original paper records that have been copied. It states the "original may be destroyed in the regular course of business unless its preservation is required by law."[5]

The Internal Revenue Service's (IRS) regulations, reflecting the clarity of both statutory and case law, permit the destruction of the original hardcopy books and records and the deletion of the original computerized records.[6]

There are a few types of paper records that should never be destroyed. Examples include:

- *Negotiability* – If the document is to be ultimately paid, like a promissory note, currency, or cash equivalent instrument such as bonds, then the document must be presented in the original to be paid.
- *Wills* – A presumption exists that if the original cannot be found, then the testator destroyed it intentionally.
- *Copyrights and certificates of naturalization.*

The biggest problem with records destruction policies is abuse, such as when a company inconsistently applies its destruction policies – be it hard copy or digital image copies.

When ESI content is either beyond its retention period, or is subject to an expungement order, there is a three part "best practice" for destroying such content. First, delete the metadata pointers to the content designated for destruction; second, copy the content that is not to be destroyed to another non-erasable or non-rewritable unit of ESI storage media, and third, physically destroy the unit(s) of non-erasable or non-rewritable media containing the content to be deleted or expunged. All such destruction should be performed in accordance with specific policies and procedures that create management evidence of the actions performed. The destruction of all ESI content should reflect diligent implementation of an organization's approved records retention policies.

6.2 The Obligation to Preserve

Once an organization has notice or learns of potential litigation, it has a legal duty to preserve all relevant information. This includes paper records to be destroyed as part of an ongoing conversion to digital electronic images. In such a situation, the destruction of the converted original paper must be

[4] Arthur Andersen LLP v. United States, 544 U.S. 696 at 708 (2005).
[5] 28 U.S.C. Sec. 1732.
[6] IRS Revenue Procedure 97-22, Sec. 7.

suspended if the records in question are relevant to a filed or reasonably foreseeable lawsuit, government investigation or external audit. Additionally, relevant digital electronic images (produced from paper records) scheduled to be destroyed as part of an organization's established retention policies should not
be destroyed.

There is absolutely no authority that would allow for the intentional destruction of records (both "original" paper and digital image copies) that are responsive to litigation or threatened litigation.[7] Robust records management practices therefore must manifest policies emphasizing that any destruction of records, relevant to a lawsuit either filed or reasonably anticipated, is *forbidden*.

Legal record hold prohibitions on shredding must be followed diligently by all organizations for all types of media manifesting a) a key component of robust electronic information management practices and b) an organizational culture that values ethics and compliance.[8] Certain information management software products automate and therefore facilitate managing legal holds correctly.

6.3 Judge Hedges' Comments

A violation of the duty to preserve information and ESI, triggered when litigation is "reasonably anticipated," that results in the destruction of potentially relevant documents and ESI may have significant legal ramifications. Courts have considerable discretion in imposing sanctions upon an organization or any responsible employees. Court-imposed sanctions range from criminal and civil penalties to unfavorable evidentiary presumptions at trial and discovery-specific sanctions.

In light of the consequences for destroying relevant information in anticipation of litigation, the need to establish detailed procedures governing the destruction of paper records and ESI cannot be overstated. Adherence to a thorough information management policy may protect against the imposition of severe sanctions for the innocent destruction of potentially relevant evidence. This is true only if the procedures set forth in the information management policy of a business are geared to the specific needs of that business, implemented in good faith, properly supervised, and all duties therein are performed in a timely manner. The information management procedures must also be flexible, as they may need to be halted at any time with respect to some, or possibly all, of the paper records and ESI being retained.

The improvements in information management technology, particularly the ability to create and store imaged records, can assist a business in avoiding costly sanctions and litigation expenses if properly organized and supervised. The characteristics of an effective information management system discussed in the previous section and the previous paragraph provide a business with a convenient and cost-effective means of high volume data storage, ensure that there are knowledgeable personnel in

[7] For example, In re the Prudential Ins. Co. of Am. Sales Practices Litig., 169 F.R.D. 598, 615 (D.N.J. 1997).
[8] See: R. Williams and L. Ashley, *Cohasset ARMA AIIM Electronic Records Management Survey – Call for Collaboration* (2007).

charge of implementing and supervising proper data retention practices, and results in the production of policies and guidelines that can be used as documentary evidence to prove good faith compliance with the duty to preserve documents.

7. Operational Implications

This section provides guidance regarding incorporating the legal requirements discussed in Sections 2 through 6 into an organization's ongoing operations – specifically, the creation and lifecycle management of digital image copies. This guidance is based on the requirements set forth in the law. As such, this guidance seeks to assist organizations in meeting the standards that triers of fact will use in their decision-making regarding a) the admissibility of digital image copies, b) the destruction of paper records that have been converted to digital image copies and c) the management of digital image copies – from their creation to their ultimate disposition.

Cohasset believes that for organizations to have their digital image copies admitted into evidence, the records/images must manifest certain admissibility requirements in six operational contexts:

1. Authentication Processes for All Types of ESI;
2. Secure and Reliable Systems;
3. Network of Support Resources;
4. Changes in the Volume, Function, and Importance of Records;
5. Proving the Negative with Metadata Management Evidence; and
6. Establishing Evidentiary Foundations.

7.1 Authentication Processes for All Types of ESI

A best-practice records management program should include determining the optimal technology for electronic copying and preservation of records (scanning from paper copies). This determination should be guided by efficiency and ease of access, together with discovery and evidentiary requirements. The Sedona Conference Commentary provides an extensive discussion of the various types of ESI and the different authentication approaches associated with each type.[9] For example, because there is more than one FRE authentication method, the authentication of e-mail needs attention at multiple stages in its life span: collection, retention, preservation, and production.[10]

Different challenges are posed when authenticating website postings, text messaging, and chat room content.

[9] Sedona at 4 -8.
[10] Id. At 4-5.

Computer-stored records and databases, which would include scanned digital image copies, would be subject to the 14 Imwinkelried/Cohasset requirements for establishing a foundation for the admissibility of computer records – especially those with robust policies and procedures for using and accessing equipment, databases, and programs.[11] Organizations using digital image copies should consider the circumstances when, where and how the scanning is performed.

Of the many different types of electronic records, digital image copies are one of the most difficult to alter or manipulate. Accordingly, their use has expanded, from being created only from scanning paper records, to also including digital "snapshots" because they will more likely be able to overcome evidentiary challenges.

7.2 Secure and Reliable Systems

To meet evidentiary challenges, organizations should ensure the stability and reliability of its computing environments. In pursuit of that goal:

- *Enterprise content management solutions and electronic records management systems can facilitate managing complex documents as well as control and access content forms in a secure environment.*
- *A variety of technologies are available for electronic copying and preserving records (scanning from hard copies).* They should be deployed to improve efficiency and ease of access as well as meet discovery and evidentiary requirements.

7.3 Network of Support Resources

To integrate the evidentiary rules addressed in this white paper into a records management program that reflects and embraces an organization's operations and its culture, both in-house resources and consultants may be needed. As part of a robust records management program, records managers not only need C-level support and a new level of financial resources, they also need to be given an edict to integrate the organization's evidentiary foundational needs (and pretrial discovery needs) into its records management system. No less important, records managers and the entire ethics and compliance department need to be empowered to set forth these priorities to all employees, business units and information technology colleagues.

7.4 Changes in the Volume, Function and Importance of Records

Historically, records have been a definitive resource for recollecting the facts in the resolution of disputes (see Section 1.1). Over time, regulatory agencies, with their use of compliance as their primary governance tool, have led to extraordinary changes in the volume, function and importance of records. This has been manifested in five contexts:

[11] Lorraine, Vee Vinhnee, Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co, Inc., 2005 WL 679071 (Fla. Circ. Ct. Mar. 1, 2005), reversed on other grounds, 955 So.2d 1124 (Fla. Dist. Ct. App. Mar. 21, 2007), review denied, Case No. SC07-1251 (Fla. Dec. 12, 2007).

1. *Creation of exponentially larger volumes of records* – with the advent of electronic records,

2. *Retrieval of much larger volumes of records* – resulting from the requirements of regulations and the capabilities of computers,

3. *Compression of time to retrieve and profer records* – from months (courts), to days (inspections) to hours (news media),

4. *Expansion of the number of forums where records are used to resolve disputes* – from just courts, to also agency hearings and onsite inspections, to the media, and

5. *Expansion of the function of records in the resolution of disputes* – from just "proving the positive" (example: you signed the contract, you owe the money) to also "proving the negative" (example: the aircraft were regularly and properly inspected; i.e., the information in the records shows no circumstantial probability that an allegation of wrongdoing could have occurred).

These profound changes in the volume, utilization, and function of records have resulted in an unprecedented level of importance in the processes associated with the creation, retention, management, and disposition of electronic records.

7.5 Proving the Negative with Metadata Management Evidence

With media-centric records (paper and microfilm), the content of records is all-important to proving the negative. However, with all content-centric electronic records, the intrinsically created metadata – associated with both the records themselves and their management systems – provides a usually easier, and almost always more definitive way to prove the negative: metadata management evidence.

Metadata management evidence is simply information produced by computers in the course of creating and managing electronic records (detailed operating information typically unseen by users). This metadata relates to the contents of records as well as to events in the life of a record: who did what, where and when – from the time the record was created to the present.

Analysis of available metadata regarding activity and behavioral patterns can greatly facilitate demonstrating "circumstantial probability" in the accuracy, reliability and trustworthiness of specific actions relating to certain records over time. As such, this metadata management evidence can be very helpful to proving the negative.

For digital image copies, the metadata "restored" at the time of the paper conversion/image creation, together with the ongoing metadata generated by their management systems, provide a mass of management evidence that can be very useful in establishing the facts and proving the negative.

7.6 Establishing Evidentiary Foundations

Should an organization's records need to be introduced in court (or as they are produced in discovery), legal counsel will benefit from good strategic ESI generation and retention decisions, quality software and hardware, and top-flight professional support both within and without the company in laying a strong evidentiary legal foundation.

As seen in the jurisprudence in *Lorraine* and *Vee Vinhnee* as well as in other high-profile cases such as *Morgan Stanley,*[12] attorneys who ignore discovery obligations or foundational evidence rules shall not prevail, no matter how robust the ESI or the records management.

Readers are directed to the Appendix, which identifies guidance on best practice requirements and standards for electronic imaging and records management programs, much of which is founded in IRS regulations, ISO standards and AIIM/ANSI technical reports.

7.7 Judge Hedges' Comments

Section 7 is, in effect, a mirror image of Sections 2 through 6, looking as it does to the operational implications of the law. The goal of any process should be, reduced to its essentials, reliability and reasonableness. The six operational contexts described above appear likely to further that goal, "enhance" admissibility, and increase the weight to be given to admitted digital image copies by a finder of fact.

8. Conclusions

This white paper has addressed the extent to which digital image copies, a subset of ESI, a) are legal as records, b) can substitute for paper originals and c) can be admitted into evidence in a court of law as credible records – imbuing accuracy, reliability and trustworthiness.

The specific purpose of this white paper was to provide authoritative answers to four all-important questions regarding the utilization of digital image copies:

1. *Are digital image copies legally as acceptable as "writings" and "original" paper records?*

   Yes, digital image copies of information converted from paper (and microfilm) are the legal equivalent of their paper counterparts and may be considered as admissible in evidence as the original paper record in any legal or administrative proceeding – subject to certain legal admissibility provisos that apply to all types of records.

[12] Lorraine, Vee Vinhnee, Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co, Inc., 2005 WL 679071 (Fla. Circ. Ct. Mar. 1, 2005).

2. *What evidentiary hurdles must be overcome so that digital image copies are admissible in court?*

   The law, through rules of evidence and recent case law, sets forth authenticity standards for the admission of digital image copies into evidence in legal proceedings. The rules and case law collectively manifest these standards in certain operational tenets that organizations should adhere to – in both their conversion of paper records to digital images as well as the ensuing management of those digital image copies over time.

3. *Can original paper records that have been digitally copied then be destroyed?*

   Yes, original paper records, for which there are accurate digital image copies, can be destroyed (as documented in Section 6). This is because digital image copies, like all other types of copies, are acceptable in any legal or administrative proceeding regardless of whether the original is in existence or not – so long as a) the records to be destroyed are not relevant to a lawsuit either filed or anticipated, b) the destruction is not contrary to any law or regulation and c) the paper records are not of the type that should never be destroyed (wills, etc.).

4. *How does a company integrate the rules of evidence and case law into the management of records in a way that increases the admissibility of digital image copies?*

   An organization should establish a lifecycle records management system (that is part of a corporate culture of compliance) to ensure that digital image copies a) are kept reliably with an adequate chain of control and b) can be authenticated by records management professionals and legal counsel.

   Additionally, this white paper focused on the need to have ongoing resources that will ensure ESI is managed and monitored "from cradle to grave" in a way that positions an organization for success in compliance and litigation.

Appendix: Good Image Capture Practices

Policy, Process and Procedures

These primary sources detail the requirements for documenting policies, processes, and procedures related to the implementation and operation of an electronic imaging and/or records management:

- *Federal case law* (see Section 3.4),
- *Internal Revenue Service Revenue Procedures 97-22,* and

- *International Standards Organization (ISO) – 15489 and 15801.*

Documentation of good practices for electronic imaging projects are presented in *AIIM TR15-1997, Planning Considerations Addressing the Preparation of Documents for Image Capture.*

Document Preparation

Good document preparation practices, such as those identified in *AIIM/ANSI TR15-1977 (6.2),* are paramount for achieving completeness and accuracy when imaging hard copy records. Adequate document preparation is a key component for properly identifying documents and ensuring that the input quality of the source document will allow rendering of the resulting images in human readable form.

Image Scanning

A very specific procedural regulation that defines the requirements for image scanning is Internal Revenue Service (IRS) Revenue Procedure 97-22. Among the requirements specified in 97-22 are:

- *Accuracy means that the scanning process captures all of the significant information* so that the resulting image represents an accurate facsimile of the original document, and that the resulting digital image subsequently can be rendered accurately and completely on a display device or via a printer.
- *Reliability of the scanning process that ensures consistent scanning* of all documents within the established parameters.
- *Utilization of controls to ensure the integrity, accuracy, and reliability of electronically scanned images.*

Indexing

Indexing relates to defining certain attributes that sufficiently describe imaged documents (and other electronic documents) so that they may be searched and retrieved for processing or viewing.

Sufficient indexing attributes must be associated with imaged documents to meet legal and regulatory requirements. Most regulations and industry guidelines as well as good practices for electronic recordkeeping require that records be “readily” accessible for the required retention period, including any extensions to the retention period resulting from a legal or regulatory hold order. Again, *IRS Revenue Procedure 97-22* clearly states certain indexing requirements, such as:

- *A retrieval system that includes an indexing system* (Section 4.01(2)(d)),
- *The requirement to maintain an indexing system will be satisfied if the indexing system is functionally comparable to a reasonable hardcopy filing system* (Section 4.02(1)), and

- *Reasonable controls must be undertaken to protect the indexing system against the unauthorized creation of, addition to, alteration of, deletion of, or deterioration of any entries* (Section 4.02(2)).

Information retained in digital image copies usually is much easier to find than when it is retained on paper. This is due to the metadata created when the information is converted from paper to a digital image copy. The metadata enables the creation an index which, in turn, makes finding needed information in digital image copies much easier than if it had to be found in the files of paper. The metadata automatically generated in the creation of digital image copies makes all digital image copies clearly advantageous over paper records – in both finding needed records and also enhancing their admissibility in any legal proceeding.

Born digital information automatically generates even more metadata than digital image copies. This additional metadata facilitates linking born digital information to a transaction or the relevant actions that are the basis for creating the born digital information. This additional metadata also can greatly facilitate establishing a record's chain-of-custody – something that is very important to the legal admissibility of all ESI.

Quality Assurance

Quality assurance is a "final" quality check to determine that the overall imaging process is being performed in an accurate, complete and reliable manner. Quality assurance differs from quality control: whereas quality control is conducted as an integral part of each imaging process step, quality assurance addresses the quality and accuracy of the imaging process as a whole. Quality assurance is conducted using a representative sample of the imaged records and their associated index data. The quality assurance process typically entails searching for selected imaged records using various index data attributes, retrieving and displaying the imaged records and complete index data, and verifying their accuracy (legibility) and completeness.

Accessibility

Access to stored electronic records and the ability to retrieve and present them in a human readable form (such as a visual display screen or a printed rendition) is a fundamental requirement for meeting regulatory and legal requirements as well as for business purposes.

Most regulations require that records of all types, including electronic records, be accessible and reproducible or presentable in human legible and readable form. *IRS Revenue Procedure 97-22* specifies accessibility requirements that include:

- *The ability to reproduce legible and readable "hardcopies" of electronically imaged books and records* when displayed on a video display terminal (Rev. Proc. 97-22, Section 4.01(2)(e)) and

- *All books and records reproduced by the electronic storage system must exhibit a high degree of legibility and readability* when displayed on a video display terminal when reproduced in hardcopy (Rev. Proc. 97-22, Section 4.01(3)).

Record Integrity

Protecting the integrity of records is a fundamental requirement of all regulations independent of the industry and/or the documentation being converted to digital images. Integrity protection also is a threshold requirement in all electronic records management standards and good records management practices.

Internal Revenue Procedure 97-22 stipulates two requirements for protecting the integrity of records:

- *Reasonable controls to prevent and detect the unauthorized alteration of, deletion of, and deterioration of electronically stored books and records and associated indexing system* (4.01(2)(b)) and

- *Regular inspection and quality assurance that includes periodic checks of electronically stored books and records* (4.01(2)(c)).

International Standards Organization (ISO) 15489 (Information and Documentation – Records Management, Parts 1 and 2) and ISO 17721 (Open Archival Information System Reference Model) amplify the meaning of integrity and recommends integrity protection procedures:

- *The integrity of records refers to their being complete and unaltered, that is the records have been protected against unauthorized alteration* (ISO 15489, Part 1.7.2.4).

- *Data integrity service ensures that data is not altered or destroyed in an unauthorized manner* (ISO 14721, Part 4.1.1).

- *Control measures such as access monitoring, user verification, authorized destruction, and security should be implemented to prevent unauthorized access, destruction, alteration, or removal of records* (ISO 15489, Part 1.8.2.3).

Digital Image Copies vs. Born Digital

The majority of paper business records used in business processes and then stored as digital image copies are born digital. Examples include computer generated reports, word processing files, spreadsheets and web pages. Amazingly, a significant number of organizations still believe they must first print many of these records to paper and then store the paper in the event the records are required for legal admissibility. In most instances, this is not required. In reality, having multiple copies of identical records on different media is not a good practice because it usually significantly increases

both the complexity and the cost of responding to legal discovery. The best practice is to store born digital documents in their native, originally-born digital state wherever possible.

In certain circumstances, born digital records may need to be printed to paper, converted to digital image copies and then retained in that electronic format – pursuant to the organization's retention schedule. Two examples are documents requiring the addition of a signature or the need to include manual annotations of a document's original information. In such instances, digital image copies are an ideal way to store all the relevant information digitally.

ESI Retention and Disposition/Destruction

When ESI content either is beyond its retention period, or is subject to an expungement order, there is a three part "best practice" for destroying such content stored on non-erasable, non-rewritable portable media (optical disks and magnetic tapes):

1. Copy the content that is not to be destroyed to another non-erasable or non-rewritable unit of ESI storage media;

2. Delete the metadata pointers to the content designated for destruction, and

3. Physically destroy the unit(s) of non-erasable or non-rewritable media containing the content to be deleted or expunged.

All such destruction should be performed in accordance with specific policies and procedures that create management evidence of the actions performed. The destruction of all ESI content should reflect diligent implementation of an organization's approved records retention policies.

Bob Williams (williams@cohasset.com) is president of Cohasset Associates, Inc., one of the nation's foremost management consulting firms specializing in records and information management. Mr. Williams is a leading records management consultant, a respected legal authority on the legal acceptance of records stored on non-paper media and as a pioneering RIM educator and highly sought speaker. Mr. Williams has: authored many legally-focused articles in a spectrum of professional publications; edited two definitive legal research studies (Legality of Microfilm and Legality of Optical Storage); served as a contributor and editor of The Sedona Guidelines: Best Practice Guidelines for Managing Information & Records in the Electronic Age; and provided expert witness testimony on records management practices – including the landmark United States Supreme Court punitive damages decision: State Farm Insurance v. Campbell. Since 1992, Mr. Williams has organized, sponsored, and co-chaired the National Conference on Managing Electronic Records (MER), recognized for nearly two decades as the premier electronic records management conference.
(www.merconference.com).

Ron Hedges is the principal of Ronald J. Hedges LLC. Ron serves as a special master, mediator and arbitrator and consults on electronic discovery and records management. He sat as a United States

Magistrate Judge in the District of New Jersey from 1986 to 2007. Among other things, Ron is a member of the adjunct faculty of Georgetown University Law Center and Rutgers School of Law (Newark), where he teaches an introduction to electronic discovery and evidence, and of the advisory boards of Georgetown's Advanced E-Discovery Institute and The Sedona Conference. He is also a Visiting Research Collaborator at the Center for Information Technology at Princeton University. He can be contacted at r_hedges@live.com.

Virginia Becomes First Jurisdiction to Authorize Online Notarization

By Timothy Reiniger and Dr. Richard Hansberger

On March 26, 2011, Virginia enacted a law that authorizes online notarization by means of internet video/audio conference technology.[1] Using these provisions, the signer does not need to appear physically in front of a notary but may elect to appear before the notary online. The law becomes effective July 1, 2012. Following years of discussion and speculation about the future of "cyber notaries" at the ABA, this marks the first time that remote notarization has been authorized in the United States.[2]

What the Legislation Does

Historically, a signer had to appear physically before a notary to request a notarization. The notary then had the duty to verify the signer's identity either by personal knowledge or by the signer's presentation of satisfactory evidence of identity such as a drivers license, Passport or military identification card. Virginia's bill permits the signer to appear before the notary using internet video and audio conference technology instead.

To ensure that remote electronic notarization is reliable, the notary now has a duty under Virginia's law to *confirm* the identity of the signer either by personal knowledge or reliance upon high assurance evidence of identity. If the notary personally knows the signer, no further identification is required. If the notary does not personally know the signer, then the notary must identify the signer either by reliance on prior (antecedent) in-person identity proofing by a third party such as a state department of motor vehicles, bank, law firm or title company and pursuant to the antecedent proofing[3] specifications of the Federal Bridge Certification Authority, or reliance on the signer's use of a digital certificate that is authenticated either by a biometric or a high-security interoperable PIV card[4] issued either publicly or privately in accordance with federal standards.

To enhance consumer protection and deter fraud, the notary must keep and provide for lawful inspection an electronic record of notarial acts that contains at least the following information: (i) the date and time of day of the notarial act; (ii) the type of notarial act; (iii) a description of the document

---

[1] *Available at* http://leg1.state.va.us/cgi-bin/legp504.exe?111+ful+CHAP0731.

[2] Note that French notaries have been the first to use video conferencing for the notarization of deeds. Ugo Bechini and Dominik Gassen, *A New Approach to Improving the Interoperability of Electronic Signatures in Cross-Border Legal Transactions*, 17 MICH. STATE J. INT'L L., No. 3 (2009) at 4.

[3] For a description of "antecedent in-person proofing" *see* FPKIPA – CPWG Antecedent, In-Person Task Group, "FBCA Supplementary Antecedent, In Person Definition," (July 16, 2009) *available at* http://www.idmanagement.gov/fpkipa/documents/FBCA_Supplementary_Antecedent.pdf.

[4] For a description of PIV-I, *see* Federal CIO Council, "Personal Identity Verification (PIV) Interoperability For Non-Federal Issuers," v1.0.0 (May 2009) *available at* http://www.idmanagement.gov/documents/PIV_IO_NonFed_Issuers_May2009.pdf.

or proceeding; (iv) the printed name and address of each signer; (v) the evidence of identity each signer presented to the notary; and (vi) the fee, if any, charged for the notarial act. Where the signer appears before the notary online using video and audio conference technology, the notary must keep a copy of the recording of the video and audio conference.

Finally, Virginia's bill permits the notary to verify facts contained in public records and on identity credentials, such as date of birth and date of marriage. This provision intends to minimize hardships on couples pursuing foreign adoptions as well as entities needing to identity-proof large numbers of people (such as for electronic medical record implementation mandated by federal law).

What The Law Does Not Change

Traditional paper-based notarization is not impacted by this bill. Under that traditional process, a signer appears physically before a notary and presents a paper document requiring notarization. After verifying the signer's identity (either by personal knowledge or the signer's presentation of a legally permissible identity card such as a drivers license, Passport, or military ID), the notary signs the appropriate notarial certificate and affixes his or her seal imprint on the certificate. The paper notary is not required to validate the signer's identification credentials and, historically, the notary has had no means to do so. Again, this paper notarization process remains unchanged under the Virginia bill.

The Significance Of Online Notarization

Online or "remote" notarization allows the signer to appear before the notary using internet based video/audio conference technology.[5] No longer must the signer physically appear before the notary; instead, the signer and notary meet online, the signer presents an electronic document to the notary, and the notary electronically notarizes the document by affixing a tamper resistant electronic signature and electronic notary seal to the electronic document.

Perhaps most importantly for consumers and other relying parties, Virginia's bill significantly strengthens the notary's ability to detect and deter fraud and abuse of the notarial process, issues that have plagued the paper notary office. Because the notary must keep a recording of each remote notarial act and the signer's identity credential is subject to much more stringent authentication standards (including real-time online verification of identity in the case of biometric or PIV authentication), relying parties will be afforded a higher level of assurance of the signer in the remote process than is possible in the current *in-person* paper and electronic notarial processes.

[5] But this has not been without some controversy. For a discussion of physical appearance in notarial practice, *see* Charles N. Faerber, *Being There: The Importance of Physical Presence to the Notary,* 31 J. MARSHALL LAW REVIEW NO. 3, 749 (1998) at 775 ("The notary's audial interaction with the absent signer and real-time acquisition of the signer's video image would seem prerequisites for such remote electronic notarizations."). For concerns raised about the possibility of a "virtual trial" conducted by videoconferencing, *see* Richard L. Marcus, "E-Discovery & Beyond: Toward *Brave New World* or *1984*?" 236 F.R.D. 598, 630 (2006) ("Video conferencing might be thought preferable, but still seems unlikely to recreate that opportunity of the party or witness to feel that she has fully told her story to the decision maker.").

Significantly, Virginia's bill moves the notary into the stream of electronic commerce in a manner never before possible.[6] Now, signers may appear remotely before a duly commissioned Virginia notary taking advantage of all the advantages of online transaction processing, including greater speed, efficiency and security. Relying parties can place greater trust in the reliability of remotely notarized transactions due to the more stringent identity and authentication requirements for signers and the notary's electronic journal, which will include a real time recording of the notarial act itself. When questions about the authenticity of the act arise, those questions can be resolved more quickly and efficiently to protect all the parties to the transaction, a problem that traditional in-person notarization simply has not been able to solve.

Implications for Digital Evidence

Authenticity of digital public documents requires proof of origin (identity of the signer), content integrity (whether the document has been altered), and time of execution or issuance.[7] A critical part of the authentication inquiry is whether safeguards have been implemented to assure the continuing accuracy and integrity of the originally created record.[8] Thus identity, integrity, and time, recognized as the three main components of authenticity, must be handled in a fashion that will allow strong tests, or strong proof, in the future should questions arise.[9]

It is important to remember that courts in Virginia and a growing number of states already use video conferencing. Accordingly, the online notarization law expressly cross-references the Virginia court standards for video conference testimony in criminal procedure as follows:[10]

"Any two-way electronic video and audio communication system used for an appearance shall meet the following standards:

1. The persons communicating must simultaneously see and speak to one another;

2. The signal transmission must be live, real time;

3. The signal transmission must be secure from interception through lawful means by anyone other than the persons communicating."

Implications for Cloud Computing

---

[6] *See,* THOMAS L. FRIEDMAN, THE WORLD IS FLAT (Picador 2007) at 205-10 (new business processes are needed to fully leverage new technological capabilities like videoconferencing).

[7] WINN & WRIGHT, THE LAW OF ELECTRONIC COMMERCE, § 20.05 (4th ed. Aspen Publishers, Inc. 2007); *See generally* George L. Paul, *The 'Authenticity Crisis' in Real Evidence*, 15 THE PRACTICAL LITIGATOR No. 212-13 (2004).

[8] *See* In re Vinhnee, American Express Travel Related Service Co. Inc. v. Vinhnee, 336 B.R. 437 (9th Cir. B.A.P. 2005) (proponent failed to authenticate computer generated business records because of an inability to assure content integrity from the time they were originally created).

[9] GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE (American Bar Association 2008) at 36.

[10] VA. CODE ANN. § 19.2-3.1 (B)(1), (2), and (3).

The law recognizes the reality that with Cloud storage, electronic documents are increasingly located outside of Virginia and cannot be in the *physical* presence of the signer. Nevertheless, the need for parties to establish legal authenticity of electronic documents persists. Online notarization enables a virtual and *conscious* presence of signers and the individuals who must witness acts for self-authenticating proof and provides a legal means of attributing the document to a particular individual. As industry and government moves increasingly to Cloud-based computing platforms, the message truly matters more than the medium. Virginia's remote notary law enables signers and notaries to transact business securely and efficiently across virtual legal landscapes.

Domestic and International Significance of Online Notarization: Final Thoughts

The intent of the law is to improve the e-notary process and make it more usable for business and government in today's networked global economy. It is expected that out of state Cloud providers and customers will desire to leverage online notarization through the use of contractual choice of law terms invoking Virginia law.[11]

The remote capability will greatly expand the usefulness of Virginia electronic notaries to industry and the federal government by leveraging widely adopted and trusted biometric validation, video and audio teleconferencing, and identity management technologies. At the same time, by requiring two factor authentication of the signer (i.e., digital certificate combined with either a biometric or PIV authentication) relying parties will be afforded a higher level of assurance of signer identity in the remote process than is possible in the current *in-person* paper and electronic notarial processes, which requires only single factor authentication (i.e., a government issued identity card or a credible witness).

Online notarization of electronic documents is also consistent with the recommendations of the Hague Conference on Private International Law. An international e-document authenticity standard has emerged for electronic public documents that reflects the evidentiary need for these documents to have the capability of authenticity testing.[12] This standard requires that any relying party be able to verify the origin and integrity of the electronic public document.[13] The Virginia e-notary law had already adopted this standard.[14] Establishing the authenticity of a notarized document thus requires the capability, in perpetuity, of independently authenticating the documents origin and verifying whether the content of the electronic document is complete and unaltered.

Timothy Reiniger, a member of the EDDE Committee, is an attorney currently serving as President of IA Corporation-VA and as a consultant in the area of information assurance strategy with FutureLaw, LLC

---

[11] *See, e.g.,* VA. CODE ANN. § 59.1-501.9.

[12] *See, e.g.,* FIRST INTERNATIONAL FORUM ON E-NOTARIZATION AND E-APOSTILLES, Conclusions 15 and 18 (Nat'l Notary Ass'n 2005), *available at* http://www.e-app.info.

[13] *Id. See also* NATIONAL E-NOTARIZATION STANDARDS, Standards 14 and 15 (Nat'l Ass'n of Secretaries of State 2006) *available at* http://www.nass.org.

[14] VA. CODE ANN. § 47.1-16 (D).

in Richmond, Virginia. He is a contributing author to George Paul's book, FOUNDATIONS OF DIGITAL EVIDENCE. Mr. Reiniger is licensed to practice in California and New Hampshire.

Richard Hansberger is an internationally recognized leader in electronic notary and electronic signatures. He is the former Vice President of Electronic Notarization at the National Notary Association and, while there, developed electronic notarization solutions for Fortune 500 member companies, developed the nation's first statewide electronic notary credentialing system for the State of Pennsylvania, successfully obtained SISAC[i] accreditation for this system and advised dozens of state and local government entities on electronic notarization laws, regulations, policies and best practices. For more information see: http://www.futurelaw.net/digital-services-group.htm

Committee Co-Chairs' Message

Dear Colleagues and Friends,

The EDDE committee is proud to present our seventh issue of the *EDDE Journal*. This edition's articles address issues that remain cutting edge in our field of practice, and we thank each of the authors for their contributions. The EDDE Committee Leadership (George Paul, Lucy Thompson, Steven Teppler, Eric Hibbard and Hoyt L. Kesterson II) extend our special thanks to *EDDE Journal* Editor Thomas Shaw, who lives and works in Japan. Despite tremendous pressures arising out the tragic earthquake and resulting tsunami, and without skipping a beat, Thomas brought to e-print not only this magazine, (the *EDDE Journal*) but a sister publication for the Information Security Committee. During that time, he also published a new book, *Cloud Computing for Lawyers and Executives – A Global Approach* (here), which covers not only how e-discovery and forensics are different in the cloud but also covers the basic rules of e-discovery in many countries throughout the world.

We would like to say welcome to the members of the International Litigation Committee of the ABA's Section on International Law. Our editor reached out to this committee's leaders to seek permission to add them to the distribution list of our publication. We have been immediately rewarded, as the first article in this issue has been submitted by a member of that committee, located overseas in France. We look forward to continued insights from our internationally-based and focused colleagues.

Our committee continues to grow in number and expand its domain purview as our field of practice continues to evolve. We presented the Second e-Discovery and Digital Evidence Practitioner's Workshop February 18-19 in San Francisco on the heels of the 2011 RSA Security Conference. That program featured moot court programs and workshops with U.S. Federal Magistrate Judges, Andrew Peck, (SDNY), John Facciola, (DDC), and Frank Maas, (SDNY). The workshop was a success, with participants able to receive the latest information on electronic, discovery and complex litigation, the Federal Rules of Civil Procedure, computer forensics, digital evidence, search, ethics, and criminal law, together with a full day of mock meet and confers, and discovery and spoliation/discovery abuse hearings. Our thanks to all the conference presenters and participants. Future EDDE activities include one in-person meeting and two Webex meeting before the end of 2011. We are also in the planning stages for our fourth EDDE conference tentatively scheduled to be held January 2012 at Stetson University College of Law in Tampa, Florida.

Future Events:

> **EDDE Committee Meeting**: The next EDDE committee meeting will be held virtually (by way of Webex) and graciously hosted by our co-chair Eric Hibbard of Hitachi Data Systems June 8, 2011 between 1:00pm and 3:00pm Eastern. We will be reviewing recent decisional authority, setting up subcommittees for work projects discussed at prior meetings (standards, information governance, judicial outreach, discovery request development, etc.), and have an expert

presentation on a topical and timely e-Discovery topic. All are invited to participate. Dial-in/web-access details will follow in short order.

Third e-Discovery and Digital Evidence Workshop: Our next two day workshop will be held August 15-16 at Cardozo Law School in NYC. The conference format will continue its focus on e-Discovery and digital evidence management from both the legal and technology perspectives, and include sessions on complex litigation, emerging technologies, practitioner panel and case-law update, ethics, latest search developments (yes, there have been search developments since February), computer forensics, HIPAA/HITECH implications, and a full day of 26(f) conferences, discovery hearings, discovery abuse/spoliation hearings, and a judicial roundtable. Here's an excerpt from the brochure that is being sent out:

"The curriculum consists of case studies, a mock 26(f) meet-and-confer, a mock spoliation hearing, and panel discussions with luminaries in the field. Judges and experienced practitioners will analyze recent judicial decisions on the production of ESI and the key rules from the Federal Rules of Civil Procedure that impact e discovery; legal experts and researchers will describe how new search technologies will lead to cost efficient, yet defensible, automated production of relevant ESI; practitioners and technologists will examine the e discovery implications of the increasing use of encryption and data stored in the cloud; and forensics experts will describe how to extract information from those increasingly complex systems."

We look forward to seeing you at our next meeting. Please send us your ideas, and stay tuned for updates to our committee's activities this year. And consider submitting an article for publication in the *EDDE Journal*, on any topic related to e-discovery, digital evidence or forensics.

The EDDE Chairs, Eric Hibbard, George Paul, Steve Teppler and Lucy Thomson