EDDE JOURNAL

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

SPRING 2010 VOLUME 1 ISSUE 2

E-Discovery and Cloud Computing: Control of ESI in the Cloud

By David D. Cross and Emily Kuwahara

Even if you do not yet know what cloud computing is, chances are you already are in the cloud. Cloud computing generally refers to accessing and using software, platforms, and infrastructure over the Internet to do your computing. Cloud computing can be as simple as using a web-based email account or document collaboration tool such as the ones provided by Google, or it can be more complex, such as the rental of processing power of a network of computers or customized applications to be run across the Internet. [It] has the potential to reduce IT management costs for companies by placing IT and software maintenance in the hands of a third-party service provider, while gaining the ability to expand quickly. *Read more*

Federal Magistrate Sets Example for Digitally Signed Official Court Orders

By Timothy Reiniger and Jacques R. Francoeur

On June 7, 2010 in Washington, D.C., the Honorable John M. Facciola, Magistrate Judge for the U.S. District Court in the District of Columbia, will be honored as the designated Laureate for 2010 by the Computerworld Information Technology Awards Foundation Honors Program in recognition of his being the first United States judge to digitally sign judicial orders. Since the first test case, Judge Facciola has been digitally signing official court orders and warrants. "The capability to sign electronically an order or other document should create in the people who see it an assurance that the document was signed by the judge and eliminate corrupt attempts to use forged, electronically created documents for improper ends." *Read more*

How to Select and Work with Digital Data Forensic Experts

By John Jorgensen

E-Discovery and Digital Data Forensics is upon us with a vengeance. In so many cases, digital data has become crucial during the discovery process, both because of the information it yields between agreeable parties as well as the information opposing parties try to hide. In a real life example, a financial agreement has been made between two parties. The agreement is nebulous concerning the length of the agreement terms. Party “A” (Plaintiff) claims that the length of term was a recognized element and was discussed and acknowledged in an exchange of emails between the Parties. Opposing Party “B” (Defendant) states *Read more*

The *Pension Committee* Decision

By Steven W. Teppler

Self-referred to as “Zubulake Revisited, Six Years Later,” the Pension Committee decision advances the practice of law in the digital age as much by what it implies as what it holds for issues involving ESI preservation, holds, and attorney competency and candor. This 87 page decision has drawn much attention from both the legal as well as the vendor community. This decision, from U.S. District Judge Shira Scheindlin of the Southern District of New York (and the author of the seminal Zubulake opinion series) involves a lawsuit by nearly 100 investors of a failed hedge fund. The losses alleged exceeded 500 million dollars. Like a preacher beginning a sermon, and in what is probably one of the finest examples of a contextual set piece I’ve seen, the court first provides a comforting homily: “In an era where *Read more*

E-Discovery and Cloud Computing: Control of ESI in the Cloud

By David D. Cross and Emily Kuwahara


Even if you do not yet know what cloud computing is, chances are you already are in the cloud.[1] *Cloud computing generally refers to accessing and using software, platforms, and infrastructure over the Internet to do your computing.*[2] *Cloud computing can be as simple as using a web-based email account or document collaboration tool such as the ones provided by Google, or it can be more complex, such as the rental of processing power of a network of computers or customized applications to be run across the Internet.*[3] *Cloud computing has the potential to reduce IT management costs for companies by placing IT and software maintenance in the hands of a third-party service provider, while gaining the ability to expand quickly.*[4]

Where ESI goes, e-Discovery often follows.[5] The categories and services provided in the cloud are as varied as the customers that use them. Attorneys who must chase down data for litigation should be aware that cloud computing may dramatically expand the number of places that ESI may reside – and may significantly increase the complexity and difficulty of locating and obtaining that data.

The client's relationship with the cloud provider may dictate the ease with which a party will be able to comply with its obligations to preserve or produce data in litigation. Some cloud providers may operate under a contract that expressly address e-Discovery obligations, should the data be subject to litigation holds or production requirements.[6] Other contracts may limit the cloud provider's obligations or may be part of a daisy chain of contracts such that, ultimately, the data resides with a provider with whom the party has no contract. Finally, one may use free third-party services such as Google's online applications, IM services, or Facebook, where the only contract arises from the

---

[1] In one of the few cases to address "cloud computing," which was a search and seizure case, dissenting judge, Judge Sercombe, cites statistics from a 2008 article reporting that 69% of U.S. residents who are online use at least one of six popular cloud services. *Oregon v. Bellar*, 217 P.3d 1094, 1111 n. 11 (Or. Ct. App. 2009) (Sercombe, J., dissenting). He also recognized that our "social norms are evolving away from the storage of personal data on computer hard drives to retention of that information in the 'cloud,' on servers owned by internet service providers." *Id.* at 1110. Companies also are shifting to the cloud. Already in 2008, the annual global market for cloud computing was estimated to be $95 billion by 2013. Rachael King, How Cloud Computing Is Changing the World, Business Week (Aug. 4, 2008), available at http://www.businessweek.com/technology/content/aug2008/tc2008082_445669.htm.

[2] See Mark L. Austrian & W. Michael Ryan, Cloud Computing Meets E-Discovery, 14 Cyberspace Lawyer 7 (2009) for a brief description of cloud computing.

[3] *See* King, *supra* note 1.

[4] *Id.*

[5] ESI is the common acronym for electronically-stored information.

[6] *See e.g.*, Professional Services Contract between City of Los Angeles and Computer Science Corporation for SAAS Email and Collaboration Solution, dated November 10, 2009; Posting of David Sarno to LA Times Blogs, http://latimesblogs.latimes.com/technology/2009/10/city-council-votes-to-adopt-google-email-system-for-30000-city-employees.html (Oct. 27, 2009). Section 1.1.4 of the contract provides that the Contractor will implement e-Discovery with the ability to search on the basis of content, sender and/or recipient, date range, and metadata with the ability to store search results with any metadata and the ability to add and delete from search results to create an e-Discovery set.

standard terms of service agreed to by users (who likely rarely, if ever, read those terms before promptly clicking the box confirming their agreement). The cloud provider may be subject to statutory restrictions as to whom and what information may be released under the Stored Communications Act.[7]

With a third-party in possession of data that parties to litigation may view as their own (or a court may view as belonging to them), issues surrounding the duties to preserve and produce become more pronounced. Having a third-party involved will not necessarily absolve a party or its counsel from discovery responsibilities. It has long been established that a party is obligated to preserve and produce ESI that is not in the party's "possession" or "custody" but nonetheless is within its "control." This article explores the issue of control in the cloud and how courts may view e-Discovery obligations involving preservation and production of data in the cloud.

Old News: Control Is Construed Broadly

Does "Practical Ability" Constitute "Control?"

As Rule 34 and the courts have never limited the duties to preserve or produce strictly to things within a party's possession, parties likely will be required to preserve and produce relevant data in the cloud if the requisite control exists.[8] As cloud computing becomes even more prevalent, courts likely will face an increasing number of situations where possession and control are split between a party to litigation and a third-party service provider.

Whether a party has control over discoverable evidence for purposes of preservation or production often has been equated to whether a party "has the legal right to obtain the documents on demand," extending to documents to which a "party has retained any right or ability to influence the person in whose possession the documents lie."[9] In many courts, control has been interpreted to encompass when a party has the "practical ability" to obtain documents, regardless of his or her legal entitlement to them.[10] This concept of control has been applied in the context of both production and preservation when evaluating a spoliation claim.[11] Thus, broadly defined, control has been found in a wide variety

---

[7] 18 U.S.C. §§ 2701 et. seq.

[8] Federal Rule of Civil Procedure 34 allows a party to serve a request for production of documents and ESI in the responding party's "possession, custody, or control."

[9] *E.g.*, *Tomlinson v. El Paso Corp.*, 245 F.R.D. 474, 476-77 (D. Colo. 2007) (citing *Starlight Int'l v. Herlihy*, 186 F.R.D. 626, 635 (D. Kan. 1999)).

[10] *E.g., Golden Trade S.r.L. v. Lee Apparel Co.*, 143 F.R.D. 514, 525 (S.D.N.Y. 1992) (citing cases). *But see Goodman v. Praxair Servs. Inc.*, 632 F. Supp. 2d 494, 516 n. 11 (D. Md. 2009). The court in *Goodman* noted that not all courts have adopted the "practical ability" test, citing, for example, the Seventh Circuit's observation that "the fact that a party could obtain a document if it tried hard enough and maybe if it didn't try hard at all does not mean that the document is in its possession, custody, or control; in fact it means the opposite," even where the third party likely would have handed over the documents or at least sold them to plaintiffs. *Id.* (citing *Chaveriat v. Williams Pipe Line Co.*, 11 F.3d 1420, 1426-27 (7th Cir. 1993)).

[11] *See, e.g., In re NTL, Inc. Securities Litigation*, 244 F.R.D. 179, 195 (S.D.N.Y. 2007) (The parties had both the legal right and practical ability to obtain documents from the third party, and "therefore had the necessary 'control' of those documents to be able to preserve and produce them in this litigation . . . ."). *But see Goodman*, 632 F. Supp. 2d at 516 n. 11, for cases not applying the "practical ability" test.

of cases, including where a contractual provision confers a right of access, where a party's agent has possession, and where an employee or officer has possession or the legal right to obtain documents.[12]

Control in the Cloud

Because a party often will have the legal right or practical ability to obtain its own data held or maintained by a third-party cloud provider, a party using the cloud provider ultimately may be held responsible for preserving and producing it. Indeed, in a relatively recent case, a court ordered a defendant to provide the plaintiff's counsel with full access to his computers or servers, including those he rented from a third party, in order to create a copy of the hard drives. The court ordered the defendant to inform third parties with possession of the servers to relinquish control to allow this access.[13] In other words, without much analysis, the court treated the servers exactly the same as if they were within the defendant's possession.

Contracts with cloud providers often will (and generally should) establish a party's ability to control its data with relative ease. But even where no contractual right of control is established, a court may still find that a party has control over the data as a matter of law. For example, courts have held that parties had sufficient control over certain personal records, such as cell phone records and financial records, that they were obligated to produce the records.[14]

The court in *Flagg v. City of Detroit* engaged in a lengthy analysis of whether text messages sent by city employees using a system maintained by a third-party vendor were subject to the city's control.[15] The city argued that the Stored Communications Act prohibited disclosure of these text messages by the third-party telecommunications provider without consent from either the city or the employee who sent the text messages, and the city refused to grant this consent.[16] The court found that the text messages were subject to the city's control on the assumption that the city had some contractual right of access to the text messages and because if the city could withhold consent to production of the data, it had the requisite control to consent to the production as well.[17] The court further reasons that because a party who has control over relevant ESI must take the necessary steps to exercise it and

---

[12] See *Flagg v. City of Detroit*, 252 F.R.D. 346, 353 (E.D. Mich. 2008), for cases illustrating the variety of circumstances in which parties have been deemed to have control.

[13] *Zynga Game Network, Inc. v. McEachern*, No. 09-1557, 2009 WL 1108668, at *2 (N.D. Cal. April 24, 2009).

[14] *E.g.*, *Tetra Techs. v. Hamilton*, No. CIV-07-1186-M, 2008 WL 3307150, at *1 (W.D. Okla. Aug. 7, 2008) (holding that the subscriber/user of the cellphone service had the legal right to obtain the cell phone records requested); *Babaev v. Grossman*, No. CV03-5076, 2008 WL 4185703, at *3 (E.D.N.Y. Sept. 8, 2008) (holding that defendants had sufficient control over their bank records to obtain them); *A. Farber & Partners, Inc. v. Garber*, 234 F.R.D. 186, 189-90 (C.D. Cal. 2006) (ordering defendant to sign consent forms to release his documents from nonparties such as Nextel, Pacific Bell, banks, Internal Revenue Service, and California Franchise Tax Board).

[15] *Flagg v. City of Detroit*, 252 F.R.D. 346, 352-64 (E.D. Mich. 2008).

[16] *Id.* at 358.

[17] *Id.* at 354-55.

produce that data, the court could compel either the city or its employees to provide the requisite consent to produce the text messages so as not to violate the Stored Communications Act.[18]

As a general matter, if a party's data is stored in the hands of third parties and may be relevant to litigation, a party may be wise to identify relevant data in the cloud, and if possible, take necessary steps to preserve and perhaps obtain that data. This may be as easy as exercising a contractual right of control over the data, or it may be more complex, such as negotiating access to the data with the third-party cloud provider and even seeking relief from the court where the cloud provider refuses to cooperate.

New Complexities Created by ESI in the Cloud

ESI generally remains subject to the same rules of evidence and civil procedure as traditional paper and tangible things. This has created problems for e-Discovery, however, because issues of possession, custody and control involving intangible ESI are not as easily or obviously resolved as those issues involving hard copy documents and other tangible things. Courts dealing with ESI generally do not distinguish between data in one's *possession* and data in one's *control* for discovery purposes. These cases add new complexities for those grappling with e-Discovery and cloud computing, where – as demonstrated above – possession and control are not readily defined or identified.

Preserving RAM in the Cloud

E-mails, word processing documents, image files, text messages, instant messages, and the like typically are the sort of ESI that come to mind when considering discoverable ESI. But at least one court, in the context of e-Discovery, has held that RAM[19] constitutes discoverable ESI.[20] And not only was it RAM, but the RAM at issue was on a third-party server and thus was maintained in the cloud.

Columbia Pictures Inc. v. Bunnell involved a copyright dispute between Columbia Pictures and operators of a website called "TorrentSpy" that facilitated the copying of copyrighted content but did not store it.[21] As part of its business plan, the defendants never intentionally logged or recorded the IP addresses of visitors to the site.[22] The IP addresses, however, were captured and maintained in the RAM stored on defendants' servers. The court concluded that this information in RAM was discoverable ESI because (i) Rule34(a)(1) was to be interpreted broadly, (ii) information in RAM was

---

[18] *Id.* at 363. The plaintiff had originally subpoenaed the telecommunications provider. *Id.* at 366. In doing its analysis, however, the court assumed that the plaintiff had directed his request for production to the city. *Id.* After completing its analysis, the court acknowledged that it was dealing with a third-party subpoena, not a Rule 34 request for production. *Id.* Because the law was unclear as to whether a court could compel a party to consent to disclosure of materials pursuant to a third-party subpoena under the Stored Communications Act, the court instructed the plaintiff to reformulate his third-party subpoena as a Rule 34 request to the city. *Id.*

[19] RAM is an acronym for "random access memory." RAM is internal memory inside a computer that is generally "volatile" or lost when the power to the computer is turned off. *See, e.g.*, *Apple Computer, Inc. v. Franklin Computer Corp.*, 545 F. Supp. 812, 813 (E.D. Pa. 1982) (description of RAM from an early computer model).

[20] *Columbia Pictures Inc. v. Bunnell*, 245 F.R.D. 443 (C.D. Cal. 2007), *affirming* 2007 WL 2080419 (C.D. Cal. May 29, 2007).

[21] *Id.* at 445.

[22] *Columbia Pictures*, 2007 WL 2080419, at *3.

"stored," if only temporarily, and Rule 34 does exempt temporarily stored data from production or otherwise contain a temporal limitation, and (iii) the data could be obtained by the defendants by enabling logging of IP addresses in the system.[23] At some point, the defendants transferred their website to a third-party entity, such that the IP addresses were then in the RAM stored on the third-party's server.[24] Thus, the court examined whether defendants had control over the data requested by plaintiff, namely the masked IP addresses of the website users, the identity of the files requested, and the dates and times of the requests.[25] The court concluded that defendants had control of this data because they could "manipulate at will" how it was routed through either their own or third-party servers.[26]

It is important to understand the particular circumstances that led the *Columbia Pictures* court to require preservation of RAM maintained by a third-party cloud provider. It seems unlikely that the court intended to create a general rule subjecting RAM to the duty of preservation, as such would be all but impossible in many circumstances due to the temporary nature of many types of RAM.[27] The court in *Columbia Pictures* noted that in that case, the duty to preserve the RAM was imposed only after the court issued its order.[28] Notably, the court did not impose sanctions for the defendants' failure there because the defendants held a good faith belief that preservation of RAM was not legally required.[29] Hopefully, future courts will similarly limit the preservation or production of RAM, especially RAM maintained in the cloud, to (i) after the court issues an order following a showing of relevance by the requesting party and an opportunity for the responding party to demonstrate the difficulties of preserving or producing RAM, and (ii) where preserving specific information captured in the RAM involves reasonable measures, such as enabling an already existing logging function as in *Columbia Pictures*.[30]

---

[23] *Columbia Pictures*, 245 F.R.D. at 447.
[24] *Columbia Pictures*, 2007 WL 2080419, at *3.
[25] *Id.* at *6; *Columbia Pictures*, 245 F.R.D. at 447 n.3
[26] *Columbia Pictures*, 2007 WL 2080419, at *3 n.13, 6.
[27] *See Columbia Pictures*, 245 F.R.D. at 448 ("In response to *amici*'s concerns over the potentially devastating impact of this decision on the record-keeping obligations of businesses and individuals, the Court notes that this decision does not impose an additional burden on any website operator or party outside of this case.").
[28] *Id*.
[29] *Columbia Pictures*, 2007 WL 2080419, at *14.
[30] Though operators of a website may have control over IP addresses in RAM because these IP addresses are necessary to the operation of the website itself, a party who is an end-user of the cloud application may not have any legal right to the RAM on its cloud provider's servers. A contract may provide that the cloud provider will keep a log of the user's activity on the system for business purposes, but absent such a contractual provision, an end user may have no legal right or practical ability to obtain information stored in RAM even about the user's own use.

Routine Deletion of ESI in the Cloud

A party may fail to preserve ESI merely through routine use of its computer systems, even if the party never intentionally or knowingly deletes or alters the ESI on the system.[31] As one uses a computer, unallocated space is overwritten and entries in systems logs entries are routinely replaced.[32] Thus, saving potentially discoverable ESI from deletion through routine operations, to the extent required, can be a difficult task – but the task becomes even more difficult when the data at issue resides in the cloud. It is unclear how a party could effectively prevent the cloud provider from continuing the routine use of its servers and computers even where such use results in deletion of potentially discoverable ESI that a party ultimately may be responsible for preserving or producing. As a result, data within the cloud that a court may deem within a party's control for discovery purposes nonetheless may be subject to routine deletion by a nonparty *not* within the control of the party whose data has been, or is being, deleted – and there may be no way to preserve or produce that data absent causing extraordinary disruptions to the cloud provider's routine operations.

Similarly, it is unclear whether an end user may have control over the unallocated space on the cloud provider's server absent an assignment of hard drives by user or some other partitioning of server space. If a server is shared between or among the cloud provider's customers, the unallocated space and event logs on a particular server likely would contain information concerning the activities and data of nonparties, who understandably would not want their data picked over by strangers, even assuming it were lawful for the cloud provider or a customer to do so.

Finally, one of the advantages of the cloud is scalable computing and that data processing can take place over a network.[33] The identity of each server or computer that is being used is becoming less relevant to the computer user, and multiple computers or servers may be in use. Thus the ability to retrieve deleted files via forensic examination may be severely limited in the cloud.

Your Data, Your Problem

Knowing how courts deal with uncooperative third parties is instructive in understanding a party's duties involving ESI in the cloud. Courts can be unsympathetic to the hapless litigant who is stuck with an uncooperative third party who has possession of relevant data. In a case demonstrating the

---

[31] *Nucor Corp. v. Bell*, 251 F.R.D. 191 (D.S.C. 2008) (concluding that defendant engaged in spoliation of evidence because he continued to use his laptop, which he knew would be relevant to the litigation and which resulted in the alternation and loss of data).
Under the safe harbor provisions of the Federal Rules, "[a]bsent exceptional circumstances," a party is not subject to "sanctions under these rules" for the failure to produce ESI that is "lost as a result of the routine, good-faith operation of an electronic information system." Fed. R. Civ. Proc. 37(e). In *Nucor Corp.*, the court held that this safe harbor applied only to sanctions imposed under the Federal Rules, such as the failure to comply with a court order under Rule 37(b). 251 F.R.D. at 196 n.3. Because the court was imposing sanctions pursuant to its inherent powers and not under the rules, the safe harbor was inapplicable to defendant's use of his computer. *Id.*

[32] *Id.* at 197-98.

[33] *See e.g.*, Amazon Web Services, Amazon Elastic Compute Cloud, http://aws.amazon.com/ec2/ (last visited April 12, 2010). Amazon Web Services provides infrastructure as a service. *Id.* In lieu of maintaining a dedicated server and infrastructure, businesses can essentially rent computing capacity on an as-needed basis. *Id.*

importance of "control," an ERISA plan provider was subject to a motion to compel for records held on its behalf by a third party record-keeper.[34] The third party refused to produce the documents.[35] The provider had requested the documents from the third party, and the moving party also had unsuccessfully subpoenaed the third party.[36] Despite its inability to obtain the documents, the court concluded that the ERISA plan provider had control over the data maintained by the third party because it could not delegate its statutorily-imposed duty, to maintain and ensure that employee benefits records are accessible, to the third-party record-keeper.[37] The court granted the motion to compel.[38]

Similarly, in a harsh example of potential sanctions for third-party conduct, in *Bowman v. American Medical Systems, Inc.*, the court dismissed a products liability case where the product at issue, a prosthetic implant, was discarded by a third party.[39] Plaintiff's counsel had contacted the doctor who removed the implant and requested that the evidence be preserved.[40] The doctor nonetheless threw it out.[41] And the plaintiff was held responsible.[42] The court did not address the issue of whether the plaintiff had the requisite control over the evidence before finding plaintiff responsible.

In *Starlight International Inc. v. Herlihy*, the court held the defendant responsible for the actions of a joint venturer, who was not party to the suit.[43] Because the defendants "chose to venture" with the uncooperative party, they had to bear the burden of his refusal to turn over documents.[44] This conclusion stemmed from the court's holding that as joint venturers, documents were under the joint venturer's joint control and subject to the duty to produce.[45] Because the defendants failed to produce relevant documents after the court had granted a motion to compel their production, the defendants were subject to sanctions pursuant to Rule 37(b)(2).[46]

These decisions suggest that, where key evidence is held solely by a third party but deemed to be within a party's control, that party may be held responsible for preserving or producing it, even where the third party refuses to preserve or produce it. For this reason, the choice of cloud provider may be the most critical decision that ultimately impacts a party's discovery obligations – identifying a cooperative provider, coupled with appropriate contractual safeguards (including perhaps indemnification for sanctions resulting from lack of cooperation), is key.

---

[34] *Tomlinson*, 245 F.R.D. 474, 476-77 (D. Colo. 2007).
[35] *Id.* at 476.
[36] *Id.* at 476-77.
[37] *Id.* at 477.
[38] *Id.* at 477.
[39] *Bowman v. Am. Med. Sys. Inc.*, No. Civ. A. 96-7871, 1998 WL 721079 (E.D. Penn. Oct. 9, 1998).
[40] *Id.* at *1.
[41] *Id.*
[42] *Id.* at *4.
[43] *Starlight Int'l v. Herlihy*, 186 F.R.D. 626 (D. Kan. 1999).
[44] *Id.* at 649.
[45] *Id.* at 635.
[46] *Id.* at 650.

At least one court has demonstrated understanding for the difficulties a party may face when forced to preserve or produce data in the cloud. The Tenth Circuit reversed a dismissal of a case as a discovery sanction where requested ESI was maintained in a database that the plaintiff, Proctor & Gamble, paid to access but did not own or possess.[47] The court acknowledged that Proctor & Gamble faced a dilemma regarding preservation and production of this data because none of the three options available to Proctor & Gamble was feasible.[48] First, though Proctor & Gamble had the legal right to obtain all the data available on the database, it lacked the computing capability to do so and would have had to purchase a costly mainframe. Second, providing the defendants with online access would not have remedied the preservation problem because the database was regularly updated, resulting in routine alterations to the data. Third, paying the third-party provider for the archived data would have cost Proctor & Gamble $30 million.[49]

The Tenth Circuit concluded upon the circumstances that the culpability necessary to impose the sanction of dismissal was lacking.[50] Indeed, the court explained that the district court should have considered the balancing test under Rule 26(b)(2)(C)(iii), which allowed it to limit discovery where "the burden or expense of the proposed discovery outweighs its likely benefit."[51] The Court of Appeals did note that Proctor & Gamble could have asked the third party to make back-up copies, but the court did not suggest that this was required.[52] The court also noted that the defendants could have subpoenaed the information from the provider directly.[53]

Best Practices for E-Discovery and ESI in the Cloud

Given the difficulties and complexities of preserving and producing ESI in the possession of a third-party service provider, what is a cloud computing user to do when faced with pending or anticipated litigation or with discovery requests calling for production of that ESI?

The duty to preserve is well established, though the level of culpability required for imposition of sanctions for spoliation varies between jurisdictions.[54] In a recent opinion from the Southern District of New York, Judge Shira Scheindlin (famous for the *Zubulake* opinions) discussed this duty and when a party's conduct merits sanctions. Specifically, on the issue of culpability in the context of preservation, the court opined that "the failure to take all appropriate measures to preserve ESI likely falls in the

---

[47] *Proctor & Gamble Co. v. Haugen*, 427 F.3d 727, 739 (10th Cir. 2005)
[48] *Id.*
[49] *Id.*
[50] *Id.* at 740.
[51] *Id.* at 739 n.8.
[52] Because the data resides with a third party in a cloud computing environment, the other side may opt to subpoena the third party instead of the party to whom the data may belong. In some cases, the court will require the other side to reframe a subpoena as a Rule 34 request for production. *E.g.*, *Flagg*, 252 F.R.D. at 366.
[53] *Proctor & Gamble*, 427 F.3d at 739 n.8.
[54] *Rimkus Consulting Group, Inc. v. Cammarata*, __ F.Supp.2d __, No. H-07-0405, 2010 WL 645253, at *6-7 (S.D. Tex. Feb. 19, 2010).

negligence category."[55] But the ESI at issue in that case was clearly within the possession of the plaintiffs or their employees, according to the opinion – and the failure to take all appropriate measures arose from the failure to ask the right people the right questions needed to identify and preserve the right data.

In the cloud computing environment, the failure to take all appropriate measures to preserve data may be due to a third party's reluctance to preserve it at all. A party may ask all the right people all the right questions needed to identify and preserve all the right data and provided all the right people with all the right instructions, but nonetheless fail to preserve or produce relevant ESI due to an uncooperative cloud provider who refuses to comply. Because a court may find that the data at issue was within the party's control, notwithstanding the third party's refusal to comply with the party's instructions, counsel might consider certain steps to demonstrate the requisite good faith and hopefully avoid sanctions.

The first step would be to turn to the underlying contract for services the party has with the cloud provider and invoking whatever contractual rights (perhaps under the threat of suit, if necessary) the party has with respect to accessing or obtaining the data. Where the contract provides no help – or where the provider refuses even to comply with the terms of the contract – a party may have to serve the provider with a subpoena for the data. This also may be necessary where the data is subject to certain statutory protections, such as those arising under the Stored Communications Act.

If a third-party provider refuses to cooperate, a party may be well served by informing the other side that relevant data exists with that third party. Where relevant data is not in a party's control, the party still may be deemed as having an obligation to inform the opposing party about the data to ensure the opposing side has an opportunity to inspect or obtain it.[56] Parties also should consider whether the relevant data held by the uncooperative cloud provider also may exist within the party's possession through local logging functions or copies saved locally on the party's own servers or computers.

Perhaps most importantly, parties should carefully document all efforts to preserve or produce relevant data within the cloud. This may be essential to demonstrating the requisite good faith later to avoid sanctions for spoliation of relevant data that otherwise might result from a third-party provider's refusal to preserve or produce data. In *Rimkus Consulting Group, Inc. v. Cammarata, et al.*, Judge Lee Rosenthal held that where spoliation has occurred, "the severe sanctions of granting default judgment,

---

[55] *Pension Committee of the University of Montreal Pension Plan v. Banc of America Securities, LLC*, __ F. Supp. 2d __, No. 05 Civ. 9016, 2010 WL 184312, at *10 (S.D.N.Y. Jan. 15, 2010) (imposing adverse inference instruction on the basis of gross negligence in preserving ESI). *But see Rimkus Consulting Group*, 2010 WL 645253, at *6-7 (declining to apply *Pension Committee* because the level of culpability required for an adverse inference instruction in Fifth Circuit was bad faith, not negligence).

[56] "If a party cannot fulfill this duty to preserve because he does not own or control the evidence, he still has an obligation to give the opposing party notice of access to the evidence or of the possible destruction of the evidence if the party anticipates litigation involving that evidence." *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583 (4th Cir. 2001) (products liability case).

striking pleadings, or giving adverse inference instructions may not be imposed unless there is evidence of 'bad faith.'"[57] She emphasized that "'[d]estruction or deletion of information subject to a preservation obligation is not sufficient for sanctions. Bad faith is required."[58] Although *Rimkus* did not address cloud computing, the court's articulation of the level of culpability required for severe spoliation sanctions suggests that parties that can demonstrate good faith efforts to preserve or produce data maintained in the cloud but that nonetheless failed to preserve or produce the data due to an uncooperative third-party provider might avoid sanctions, at least in the Fifth Circuit and most other federal circuits.[59]

Parties appearing before courts adopting the culpability standard articulated in *Rimkus* might avoid sanctions for failure to preserve or produce data held by a third-party cloud provider by presenting documentation and other proof of good faith efforts to maintain, access or obtain that data. In *Rimkus*, the court instructed the jury "that if it finds that the defendants intentionally deleted evidence to prevent its use in anticipated or pending litigation, the jury *may, but is not required to*, infer that the lost evidence would have been unfavorable to the defendants."[60] The court went on: "Rather than instruct the jury on the rebuttable presumption steps, it is sufficient to present the ultimate issue: whether, *if the jury has found bad-faith destruction*, the jury will then decide to draw the inference that the lost information would have been unfavorable to the defendants."[61]

Thus, the defendants in *Rimkus* were permitted to present evidence at trial to convince the jury that they had *not* acted in bad faith and therefore adverse inferences would not be appropriate.[62] Under this approach, evidence of a party's good faith efforts to access or obtain relevant data held by a third-party cloud provider could be crucial to avoiding severe sanctions at trial.

Finally, parties should recognize that putting data on the cloud is unlikely to absolve them of their discovery obligations. Though not within a party's possession, ESI in the cloud is likely to be deemed with the party's control, which is sufficient to trigger the party's duties to preserve and produce some or all of that data for litigation. Further, the claim that relevant data in the cloud is not reasonably

---

[57] *Rimkus Consulting Group*, 2010 WL 645253 at *6.
[58] *Id.* at *31.
[59] *Id.* at *7 (observing that the Seventh, Eighth, Tenth, Eleventh, and D.C. Circuits, like the Fifth, appear to require bad faith while the First, Second, Fourth, and Ninth Circuits do not and the Third Circuit "balance[s] the degree of fault and prejudice").
[60] *Id.* at *1 (emphasis added).
[61] *Id.* at *10 (emphasis added).
[62] It is unclear whether evidence of good faith would have been helpful or even permitted in *Pension Committee*. There the court issued a jury instruction requiring the jury to accept the court's finding that the plaintiffs were grossly negligent in performing their discovery obligations and directing the jury that it could presume that the evidence that had been lost was relevant to the case and prejudicial to the plaintiffs, unless the jury were to find that the plaintiffs had rebutted that presumption with evidence at trial. *Pension Comm.*, 2010 WL 184312, at *23-24. Although the court did permit the plaintiffs to present evidence at trial to avoid adverse inferences, it appears that, given that the jury was instructed to accept the court's finding that the plaintiffs were grossly negligent, the plaintiffs' evidence may have been limited to showing that the lost ESI was not harmful to the plaintiffs rather than showing good faith efforts by the plaintiffs to preserve or produce that ESI.

accessible under Rule 26(b)(2)(B) is unlikely to succeed, as a general matter, given how easy it often will be for the cloud provider to preserve or produce the data. Choosing the right cloud provider and establishing appropriate contractual rights, much like choosing the right computer systems and establishing appropriate retention policies, will go a long way to preventing headaches later in litigation.

David D. Cross is Counsel in the E-Discovery & Information Management (EDIM) and Litigation Groups in the Washington, D.C. office of Crowell & Moring LLP, and is co-chair of the E-Discovery Subcommittee for the Commercial & Business Litigation Committee of the ABA Section of Litigation. His practice includes antitrust, intellectual property, health care, securities, and general commercial litigation, representing both plaintiffs and defendants in federal and state courts as well as arbitration. David regularly advises a wide variety of corporate clients regarding compliance with electronic discovery and record retention programs and serves as special e-Discovery counsel in complex litigation matters.

Emily Kuwahara is an associate in Crowell & Moring's Los Angeles office and is a member of the firm's Litigation Group. Emily received a B.S. in interaction design engineering, with a focus on the design of human-computer interfaces, and an M.A. in telecommunications, with an emphasis on telecommunications policy. Emily served as law clerk to the Honorable Milan D. Smith, Jr., United States Court of Appeals for the Ninth Circuit.

Federal Magistrate Sets Example for Digitally Signed Official Court Orders

By Timothy Reiniger and Jacques R. Francoeur


On June 7, 2010 in Washington, D.C., the Honorable John M. Facciola, Magistrate Judge for the U.S. District Court in the District of Columbia, will be honored as the designated Laureate for 2010 by the Computerworld Information Technology Awards Foundation Honors Program in recognition of his being the first United States judge to digitally sign judicial orders. Since the first test case on August 26, 2009, Judge Facciola has been digitally signing official court orders and warrants.

Steven Teppler, co-chair of the Electronic Discovery and Digital Evidence Committee ("EDDE Committee"), has described Judge Facciola's official use of digital signatures as "one small step for technology, one giant leap for the legal profession."

"A judge signs his or her name many times each day," said Judge Facciola, who is also an active participant in the EDDE Committee. "The capability to sign electronically an order or other document should create in the people who see it an assurance that the document was signed by the judge and eliminate corrupt attempts to use forged, electronically created documents for improper ends."

Digital Signing Methodology Used by Judge Facciola

To ensure judicial orders signed electronically are reliable and resistant to fraud and manipulation, Judge Facciola's signing method relies upon on a digital certificate, time stamp, and signing platform that permit any relying party the ability to easily verify the authenticity of the order. The judge's digital certificate is issued and secured in accordance with an assurance level equivalent or greater to what the federal authorities refer to as Medium Assurance Hardware -- Federal Bridge Cross Certified. That certification level is based on a high standard of reliability defined by the Federal PKI Management Authority.[1]

Implications for e-Filing in the Courts

The judicial use of digital signatures in signing court orders signals a groundbreaking opportunity for U.S. courts which, despite the widespread use of electronic filing systems, still require handwritten signatures by judges on paper. The ability to implement reliable digital signatures for court filings closes this disconnect, while providing the legal confidence necessary to rely on documents that have been signed electronically.

[1] Federal PKI Management Authority at http://www.idmanagement.gov/fpkia/.

Although the federal courts nationwide have made great strides in enabling e-filing of pleadings, in the minds of many legal experts, they are overdue for a reliable, end-to-end electronic process that includes signing. In fact, otherwise efficient and cost-effective processes break down from a security viewpoint when paper-based signatures are required. Currently, in most courts only an "/s/" or typed name is needed for an electronic signature. "A fully electronic filing system -- that includes electronic signatures -- makes sense for America's courts," Judge Facciola said. "This is the next logical development in the transition from paper to electronic filing."

Implications for the Issuance of Electronic Public Documents

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.[2] 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.[3] 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.[4]

Digitally signing court orders with a high assurance digital certificate and time stamp has the effect of establishing each record as a "reference" or "authoritative source record" for relying parties.[5] This ensures the ability to test the reliability, accuracy, and integrity of the information that was intended to be the equivalent of a paper "original."

Judge Facciola's method for issuing electronic public documents is consistent with the recommendations of the Hague Conference on Private International Law. An international e-document authenticity standard has emerged for an electronic public document that reflects the evidentiary need for electronic documents to have the capability of authenticity testing.[6] This standard requires that any relying party be able to verify the origin and integrity of the electronic public document.[7] 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.

---

[2] 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 Prac. Litigator No. 6, at 212-13 (2004).

[3] 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).

[4] George L. Paul, *FOUNDATIONS OF DIGITAL EVIDENCE,* at 36 (American Bar Association, 2008).

[5] *Id* at 56-59; Jacques Francoeur, *Master Information Management and the Authoritative Source Record Life-Cycle Management Methodology,* at 7 (SAIC, 2009).

[6] *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>.

[7] *Id; see also* NATIONAL E-NOTARIZATION STANDARDS, Standards 14 and 15 (Nat'l Ass'n of Secretaries of State 2006) available at <http://www.nationalnotary.org/commission>.

Implications for Self-Authentication

This marks the first time a U.S. judge has devised a process for issuing self-authenticating official documents in digital form.[8] Signed judicial orders and other official court certifications created from a high-assurance credential are self-proving, thus rendering the attached contents self-authenticating under Rule 902 of the Federal Rules of Evidence.[9] Judge Facciola's approach of embedding intrinsic controls in the document permits relying parties to conduct strong tests of the document's origin, integrity of contents, and date and time of issuance without any need for extrinsic evidence.
Under the Federal Rules of Evidence and the equivalent state evidence rules, public documents under *seal* are admitted without further proof. Specifically, Federal Rule of Evidence 902(1) requires that documents under seal of a public officer, including a judge, be treated as self-authenticating.

Authentication of a document under seal involves the inference of three items: (1) the public officer is who he or she claims to be; (2) the signature and seal are genuine; and (3) the signature and seal were affixed by the named public officer.[10] With the use of a high assurance digital certificate from a trusted provider, the digital signature and seal authenticate a document without the need for extrinsic evidence to prove the genuineness of the judge's identity and officer status.

Judge Facciola's approach to enabling self-authentication with respect to public documents is consistent with emerging laws and standards in the U.S. for electronic notarization. The National e-Notarization Standards issued by the National Association of Secretaries of State require an electronic notarization to give relying parties the ability to independently verify the notary and detect alterations to the signatures and document.[11] Laws reflecting this requirement have recently been enacted in Delaware, Florida, and Virginia. This standard reflects the need for a notarial act, like a judicial act, to be self-proving and to provide the capability of document authenticity testing and non-repudiation.[12]

Legal Significance of the Use of Electronic Signature v. Digital Signature: Final Thoughts

In an interesting unrelated development, Judge Facciola on March 1 participated in a mock trial hosted by the CSO Council Bay Area that explored evidentiary proof aspects of electronic signatures and digital signatures. In the trial, all technical aspects of the various electronic signing approaches were scrutinized by leading attorneys, including EDDE members Steven Teppler and Stephen Wu, and technology experts in the field, including EDDE member Paul Doyle and Adobe CSO, Gary Terrell. The conclusion of the attendees was that any electronic signing method, to be deemed reliable, needed to have intrinsic methods of establishing the integrity of the document and the identity of whomever was

---

[8] *Lorraine v. Markel American Life Ins. Co.,* 241 F.R.D. 534 (D. Md. 2007) (recognizing that electronically stored information is subject to self-authentication under Rule 902 in its entirety).

[9] *See Supra,* note 3, *at 211-12.*

[10] 7 JOHN WIGMORE, EVIDENCE § 2161 (1978).

[11] NATIONAL E-NOTARIZATION STANDARDS, Standards 5 through 11.

[12] NATIONAL E-NOTARIZATION STANDARDS, Standard 13 (Nat'l Ass'n of Secretaries of State 2006). The American Bar Association defines the term "non-repudiation" as "[s]trong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents." DIGITAL SIGNATURE GUIDELINES § 1.20 (American Bar Association 1996).

clicking the button or inserting a USB or smartcard. Outside the context of an electronic signature that has been affixed in the presence of an impartial witness who is later available for trial, the final determination of a document's execution and enforceability will continue to rest on a jury's assessment of each party's veracity and, in disputes involving deceased signers, circumstantial evidence that would establish the "reference" or "authoritative source record."

Timothy Reiniger, Esq., 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 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.

Jacques Francoeur is Senior Director of Identity and Information Assurance, Commercial Business Services, at SAIC. He has authored numerous industry white papers in the area of electronic evidence, including "Master Information Management and the Authoritative Source Record Life-Cycle Management Methodology" (2009) and "Digital Signature Assurance & Digital Chain of Evidence" (2008).

How to Select and Work with Digital Data Forensic Experts

By John Jorgensen

E-Discovery and Digital Data Forensics is upon us with a vengeance. In so many cases, digital data has become crucial during the discovery process, both because of the information it yields between agreeable parties as well as the information opposing parties try to hide. In a real life example, a financial agreement has been made between two parties. The agreement is nebulous concerning the length of the agreement terms. Party "A" (Plaintiff) claims that the length of term was a recognized element and was discussed and acknowledged in an exchange of emails between the Parties. (Who doesn't communicate via email in today's world?)

Opposing Party "B" (Defendant) states that the length of the agreement was discussed but no conclusion or understanding was expressed. Party "A" retained some of the emails but not all. In fact a few crucial email exchanges were not saved. A lawsuit ensues and Party B is required to produce all emails relative to the case. Emails are produced but do not include some of the emails that Party A has. What's up?

Because of the inconsistency in production the Court allows the Plaintiff access to the Defendant's company computer network to recover all emails pertinent to the case. Now Plaintiff's counsel must select a digital data forensic expert. You notice that I did not say a "computer forensic expert." There is far more involved technically than just computers in this case. A computer forensic expert may not unravel what has occurred and therefore your case turns into "he said / she said." This case was not won on the "merits of the case" but rather on spoliation, the deletion of evidence and the complicity of counsel in not producing data relevant to the case provided by the defendant. Unraveling what happened by using network, computer, and messaging information disclosed the evidence of the acts, "abuse of process," the spoliation of data and the anti-forensic activity taken to cover up the nefarious acts.

Digital data is the backbone of almost all businesses as well as personal communications. Digital data is difficult to get rid of because it becomes duplicated across so many devices and interfaces on a networked system, even small networks in a home environment. A devious individual may shred a hardcopy of a document only to find out that the document was scanned into a digital file or there was a reference to the document in emails of people that saw the document, worked on the document or provided MS Excel spreadsheet information that went into the document.

Digital data records take the form of emails, MS Excel spreadsheets, proprietary financial databases, photographs, audio files, company Web pages, word processor documents, text files, drawings, Computer Aided Design documents, software coding, mathematical algorithms, Web based fill-in forms, specialized scientific data, encrypted or specially formatted backup data, coded machine-to-machine information and other uniquely formatted information.

Then there is computer, network and communications digital data that is less obvious: meta data of various types of documents, email attachment temporary files, email header information, Master File Table records, computer registry information, system event logs, security event logs, application event logs, event logs specific to purchased software, temporary data files, communications software logs, communications equipment logs, transaction logs, financial software activity and process logs, latent html images, temporary data backups, device attachment logs, software "run" logs and other pieces of information about what was done, when it was done, how it was done and who "done" it.

The number of cases that don't require a digital data forensic expert are becoming fewer and fewer. Our hearts and souls are being bared on the computer. Our lives are being recorded on the computer. Our businesses are run on a computer. Our company confidential and proprietary information is kept on computers. And our most precious company and personal data is stolen from our computers.

Here is a partial list of digital data related questions whose answer was decisive in winning our client's case (we are at approximately 300 cases currently):

- Who used the computer and when?
- What data is/was on the computer and when was it created, accessed, moved or copied?
- What memory devices were connected to the computer during the time period of interest?
- What computer programs were run and when?
- What web sites did the User go to and when? What was on the Web site then?
- Was the network penetrated (hacked), by whom and for what purpose?
- Did the User have any undisclosed email accounts and what were they?
- Did the computer remotely connect to the defendant's company network?
- What networks or other computers did this computer communicate with?
- What computer processes were run and when?
- How often was the computer used and for what general purpose?
- Was data or evidence deleted and/or wiped from the computer network or memory devices?

How to Choose a Digital Data Forensic Expert

Who are the digital data (computer) forensic experts? What are their backgrounds? What are their qualifications? I had an experience in Federal Court, just a few years ago, that really surprised me. Asked to provide my background and experience I provided testimony on my former 20 plus years employment by an intelligence agency and my work in digital data collection, analysis and processing

as well as my military experience in software development and computer technology. I had also previously testified in several cases, served as a Special Master and had over 150 cases under the belt.

Well, the opposing forensic expert took the stand and "fessed up" that during his deposition he had exaggerated the number of times he testified and the forensic software he was using wasn't licensed, and he wasn't actually certified by Encase, and … Even so, the Federal Judge allowed his "expert" testimony saying that, "everyone has to start someplace." Fair enough, one might say, but the case involved hundreds of millions of dollars if not a couple of billion. Six hearings later we got our "adverse inference" over spoliation issues. However, it was a costly battle for our client, over $750,000 in forensics work. You don't know who you are going up against. You cannot assume their honesty. You cannot assume their experience or expertise. There is no court or regulatory mandated criteria or requirements for the "computer forensic expert." Let's look at some of the backgrounds of digital data forensic experts:

- Ex-police officers – By virtual of government budgets, police officers frequently work with "free" or inexpensive forensic software and equipment. They have a few years of experience, limited training and restricted analysis time due to case overload. Therefore, most computer forensic experts who are from law enforcement have a lot of catching up to do. We recently hired a state law enforcement officer who was responsible for computer forensic analysis on some of the high profile child molestation and murder cases for the state. He says unequivocally that he had a lot of learning and catch up to do when he came to work for us. He now feels comfortable in being able to conduct a computer forensic investigation after having worked for us for a year. There are some excellent former law enforcement forensic experts, I'm sure. But, I haven't met the individual yet. Don't select your digital data forensic expert by virtue of their law enforcement prior service.

- Computer Information Technology (IT) personnel – simply put "computer forensic investigation" is far more exciting to some than slogging it out in the IT world, or seemingly so. These individuals are frequently self taught, may be refugees from the IT world where they were unsuccessful or overwhelmed, and bring little or no experience to forensic analysis. Frequently their use of terminology will be inconsistent, they won't know how to write an Expert Report, have no knowledge of Affidavits or Motions and brag about their "hacker" ability. Again, I'm sure there are excellent IT personnel who have taken up computer forensics and I have met a few.

- In-house Law Firm IT personnel – from what we have dealt with in law firms the IT personnel need to concentrate on their primary jobs: management of IT resources and cyber security. Of all of the professional organizations that we work with law firms have some of the worst cyber security posture and protection. Occasionally we will find an IT person within a law firm that is a good forensic analyst. However, more often the IT person is torn between IT responsibilities and forensic / e-Discovery work and nothing gets done well or on time.

- Ex-Intelligence Agency and Military Service technologists – We highly recommend individuals with this kind of background provided that they have multiple tours of duty under their belt. Typically these will be some of the most qualified forensic experts. They have the training with multiple schools in related fields. They have the budgets for some of the best software and equipment. They have the discipline from well developed processes and methodology. They are expected to produce concise and understandable reports.

- There are also a limited number of very smart technologists and academics who are self-taught and highly driven. These individuals are known within the forensics world. Many of them have written successful books and have found a niche within the industry. They are very costly and are difficult to get assigned, personally, to the forensic cases.

- The "Forensic Firms" – hiring a large firm with forensic capability can be a problem. You're hiring a name and you may not know who you are hiring. We had an experience with a large client whose legal counsel wanted to change the forensic experts in the case. Counsel wanted to present their case using a national forensic firm that could carry some weight during the trial. The national firm showed up at our door with their forensic expert lawyer and a technician. We provided them with access to the original hard drives associated with the case and space to make forensic images with their equipment. After several hours they came to us with a problem. They were trying to make the forensic images but the hard drive that we provided would not image using their software. I looked at the original hard drives, concerned that they may have corrupted the evidence. But, the data seemed intact and uncorrupted.

  I then asked to see their software tools that they were using to make the images. They handed me a disk. I looked at the disk contents on the forensic computer and noted several executable programs that looked like the forensic tools. Each program file size was 1 kilobyte. They had copied the names of the programs onto the disk but not the executable program itself. We made forensic images for them using our equipment. Several months later we received a panic call from the boutique law firm in Chicago. Could you please complete the forensic analysis that you had started. The national forensic firm could not identify the financial program databases that we had previously identified on the forensic images. They had three weeks to produce the evidence before the trial. We then completed the forensic work on the case, produced the evidence and our client won their case. But, it wasn't the national forensic firm that successfully performed the analysis; it was the little firm that knew the right questions to ask and where to find the evidence.

  Everything that I said above has exceptions; just beware and don't accept a forensic expert based solely on their former or present employment.

<u>Here are some questions to ask of your potential forensic expert</u>

- What is the Forensic Analysis firm's depth?

    - Do they conduct internal peer reviews of their analysis? Who conducts the peer review?
    - Do they have in-house software development capability?
        - When you have a problem collecting and collating data during e-Discovery do you solve the problem internally or do you depend solely on vendor software?
        - Are you familiar with how proprietary software interfaces with the cases associated databases?
- Do they have in-house technical support?
    - Build computers and networks to simulate conditions within a particular case
    - Handle forensic hardware problems and requirements
- Do they have familiarity with court proceedings and the legal process?
    - Do they produce Affidavits and Expert Reports as a normal part of their case work?
    - Do they provide support to counsel in filing Motions and other related filings?
- Is their forensic Methodology a written document submitted with their Expert's Report?
- Can they conduct e-Discovery processes internally?
    - What search software is used?
    - Have them describe their interface with counsel while conducting search
    - Have them describe their data format specification
    - Have them describe term search methodology and process
- How do you prepare and handle Privileged Data?
- What is the Forensic Expert Report's outline and structure?
    - Outline General Headings (Sample)
    - Conclusion Statements
    - Attachments and supporting information
- Have them prepare a page describing their most technologically challenging case
- Have them provide a short description of the forensic cases over the last five years. This short description would normally be provided with the forensic analyst's CV in the Expert's Report.

The response to these requests will enable you to evaluate how well the Forensic Expert is able to write, compose their thoughts and their use of technical terminology.

<u>Here are some questions for yourself</u>

Do you understand what the Forensic Expert has written? If you don't understand the terminology, argument and conclusions the judge and jury are not going to understand the points the Forensic Expert was trying to make.

Is this a one-man forensic analysis capability or is the forensic expert able to confer with peers in order to validate his ideas, beliefs and conclusions?

Has the forensic expert testified in both local judicial and federal cases?

Has the forensic expert served as Special Master to the Court?

Does the forensic expert make presentations or write papers on technical aspects of digital data forensics.

Does their forensics lab have any accreditations, e.g. ASCLAD Laboratory?

What digital data (computer) forensic software do they use? The response list should include the standards such as X-Ways and Encase. If they rely on some of the other "lighter" report-centric software you could find yourself in trouble. Report-centric software will frequently mislead the forensic analyst unless he validates the software-reported results by using data-centric forensic software such as X-Ways.

Did any of their cases make Westlaw Review or any other notable reviews?

Does the forensic expert prepare Affidavits and help counsel prepare Motions, Subpoenas, Warrants, Confidentiality Agreements and other legal documents that are part of the e-Discovery process.

Does the forensic expert participate in 26(f) and Meet & Confer Conferences?

Does the forensic expert assist in preparation of questions for the depositions and monitor depositions?

Does the forensic expert seem to know more about the e-Discovery process than you?

Does the forensic analyst participate in creating a "Preservation Notice"?

How to Work with a Digital Data Forensic Expert

The answer is, "Closely!" There are five basic areas for close cooperation between counsel and the digital data forensic expert. These five areas also represent a guideline for obtaining and explaining the evidence to the court. We feel that it's important to recognize these steps because very different things occur in each one and without completion of the previous step one cannot adequately proceed to the next. We are frequently asked to put this information in a "laundry list" format, so here it is:

1) Preparation for e-Discovery
2) Technical input for obtaining evidence
3) Obtaining evidence
4) Reporting the evidence and findings
5) Explaining the evidence to the court

In each of these steps major functions occur which require input and participation from counsel. Let's review each of the steps and see why that interface is important.

Preparation for e-Discovery

The Preparation step consists of:

1) The strategy meeting:
    a. Has an Evidence Preservation Letter been issued?
        i. Has the Preservation Letter been issued to all potential parties in the case?

ii. Has the Preservation Letter identified all potential sources of information (e.g. Computers and servers, Memory devices, Firewall logs, Backups, Email accounts to include Web-based, Communications logs, etc.)?

b. What is the objective of the case?
   i. To prove the Intellectual Property was stolen?
   ii. To prove the intent of a financial transaction?
   iii. To prove prior knowledge of some misdeed?
   iv. Other?

c. What information currently do you deem as important and bears to the merits of the case?
   i. Financial?
   ii. Email communications?
   iii. Company Confidential or Intellectual Property (IP) information?

d. What other information may be important to the case?
   i. Prior contracts with future employer?
   ii. Previously unknown private business in competition with the client's company?
   iii. Previously unknown connections with organized crime?
   iv. Web based email service not disclosed?
   v. Fraudulent financial records?
   vi. Other?

During the strategy meeting both counsel and the forensic expert will be able to focus on the information that may prove useful and any difficulty in obtaining that information. As an example; counsel may say that they want all emails within a certain period of time. The forensic expert might suggest asking for email backups as well, because the email backups may contain emails that were deleted and purged by the User on the User's computer. Or counsel may say that they want the Web Site for the opposing party's business during a certain period of time. The forensic expert might point out that counsel also wants to ask for the Web Site *source code*, *custom page directory*, and *stored procedures* for that period of time. The forensic expert may also point out the importance of making forensic images when possible and validating the computer / server data, which means ensuring that the data is valid and present for those Users and the period of time of interest.

2) The 26(f) and Meet & Confer conference;
   a. Where do you think you will find the information that you are looking for?
      i. Which computers, which servers, which network?
      ii. Which backup tapes?
      iii. Which web based email service?
      iv. Other sources such as Web Page services, etc.
   b. What format might the information be in?
      i. Native format?

ii. Proprietary financial database?
iii. Source code?
iv. Header information from the email server or an individual's computer?

c. What format are you willing to accept?
i. Non-native format?
ii. Database information without the proprietary software?
iii. .ost files rather than .pst files.
iv. .pdf rather than .tiff or .doc or …

Having a savvy forensic expert appear during the 26(f) and Meet & Confer Conference will keep you out of trouble. As an example in one of our Meet & Confer Conferences the opposing counsel stated that they would provide the financial records being requested in MS Excel format. Opposing counsel agreed to provide the Excel spreadsheets in "native format." Our client counsel was very happy and smug in getting opposing counsel to provide native format *until* the forensic expert asked, "By the way, what financial software processes data in Excel format?" (The answer was, "none"!) The financial package was Great Plains and the original database is in a proprietary format. The Excel output provides only that data that the User selects for output. Nope, we want the original data base and we will load it into our copy of Great Plains, thank you. And by the way, we want all of the databases that you might load to the Great Plains software, to include backups, alternatives, or test cases.

Technical Input for Obtaining Evidence

The forensic expert is important in identifying the sources and manner for collecting evidence during the discovery process. The forensic expert should be able to diffuse evidence collection arguments such as "confidentiality" and "overly burdensome" by describing collection processes that will protect confidential or privileged information or prevent or minimize computer downtime for the opposing parties.

The manner in which evidence is obtained can be critical if:

1) spoliation has occurred;
2) you are unsure that you have all of the evidence;
3) you are unsure that you are getting the evidence correctly the first time;
4) you are unsure that you have identified all and the right computers / servers / networks;
5) you don't know when you have been "gamed."

Spoliation has been playing a greater part in our cases over the last three years. 80% of the cases in the last three years have involved some form of spoliation and most of those have involved an attempt to cover up the spoliation by the use of anti-forensic software or methods. Spoliation has been perpetrated by individuals, IT departments and law firms. Therefore, a key element in obtaining evidence is the ability to determine if spoliation has occurred. It has driven us to developing specialized software to review the data on memory media and identify if there are unusual data sequences that do not follow the normal processes for data recording.

It's important to listen to the forensic expert if he uncovers any information that indicates spoliation may have occurred. More and more cases are being won on the issue of spoliation without the merits of the case being tried.

Obtaining Evidence

1) Did you incorporate the forensic expert's "validation of the computers and memory devices" in your Discovery documents?
2) Obtaining a Chain of Custody Report detailing who had access to what computers / servers / devices and when, will prove important in resolving data access and creation date/time stamp ambiguity.
3) Include in your Discovery request Evidence Documentation and Logs to establish who received what evidence and when. We have had cases when the wrong hard drives were delivered for forensic analysis.
4) Affidavits and Motions should include information by the forensic analyst when they are:
    a. Affidavits indicating that not all evidence defined was provided by opposing parties.
    b. Affidavits indicating that not all computers / devices / servers relative to the case were identified by opposing parties.
    c. Motions for sanctions because of spoliation.
    d. Motions to Compel.
5) Or NOT obtaining the evidence (i.e. Spoliation):
    a. Forensic "validation" of the computer / devices / servers indicates that unexplained data wiping has occurred.
    b. Devices have been identified that indicate that evidence has been transferred to them, but the device was lost / destroyed / thrown away.
    c. Forensic validation of the computer /devices / servers indicates that anti-forensic software has been run (executed) during time frames of interest.

Reporting the Evidence and the Findings

The forensic expert should understand the use of Interim and Final Reports. His reports need to be factual and detailed. The details should be further explained and proven through the use of technical attachments that provide screen shots of the data as displayed by the forensic software. There are a lot of software programs in the marketplace that claim to provide information about data on a hard drive. Few are true forensic software. Many provide erroneous information in report form and can be easily challenged in court. A forensic expert must be careful not to base his opinion on report-centric software solely. He must be capable of demonstrating his conclusions based on the actual hexadecimal and binary data recovered from the hard drive. The hexadecimal and binary data should be displayed in the Expert Report Attachments.

The Expert Report (Interim and Final) should have understandable and definitive conclusions. The conclusions should be stated at the end of the report with separate paragraphs for each conclusion.

Each conclusion should incorporate the phrase "with a reasonable degree of scientific certainty." If the forensic expert cannot incorporate that phrase into his conclusion then he does not have a conclusion.

Explaining the Evidence to the Court

Whether it be in Hearings or during the Trial certain key elements of the Experts testimony are critical to winning the case. Judges are not computer forensic experts. Therefore, clarity and simplicity play an important part in making the forensic expert's conclusions understandable. The forensic expert must, at least, do the following:

1) Speak to the court with terminology and examples that are understandable. It's always good when the judge turns to your forensic expert for further information not for clarification. If, you the counsel, are puzzled by the forensic expert's statements, so will the judge and/or jury.
2) Use demonstratives to make critical and key points as well as to summarize the conclusions.
3) Incorporate timelines for each critical facet of the conclusions.
4) Find ways to compare the technology to something the court might understand; i.e. "a hard drive is like a filing cabinet."
5) Prepare for the cross-examination. Keep the forensic expert from dropping into terminology and explanations that no one understands.
6) Go over the technical aspects of the conclusions with your forensic expert until you understand the ramifications of what's being testified to and what are the possible rebuttals by the opposing counsel or forensic expert.

In today's world of digital data communications, processing and storage, the forensic expert is becoming instrumental in recognizing what the evidence might be, in finding the evidence, and in demonstrating the significance of the evidence to the court. Take the time to evaluate your forensic expert.

John Jorgensen has been the President and CEO of The Sylint Group since 1999. Mr. Jorgensen formerly worked over 25 years for the National Security Agency in the military, as a civilian employee and as a government defense contractor. Mr. Jorgensen developed the computer forensic analytical process and techniques for the Sylint Group based on analysis and processing techniques designed, developed and implemented while working for the National Security Agency, in the military, as a direct employee, and as a government contractor. Mr. Jorgensen has briefed the Director NSA, the Under-Secretary of Defense, and the House Permanent Select Committee on Intelligence, on various intelligence matters. Mr. Jorgensen has served as Special Master to the Court, served as an Expert Witness in both Federal and local Judicial jurisdiction and has overseen the computer forensic analysis of over 200 successful cases. He has lectured before the Tiger Bay Association, Ford & Harrison LLP, Employers Association of Florida, National Private Investigator's Association, Tampa Bay FBI Infragard, American Bar Association, RSA Conference and other organizations concerning forensic analysis, e-Discovery and cyber security.

The *Pension Committee* Decision

By Steven W. Teppler

Self-referred to as "Zubulake Revisited, Six Years Later," the Pension Committee decision advances the practice of law in the digital age as much by what it implies as what it holds for issues involving ESI preservation, holds, and attorney competency and candor. This 87 page decision has drawn much attention from both the legal as well as the vendor community. This decision, from U.S. District Judge Shira Scheindlin of the Southern District of New York (and the author of the seminal Zubulake opinion series) involves a lawsuit by nearly 100 investors of a failed hedge fund. The losses alleged exceeded 500 million dollars.

Like a preacher beginning a sermon, and in what is probably one of the finest examples of a contextual set piece I've seen, the court first provides a comforting homily:

"In an era where vast amounts of electronic information are available for review, discovery in certain cases has become increasingly complex and expensive. Courts cannot and do not expect that any party can meet a standard of perfection." *Pension Committee of University of Montreal Pension Plan v. Banc of America Securities,* 2010 WL 184312, 1 (S.D.N.Y. 2010).

Thence cometh the fire and brimstone:

"Nonetheless, the courts have a right to expect that litigants and counsel will take the necessary steps to ensure that relevant records are preserved when litigation is reasonably anticipated, and that such records are collected, reviewed, and produced to the opposing party. As discussed six years ago in the *Zubulake* opinions, when this does not happen, the integrity of the judicial process is harmed and the courts are required to fashion a remedy. Once again, I have been compelled to closely review the discovery efforts of parties in a litigation, and once again have found that those efforts were flawed. As famously noted, "[t]hose who cannot remember the past are condemned to repeat it." By now, it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records-paper or electronic-and to search in the right places for those records, will inevitably result in the spoliation of evidence." *Id.*

Did someone mention spoliation? Duties to preserve ESI? Reasonable anticipation of litigation? Yes, yes, and yes.

This case is interesting in that it is defendants who asserted claims of ESI spoliation by plaintiffs. Here, defendants alleged that plaintiffs had failed to preserve ESI, that there were gaps in plaintiffs' ESI production, and that plaintiffs had falsely certified (think Fed.R.Civ.P. Rule 26(g) certification) and that plaintiffs had thereby engaged in discovery abuse (and spoliation).

Author's Note: To those who believe that spoliation is a "weapon" used by "plaintiffs" – this decision should as a reminder that one's status as an ESI requester or producer is party neutral.

The Court then reminds the reader that this case is one involving some degree of negligence, and not one of intentional failure to preserve or spoliation. It is important to keep in mind that this case addresses the outside bounds of sanctions severity (rather than determination of imposition itself) in a jurisdiction where even ordinary negligence can result in the imposition of evidential penalties.

Succinctly stated: "This is a case where plaintiffs failed to timely institute written litigation holds and engaged in careless and indifferent collection efforts after the duty to preserve arose. As a result, there can be little doubt that some documents were lost or destroyed." *Id*., at p 2.

Defining Negligence, Gross Negligence and Willfulness in the Discovery Context

The court then provides an instructive reprise of ordinary (or "mere") negligence, gross negligence, and other related concepts relevant to ESI discovery issues, highlighted below. The court also explains how conduct might fall into one category or the other.

Negligence

"[Negligence] is conduct "which falls below the standard established by law for the protection of others against unreasonable risk of harm." [Negligence] is caused by heedlessness or inadvertence, by which the negligent party is unaware of the results which may follow from [its] act. But it may also arise where the negligent party has considered the possible consequences carefully, and has exercised [its] own best judgment." *Id*., at p. 3

The court advances ESI discovery jurisprudence by applying the hoary principals of negligence (of whatever degree) to ESI discovery related conduct, beginning with a standard of care:

Standard of Acceptable Conduct

"The standard of acceptable conduct is determined through experience. In the discovery context, the standards have been set by years of judicial decisions analyzing allegations of misconduct and reaching a determination as to what a party must do to meet its obligation to participate meaningfully and fairly in the discovery phase of a judicial proceeding. A failure to conform to this standard is negligent even if it results from a pure heart and an empty head." *Id*.

*Author's Note***:** In those jurisdictions (such as the Second Circuit) where mere negligence in ESI discovery practice can result in evidential sanctions, the message is clear (and especially to those litigators who have been engaging in discovery for "decades") --- a minimum level of competence (together with cooperation and candor) is required to practice in this area. Without that competence, the risk of sanctions is great. For corroboration, one need only look to the Seventh Circuit Electronic Discovery Pilot Program principles, which require that counsel retain technology liaisons where their competency needs…augmentation. This decision teaches that from within the ESI discovery context

counsel ignorance about ESI practice can (and will) constitute negligence. Think also about the *T.J. Hooper* opinion from Judge Learned Hand, and what a party must do (or refrain from doing) in its adherence to the "standard" of acceptable conduct.

Gross Negligence

"'Gross negligence has been described as a failure to exercise even that care which a careless person would use.' According to a leading treatise - *Prosser & Keeton on Torts* - most courts find that gross negligence is something more than negligence 'and differs from ordinary negligence only in degree, and not in kind.'" [Internal footnotes omitted] *Id*.

Gross Negligence – Triggering Conduct

The court then discusses the concept of gross negligence, explaining that actions that fall into this category require at least some degree of intentionality:

"[*Prosser & Keeton on Torts*] groups willful, wanton, and reckless into one category that requires 'that the actor has intentionally done an act of an unreasonable character in disregard of a known or obvious risk that was so great as to make it highly probable that harm would follow, and which thus is usually accompanied by a conscious indifference to the consequences.'" *Id*.

Application of Negligence Standards in the Discovery Process

The court next discusses how the concept of ordinary and gross negligence find application within the ESI discovery process, and begins its discussion in "chronological" order, summarized below:

Step One – Failure to Preserve Relevant Information, Negligence Triggers, and Litigation Holds

Here, the court notes that a failure to preserve is at least negligent, and may under certain circumstances, constitute gross negligence. (The decisional precedent cited by the court in footnotes – omitted in these excerpts - provides an excellent referential framework). The court notes that the intentional destruction of relevant ESI, after a duty to preserve has attached, is considered willful (and a gross negligence conduct trigger).

The court takes special notice that, post-*Zubulake*, the failure to implement a written litigation hold constitutes gross negligence because that failure is likely to result in destruction of relevant evidence:

"A failure to preserve evidence resulting in the loss or destruction of relevant information is surely negligent, and, depending on the circumstances, may be grossly negligent or willful… For example, the intentional destruction of relevant records, either paper or electronic, after the duty to preserve has attached, is willful… Possibly after October, 2003, when *Zubulake IV* was issued, and definitely after July, 2004, when the final relevant *Zubulake* opinion was issued, the failure to issue a written litigation hold constitutes gross negligence because that failure is likely to result in the destruction of relevant information…" *Id*.

Step Two – Collection and Review – Failure to Collect as Negligence

The court employs similar negligence analysis standards to a party's ESI collection and review obligations, with the degree of negligence (whether ordinary or gross) dependent upon the degree of intentionality or willfulness.

"The next step in the discovery process is collection and review. Once again, depending on the extent of the failure to collect evidence, or the sloppiness of the review, the resulting loss or destruction of evidence is surely negligent, and, depending on the circumstances may be grossly negligent or willful." *Id.*

Intentionality Continuum and the Duty to Collect or Preserve – "Key" vs. "All" Players

The court then compares a complete failure to collect records from key players (deemed gross negligence) with a failure to obtain records from all players.

"For example, the failure to collect records-either paper or electronic-from key players constitutes gross negligence or willfulness as does the destruction of email or certain backup tapes after the duty to preserve has attached. By contrast, the failure to obtain records from *all* employees (some of whom may have had only a passing encounter with the issues in the litigation), as opposed to key players, likely constitutes negligence as opposed to a higher degree of culpability." *Id.*

Author's Note: This analysis is helpful to some extent, but as ESI spoliation practice (and decisional authority) evolves, the ordinary vs. gross negligence determination will probably be more fact-bound than mechanistic. For example, some "players" may be more "key" than others, and failing to preserve and collect from these individual(s) might be considered mere, or ordinary negligence. The court so notes:

"These examples are not meant as a definitive list. Each case will turn on its own facts and the varieties of efforts and failures are infinite. I have drawn the examples above from this case and others. Recent cases have also addressed the failure to collect information from the files of former employees that remain in a party's possession, custody, or control after the duty to preserve has attached (gross negligence) or the failure to assess the accuracy and validity of selected search terms (negligence)." *Id*.

The Duty to Preserve and Spoliation

The court turns next to the intersection between the duty to preserve and the act of spoliation, and provides a good working definition:

"Spoliation refers to the destruction or material alteration of evidence or to the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. The right to impose sanctions for spoliation arises from a court's inherent power to control the judicial process and litigation, but the power is limited to that necessary to redress conduct "which abuses the judicial

process." The policy underlying this inherent power of the courts is the need to preserve the integrity of the judicial process in order to retain confidence that the process works to uncover the truth.... The courts must protect the integrity of the judicial process because, "[a]s soon as the process falters ... the people are then justified in abandoning support for the system." *Id.*, at p. 4

"The common law duty to preserve evidence relevant to litigation is well recognized. The case law makes crystal clear that the breach of the duty to preserve, and the resulting spoliation of evidence, may result in the imposition of sanctions by a court because the court has the obligation to ensure that the judicial process is not abused." *Id.*

"'It is well established that the duty to preserve evidence arises when a party reasonably anticipates litigation.' [footnote omitted].' '[O]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents.' A plaintiff's duty is more often triggered before litigation commences, in large part because plaintiffs control the timing of litigation." *Id.*

Author's Note: The reasonable anticipation of litigation standard is federal common law, but inter-district interpretation is fluid. Some courts have interpreted the anticipation standard narrowly, and require some showing that anticipation of some specific litigation be shown. Other federal courts have required demonstration of a reasonable anticipation of a specie, or type of litigation involving a type of evidence. Some state courts (such as Florida) have no reasonable anticipation of litigation requirement, and impose a duty to preserve only where required by contract, statute, regulation, or where a discovery request has been propounded. The discussion of a court's power to sanction for spoliation (whether pursuant to its "inherent powers" or through the operation of Fed.R.Civ.P. Rule 37 --- and perhaps Rule 26) also relates to federal courts.

Burdens of Proof

The court next discusses "what can be done" when ESI is no longer available. The court first acknowledges the problem that faces current evidence spoliation practice, and that is assessment of what lost documents might have contained, and points out that although "lost" information content might be inferred from either witness testimony or related documents, it is still "almost impossible" to know what was contained in what is now lost.

<u>Relevance and Prejudice</u>

The court then lasers in on the two critical issues to any spoliation analysis: who should bear the burden of establishing that the lost evidence would have been relevant, and who should be required to "prove that the absence of the missing material has caused prejudice to the innocent party." Diverting into an analysis of these burdens as it is applied to sanctions severity (rather than imposition), the court explains that where the sanctions are non-evidential (attorney fees and costs, cost-shifting) the burden focuses more on the spoliating party than on the content of the document lost. Where

evidential (outcome dispositive or outcome determinative) sanctions are at stake, the analysis includes both spoliating party conduct and relevance of the evidence spoliated:

"The burden of proof question differs depending on the severity of the sanction. For less severe sanctions-such as fines and cost-shifting-the inquiry focuses more on the conduct of the spoliating party than on whether documents were lost, and, if so, whether those documents were relevant and resulted in prejudice to the innocent party. As explained more thoroughly below, for more severe sanctions-such as dismissal, preclusion, or the imposition of an adverse inference-the court must consider, in addition to the conduct of the spoliating party, whether any missing evidence was relevant and whether the innocent party has suffered prejudice as a result of the loss of evidence." *Id.*

Relevance – Second Circuit Approach; Proof of Relevance vs. Proof of Prejudice

The court then turns to Second Circuit decisional authority for the definition of relevance. The Second Circuit has held that relevance means "more than sufficiently probative to satisfy Rule 401 of the Federal Rules of Evidence." *Id*., at p. 5. Relevance in a spoliation analysis under Second Circuit authority means that the innocent party is required to establish that the missing evidence would have been helpful to its claims or defenses (which, in my opinion, is very close to requiring proof of a negative). The court provides by way of example the imposition of the evidential sanction of an adverse inference:

"Rather, the party seeking an adverse inference must adduce sufficient evidence from which a reasonable trier of fact could infer that "the destroyed or unavailable evidence would have been of the nature alleged by the party affected by its destruction."

"It is not enough for the innocent party to show that the destroyed evidence would have been responsive to a document request. The innocent party must also show that the evidence would have been helpful in proving its claims or defenses- i.e., that the innocent party is prejudiced without that evidence. Proof of relevance does not necessarily equal proof of prejudice." *Id.*

Author's Note: This last sentence, "proof of relevance does not equal proof of prejudice" is where many spoliation assertions hit a brick wall. Proving prejudice necessarily entails some proof of information contained in lost ESI. Well, if ESI is lost, the chances of proving content, save for some exceptional circumstances involving related documents, witness testimony, or other probative circumstantial evidence, are small at best. The court fashions a remedy for this later in the opinion.

Proving Prejudice – The Second Circuit Three-Step Test

Author's Note: Before reading what follows, keep in mind that the court's discussion centers on sanctions severity, not on whether sanctions imposition determination.

The court then provides the three-step test for determination of sanction severity imposition. Note that the test itself is somewhat tautological, in that it while it describes relevance, to a proof of a claim or defense, but does not expressly mention "prejudice," which appears to impose a stronger showing:

"In short, the innocent party must prove the following three elements: that the spoliating party (1) had control over the evidence and an obligation to preserve it at the time of destruction or loss; (2) acted with a culpable state of mind upon destroying or losing the evidence; and that (3) the missing evidence is relevant to the innocent party's claim or defense." *Id*.

Presumption of Relevance and Prejudice – Second Circuit Doctrinal Authority

If there is any wonder why spoliation determinations provide fertile ground for migraines, let's look at Judge Scheindlin's excellent requirements analysis for imposing evidential sanctions. The short version (which is only the camel's nose in the tent):

"In short, the innocent party must prove the following three elements: that the spoliating party (1) had control over the evidence and an obligation to preserve it at the time of destruction or loss; (2) acted with a culpable state of mind upon destroying or losing the evidence; and that (3) the missing evidence is relevant to the innocent party's claim or defense." *Id*.

Now, follow the bullets (excerpts from p. 5 of the opinion. Footnotes, citations, etc. are omitted):

1. Relevance and prejudice may be presumed when the spoliating party acted in bad faith or in a grossly negligent manner.

2. Where a party destroys evidence in bad faith, that bad faith alone is sufficient circumstantial evidence from which a reasonable fact finder could conclude that the missing evidence was unfavorable to that party.

3. Although many courts in this district presume relevance where there is a finding of gross negligence, application of the presumption is not required.

4. However, when the spoliating party was merely negligent, the innocent party must prove both relevance and prejudice in order to justify the imposition of a severe sanction.

5. The innocent party may do so by "adduc[ing] sufficient evidence from which a reasonable trier of fact could infer that 'the destroyed [or unavailable] evidence would have been of the nature alleged by the party affected by its destruction.'"

6. In other words, the [innocent party] must present extrinsic evidence tending to show that the destroyed e-mails would have been favorable to [its] case.

That's clear enough, eh what? Bad faith or gross negligence creates permissive presumption of relevance *and* prejudice. Bad faith is sufficient circumstantial evidence from which finder of fact *could* find prejudice. Presumption of prejudice where bad faith is shown is not uniformly followed in the

Southern District of New York. In the case of mere negligence, non-spoliator must prove both relevance and prejudice. In the case of mere negligent spoliation, evidence must be "adduced" sufficient for trier of fact to infer that evidence was of a nature (prejudicial) alleged by non-spoliator. Ordinary, negligent ESI destruction requires showing of prejudice by extrinsic evidence (extrinsic to spoliated evidence, that is) to pass hurdle for evidential sanction imposition. What the *Pension Committee* court changes is bullet number 3. Stay tuned.

Now pass the aspirin. And temper the above with the court's excerpt of Second Circuit guidance, courtesy of *Kronisch* and *Residential Funding*:

"Courts must take care not to 'hold[ ] the prejudiced party to too strict a standard of proof regarding the likely contents of the destroyed [or unavailable] evidence,' because doing so 'would ... allow parties who have ... destroyed evidence to profit from that destruction." *Id.*

Presumption Operation

The court now undertakes an analysis of how the presumption of bad faith operates in practice. In essence, the presumption is always rebuttable, the spoliating party should have the opportunity to rebut (note that spoliation has been established; we're looking at sanction severity determination here). Note that the non-spoliating party will also have the opportunity to counter any proof of "non-prejudice":

- "No matter what level of culpability is found, any presumption is rebuttable and the spoliating party should have the opportunity to demonstrate that the innocent party has not been prejudiced by the absence of the missing information."

- "If the spoliating party offers proof that there has been no prejudice, the innocent party, of course, may offer evidence to counter that proof." *Id*.

Author's Note: Spoliation proceedings are evidentiary hearings, and involve evidence, witness testimony, expert opinion and testimony, and may also include "guest" witness appearances by counsel. Other than there being no right to a jury, there is no functional difference between a spoliation hearing and a full-fledged trial. This is where the terms "outcome dispositive" and "outcome determinative" show their teeth. The court so notes:

"While requiring the innocent party to demonstrate the relevance of information that it can never review may seem unfair, the party seeking relief has some obligation to make a showing of relevance and eventually prejudice, lest litigation become a "gotcha" game rather than a full and fair opportunity to air the merits of a dispute." *Id.*

Spoliation Analysis – The New SDNY Burden Shifting Test

In order to insure that no party (to a spoliation proceeding) carries too onerous a burden of proof, the court adopts a burden shifting framework for determination of prejudice. In essence, where evidence of spoliation is egregious enough (read, gross negligence or intent-based) the court will impose a rebuttable presumption of prejudice as well as relevance, which may then be rebutted by the spoliating party, and subject, of course, to the non-spoliating party's right to counter that proof:

"To ensure that no party's task is too onerous or too lenient, I am employing the following burden shifting test: When the spoliating party's conduct is sufficiently egregious to justify a court's imposition of a presumption of relevance and prejudice, or when the spoliating party's conduct warrants permitting the jury to make such a presumption, the burden then shifts to the spoliating party to rebut that presumption. The spoliating party can do so, for example, by demonstrating that the innocent party had access to the evidence alleged to have been destroyed or that the evidence would not support the innocent party's claims or defenses. If the spoliating party demonstrates to a court's satisfaction that there could not have been any prejudice to the innocent party, then no jury instruction will be warranted, although a lesser sanction might still be required." *Id.*, at p. 6

Author's Note: One of the critical (and perhaps most often overlooked) holdings in this decision is the court's creation and imposition of a rebuttable presumption of prejudice where spoliation resulting from gross negligence has been established. Note also that while rebutting the presumption may preclude the imposition of evidential sanctions, it does not remove the possibility for imposition of lesser sanctions such as attorneys' fees and costs, or cost-shifting.

Remedies

The court turns next to a Second Circuit imposition of remedies analysis, noting that such analyses consume both judicial time and resources. In essence, the imposition of such sanctions are discretionary, but should be appropriate to deter, reward wrongdoing, and/or put the non-spoliating party into a status quo ante as if the evidence had not been spoliated (the decision does not make clear whether these considerations are to be made contemporaneously). Here again, in bullet/number format, the highlights:

"The remaining question is what remedy the court should impose.

- "The determination of an appropriate sanction for spoliation, if any, is confined to the sound discretion of the trial judge and is assessed on a case-by-case basis.

- Where the breach of a discovery obligation is the non-production of evidence, a court has broad discretion to determine the appropriate sanction.

- Appropriate sanctions should:
  1. Deter the parties from engaging in spoliation;
  2. Place the risk of an erroneous judgment on the party who wrongfully created the risk; and

3. Restore the prejudiced party to the same position [it] would have been in absent the wrongful destruction of evidence by the opposing party."

It is well accepted that a court should always impose the least harsh sanction that can provide an adequate remedy. The choices include-from least harsh to most harsh-

1. Further discovery;
2. Cost-shifting;
3. Fines;
4. Special jury instructions;
5. Preclusion; and
6. The entry of default judgment or dismissal (terminating sanctions)" *Id.*, at p. 6

Spoliation Sanctions – Terminating, Outcome Dispositive, Outcome Determinative, and Monetary
In this case, the defendants (the "Citco Defendants") requested that the court impose dismissal for spoliation they asserted was undertaken by plaintiffs. Rather, the court provides another good overview of the evidential sanctions imposition spectrum.

Terminating Sanctions Imposition - "[W]here a party has engaged in perjury, tampering with evidence, or intentionally destroying evidence by burning, shredding, or wiping out computer hard drive." *Id*.

Adverse Inferences Imposition - The court then explains that plaintiffs' behavior warranted the imposition of the evidential sanction of an adverse inference.

"Instead, the appropriate sanction here is some form of an adverse inference instruction that is intended to alleviate the harm suffered by the Citco Defendants. *Id*.

Happily enough, the court then proceeds to de-mystify the term, and explain its various types:

"Like many other sanctions, an adverse inference instruction can take many forms, again ranging in degrees of harshness. The harshness of the instruction should be determined based on the nature of the spoliating party's conduct-the more egregious the conduct, the more harsh the instruction." *Id.*

Evidential sanction flavors, excerpted from page 7 of the opinion, in bullets:

- Spoliation Charge - The least harsh instruction permits (but does not require) a jury to presume that the lost evidence is both relevant and favorable to the innocent party.

  a) If it makes this presumption, the spoliating party's rebuttal evidence must then be considered by the jury, which must then decide whether to draw an adverse inference against the spoliating party.

  b) This sanction still benefits the innocent party in that it allows the jury to consider both the misconduct of the spoliating party as well as proof of prejudice to the innocent party.

c) Such a charge should be termed a "spoliation charge…"

- Spoliation Presumption (rebuttable)
  a) …[A] charge where the a jury is directed to presume, albeit still subject to rebuttal, that the missing evidence would have been favorable to the innocent party,

- Direction to Deem Admitted –…[A] charge where the jury is directed to deem certain facts admitted.

Author's Note: Spoliation charges permit the jury to presume (rather than infer?). Directed to presume rather than "permitted" to presume? While the technical distinctions between "directed," "permitted," "inference" and "presumption" may be, er, clear, one can only wonder whether such fine distinctions are lost on a jury during its deliberations, particularly where the "directed" flavor is still rebuttable. Perhaps this is why these sanctions are called "outcome determinative" --- even where both are rebuttable, it may ultimately make no difference whether posed as a presumption or inference.

Author's Note: The court did not find evidence of misconduct sufficient to impose terminating sanctions but did find sufficient intentionality to impose an adverse inference. Note also that adverse inferences come in many flavors. Note also that this decision is the first to state unequivocally, albeit in dicta, that the wiping of a computer hard drive is sufficient bad faith (either by intentional or grossly negligent conduct) to impose terminating sanctions, at least in the Southern District of New York.

The court reminds us that monetary sanction may be appropriately imposed together with evidential sanctions:

"Monetary sanctions are also appropriate in this case. "Monetary sanctions are appropriate 'to punish the offending party for its actions [and] to deter the litigant's conduct, sending the message that egregious conduct will not be tolerated.'" Awarding monetary sanctions "serves the remedial purpose of compensating [the movant] for the reasonable costs it incurred in bringing [a motion for sanctions]." This sanction is imposed in order to compensate the Citco Defendants for reviewing the declarations, conducting the additional depositions, and bringing this motion." *Id.* at p. 7

<u>Articulated Gross Negligence Standard for Discovery Duties</u>

In another first, the court explains that failure to adhere with contemporary standards in complying with one's discovery obligations constitutes gross negligence (and, in accordance with this decision, the imposition of a rebuttable presumption of lost ESI prejudicial value). These include (bullet list first, followed by excerpt):

<u>Duty to Preserve Failure Triggers</u>

- Issuance of written litigation hold

- Identify all key players (to ensure relevant records are preserved)
- Cease deletion of email (in party's possession, custody, or control)
- Preserve records of former employees (in party's possession, custody, or control)

"After a discovery duty is well established, the failure to adhere to contemporary standards can be considered gross negligence. Thus, after the final relevant Zubulake opinion in July, 2004, the following failures support a finding of gross negligence, when the duty to preserve has attached: to issue a written litigation hold; to identify all of the key players and to ensure that their electronic and paper records are preserved; to cease the deletion of email or to preserve the records of former employees that are in a party's possession, custody, or control; and to preserve backup tapes when they are the sole source of relevant information or when they relate to key players, if the relevant information maintained by those players is not obtainable from readily accessible sources." *Id.*

Sanctions Applied

Counsel Litigation Hold Letter Instructions Inadequate

- Inadequate Preservation Instructions: Failure to adequately instruct about preservation of ESI and paper records
- Failure to Create Collection Mechanism – for review by non-employee, total reliance on employee to collect does not meet "contemporary standard"
- Duty to Preserve – includes ESI

Plaintiffs failed, and quite spectacularly, to comply with their discovery obligations, and the court took them to task for their failures. EDDE leaves the facts behind each of the individuals and entities responsible to the reader. Suffice it to say that plaintiffs' actions were sufficiently egregious for the court to hold thus:

"While litigants are not required to execute document productions with absolute precision, at a minimum they must act diligently and search thoroughly at the time they reasonably anticipate litigation. All of the plaintiffs in this motion failed to do so and have been sanctioned accordingly." *Id.* at p. 24

Additional Limited Discovery - Backup Tapes Ordered Restored and Searched

It was demonstrated to the court that plaintiffs failed to conduct adequate ESI search as well, and in recognizing this, the court permitted additional limited discovery:

"I have also considered whether the Citco Defendants should be entitled to additional discovery. If a lesser sanction is appropriate that is always a better course. With regard to Coronation and Okabena, plaintiffs admit that backup tapes exist and have not been searched. They do not explain why such a search cannot still be conducted. The goal of discovery is to obtain evidence, not to issue sanctions.

Thus, Coronation and Okabena are ordered to search their backup tapes for the relevant period at their expense, or demonstrate why such backup tapes cannot be searched, within thirty days." *Id.*

Attorneys' Fees and Costs

"In addition, all plaintiffs are subject to monetary sanctions. The Citco Defendants are entitled to an award of reasonable costs, including attorneys' fees, associated with reviewing the declarations submitted, deposing these declarants and their substitutes where applicable, and bringing this motion. The Citco Defendants shall submit a reasonable fee application to this Court for approval. Once approved, the costs are to be allocated among these plaintiffs." *Id*.

Jury Instruction

Practice Tip: For those engaged in spoliation proceedings, the following excerpt provides excellent verbiage for crafting a jury instruction:

"The Citco Defendants have demonstrated that most plaintiffs conducted discovery in an ignorant and indifferent fashion. With respect to the grossly negligent plaintiffs-2M, Hunnicutt, Coronation, the Chagnon Plaintiffs, Bombardier Trusts, and the Bombardier Foundation-I will give the following jury charge:

The Citco Defendants have argued that 2M, Hunnicutt, Coronation, the Chagnon Plaintiffs, Bombardier Trusts, and the Bombardier Foundation destroyed relevant evidence, or failed to prevent the destruction of relevant evidence. This is known as the "spoliation of evidence."

Spoliation is the destruction of evidence or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation. To demonstrate that spoliation occurred, the Citco Defendants bear the burden of proving the following two elements by a preponderance of the evidence:

First, that relevant evidence was destroyed after the duty to preserve arose. Evidence is relevant if it would have clarified a fact at issue in the trial and otherwise would naturally have been introduced into evidence; and

Second, that if relevant evidence was destroyed after the duty to preserve arose, the evidence lost would have been favorable to the Citco Defendants.

I instruct you, as a matter of law, that each of these plaintiffs failed to preserve evidence after its duty to preserve arose. This failure resulted from their gross negligence in performing their discovery obligations. As a result, you may presume, if you so choose, that such lost evidence was relevant, and that it would have been favorable to the Citco Defendants. In deciding whether to adopt this presumption, you may take into account the egregiousness of the plaintiffs' conduct in failing to preserve the evidence.

However, each of these plaintiffs has offered evidence that (1) no evidence was lost; (2) if evidence was lost, it was not relevant; and (3) if evidence was lost and it was relevant, it would not have been favorable to the Citco Defendants.

If you decline to presume that the lost evidence was relevant or would have been favorable to the Citco Defendants, then your consideration of the lost evidence is at an end, and you will not draw any inference arising from the lost evidence.

However, if you decide to presume that the lost evidence was relevant and would have been favorable to the Citco Defendants, you must next decide whether any of the following plaintiffs have rebutted that presumption: 2M, Hunnicutt, Coronation, the Chagnon Plaintiffs, Bombardier Trusts, or the Bombardier Foundation. If you determine that a plaintiff has rebutted the presumption that the lost evidence was either relevant or favorable to the Citco Defendants, you will not draw any inference arising from the lost evidence against that plaintiff. If, on the other hand, you determine that a plaintiff has not rebutted the presumption that the lost evidence was both relevant and favorable to the Citco Defendants, you may draw an inference against that plaintiff and in favor of the Citco Defendants-namely that the lost evidence would have been favorable to the Citco Defendants.

Each plaintiff is entitled to your separate consideration. The question as to whether the Citco Defendants have proven spoliation is personal to each plaintiff and must be decided by you as to each plaintiff individually.

In addition, all plaintiffs are subject to monetary sanctions. The Citco Defendants are entitled to an award of reasonable costs, including attorneys' fees, associated with reviewing the declarations submitted, deposing these declarants and their substitutes where applicable, and bringing this motion. The Citco Defendants shall submit a reasonable fee application to this Court for approval. Once approved, the costs are to be allocated among these plaintiffs." *Id.,* at pp. 23-24.

Steven W. Teppler is a Partner at Edelson McGuire LLC, a high-tech litigation boutique with offices in Chicago, New York City, and Los Angeles, and directs the firm's electronic litigation and digital evidence consultation practice. Steven has practiced law since 1980, is admitted to the bars of New York, the District of Columbia and Florida, and advises private and public sector clients about risk, liability, and compliance issues unique to electronic data generation, alteration, transmission and archiving. He also lectures nationwide on evolving theories of computer generated information and evolving theories of liability, practice and evidence in an electronic data universe. Steven holds six patents in the field of content authentication, and is the founder and CEO of a content authentication provider. Steven is the Co-Chair of the E-Discovery and Digital Evidence Committee of the American Bar Association, a founding member of the Information Assurance Consortium, and a co-author of the ANSI X9F4 trusted timestamp guideline standards for the financial industry.