2010 EASTERN CLAIMS CONFERENCE

February 28 – March 2, 2010

Dr. StrangeRule, Or How I Learned To Stop Worrying And Love E-Discovery

Elizabeth G. Doolin, Esq.
Joseph R. Jeffery, Esq.
Chittenden, Murday & Novotny, LLC
303 W. Madison Street, Suite 1400
Chicago, Illinois 60606
(312) 281-3600
edoolin@cmn-law.com
jjeffery@cmn-law.com

TABLE OF CONTENTS

"YOU'RE GONNA NEED A BIGGER BOAT."

I. Why Worry About E-Discovery?

There are plenty of reasons to worry about e-discovery. To begin with, most companies generate **a lot** of electronically stored information ("ESI"). One CD holds the equivalent of 35,000 pages or 15 boxes of documents.[1] The desktop or laptop hard drive for one employee can hold 1.5 million pages or 600 boxes of documents.[2] One company server can hold 100 million pages or 43 semi-truck loads of documents.[3] Even a mid-sized company typically has 1.625 *billion* pages of documents; enough to reach from the Earth to the Moon.[4] Another challenge is locating all of the ESI relevant to a lawsuit or other dispute. There are so many types of media on which ESI can be stored that it would be easy to overlook some of it. Obvious sources of information include documents contained in file cabinets and e-mails in computer servers.[5] Other less obvious sources include "thumb drives and PDAs used by employees."[6] Information may also be in the possession or control of third parties, such as "outsourced service providers, storage facilities operators, and Application Service Providers."[7]

Once located, the databases on which ESI resides must be searched for relevant information. Computer software can help with this but, as this paper explains, it is no silver bullet as the search results are usually over- or under-inclusive, adding time and expense to the privilege and relevance review of the documents identified by the software search.

Another concern is production. Documents often contain hidden information in the form of "metadata," some of which can be privileged or at least embarrassing to its authors if disclosed. Consider what happened when documents containing "metadata" were produced and/or made public. Metadata in a 2004 complaint against DaimlerChrysler not only disclosed attorney work product concerning jurisdiction and venue issues,[8] it also showed that the plaintiff originally trained its sights on a completely different defendant – Bank of America – thereby undermining the moral force of its complaints against DaimlerChrysler.[9] More embarrassing was the disclosure in a United Nations report on Syria's ties to the assassination of a former Lebanese Prime Minister. Prior to the release of the U.N.'s report on Syrian involvement in the assassination of former Lebanese Prime Minister Rafik Hariri, U.N. Secretary General Kofi Annan promised not alter the report before giving it to the U.N. Security Council.[10] The electronic version of the report, however, showed that he did just that, scrubbing the names of four members of the Syrian president's inner circle and replacing them with the euphemistic "Senior Lebanese and Syrian officials."[11]

Compounding these challenges are the consequences of failing, in the context of a lawsuit, to properly preserve, search for, retrieve, review, and produce relevant information. A party that fails in one or more of those tasks risks having sanctions imposed against it. The sanctions available can be harsh, ranging from fines and having to pay the costs of an opponents' discovery to judgment or dismissal in favor of an opposing party.

So, why should companies, their employees, and lawyers stop worrying? They probably shouldn't stop completely, but they can at least lighten up a bit. The past couple of years have seen Congress, courts, and commentators set standards of conduct for e-discovery, bringing

needed clarity to this intersection of technology and the law. Congress, for instance, revised the Federal Rules of Civil Procedure and the Federal Rules of Evidence to address concerns created by the increasing significance of e-discovery in litigation. As courts have had to address more e-discovery disputes, standards of conduct related to e-discovery have begun to emerge providing needed guidance to the parties and their attorneys. Commentators, too, have helped conceive of new approaches to the mechanics of dealing with e-discovery.

This paper first discusses the ground rules for e-discovery as established by the Federal Rules of Civil Procedure and Federal Rules of Evidence to provide a baseline understanding of the federal e-discovery framework. Next, the paper discusses the importance of the litigation hold and case law that both illustrates the dangers of spoliation and provides guidance for managing e-discovery going forward. Finally, the paper offers practical advice concerning a company's management of e-discovery and the integration of e-discovery obligations with a document retention program.

II. Ground Rules: The Federal Rules Of Civil Procedure And The Federal Rules Of Evidence Address E-Discovery Concerns.

The Federal Rules of Civil Procedure were revised in 2006 and 2007 to establish a framework for managing the discovery of ESI. In 2008, Rule 502 of the Federal Rules of Evidence was added to alleviate some of the privilege issues that arise in connection with the production and review of electronically stored information.

"YOU WANT THE IMPOSSIBLE!"

A. Addressing E-Discovery Issues Early On

1. Rule 26(a)(1)(A)(ii): Initial Disclosures

Rule 26(a)(1) governs parties' initial disclosures of relevant information. Under Rule 26(a)(1)(A)(ii), a litigant must provide "a copy—or a description by category and location—of all documents**, electronically stored information** and tangible things that the disclosing party has in its possession, custody or control and may use to support its claims or defenses, unless the use would be solely for impeachment."[12] "The term 'electronically stored information' has the same broad meaning … as in Rule 34(a)."[13]

2. Rule 26(f)(2): E-Discovery At The Initial Attorneys' Conference

Rule 26(f)(2) requires parties to "discuss any issues relating to preserving discoverable information" at their initial conference.[14] Specifically, the Rule requires the parties to "develop a proposed discovery plan"[15] that states "the parties' views and proposals on ... any issues about disclosure or discovery of electronically stored information, including the form or forms in which it should be produced … [and] any issues about claims of privilege or of protection as trial-preparation materials, including—if the parties agree on a procedure to assert such claims after production—whether to ask the court to include their agreement in an order …."[16] To encourage thoughtful consideration of issues and development of a discovery plan, the Advisory Committee "discourage[d] courts from entering blanket preservation orders and suggest[ed] that any preservation order be narrowly tailored."[17]

3. Rule 16(b)(3)(B): Discussing E-Discovery At The Outset Of Litigation

Scheduling orders typically follow the initial conference discussed immediately above. Rule 16(b)(3)(B) accounts for the party agreements Rule 26(f)(2) was intended to promote by confirming that a "scheduling order may … provide for disclosure or discovery of electronically stored information … [and may] include any agreements the parties reach for asserting claims of privilege or of protection as trial-preparation material after information is produced …."[18]

"I'LL BE TAKING THESE HUGGIES AND WHATEVER CASH YOU GOT."

B. Discovery Requests

1. Rule 33(d): Interrogatories And The Production Of ESI

Rule 33 has long permitted parties to produce records containing information sought in an interrogatory in lieu of supplying a written answer. Rule 33(d) specifically extends that practice to ESI. The Rule provides in pertinent part: "[i]f the answer to an interrogatory may be determined by examining, auditing, compiling, abstracting, or summarizing a party's business records (**including electronically stored information**), and if the burden of deriving or ascertaining the answer will be substantially the same for either party, the responding party may answer by … specifying the records that must be reviewed …."[19] Thus, a party has the option of specifying ESI in response to a written interrogatory.

2. Rule 34: Document Requests And The Production Of ESI

Similarly, Rule 34(a)(1)(A) provides a party may request "any designated documents or **electronically stored information** – including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations – stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form …."[20] Rule 34(a)(1) also allows parties to "inspect, copy, test or sample" the documents, ESI, and tangible things covered by that Rule.[21]

Notably Rule 34(b)(1)(C) allows the requesting party to "specify the form or forms in which electronically stored information is to be produced."[22] "The response may state an objection to a requested form for producing electronically stored information. If the responding party objects to a requested form—or if no form was specified in the request—the party must state the form or forms it intends to use."[23] Also, "[i]f a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms …."[24]

3. Rule 45: Subpoenas For ESI

Rule 45(a)(1)(C), like Rule 34 provides that ESI may be subpoenaed from third parties. "A command to produce documents, **electronically stored information**, or tangible things or to permit the inspection of premises may be included in a subpoena commanding attendance at a deposition, hearing, or trial, or may be set out in a separate subpoena. A subpoena may specify the form or forms in which electronically stored information is to be produced."[25] Also, Rule 45(a)(1)(D) provides, "[a] command in a subpoena to produce documents, electronically stored information, or tangible things requires the responding party to permit inspection, copying, testing, or sampling of the materials."[26]

"COME OUT, COME OUT WHEREVER YOU ARE!"

C. Discovery Collection & Production

1. Rule 26(b)(2)(B)–(C): Accessibility Of Data

Under Rule 26(b)(2)(B), "[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost."[27] Discovery of inaccessible ESI may be had, however, where good cause is shown.

> On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.[28]

Rule 26(b)(2)(C)(iii) provides that discovery meets the "undue burden or cost" standard and must be limited when "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues"[29]

2. Rule 26(c): Cost-Shifting

A court can under Rule 26(c)(1), issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense ...."[30] Retrieving and producing ESI has obvious cost implications for the producing party. While the presumption "is that the responding party must bear the expense of complying with discovery requests" a party can seek an order protecting it from undue burden or expense (as described above) "conditioning [it] on the requesting party's payment of the costs of [the] discovery."[31]

The United States District Court for the Southern District of New York in *Rowe Entertainment, Inc. v. The William Morris Agency*[32] noted "courts have adopted a balancing approach," and apply the following test to requests to shift the costs of discovery.

> (1) the specificity of the discovery requests; (2) the likelihood of discovering critical information; (3) the availability of such information from other sources; (4) the purposes for which the responding party maintains the requested data[;] (5) the relative benefit to the parties of obtaining the information; (6) the total cost associated with production; (7) the relative ability of each party to control costs and its incentive to do so; and (8) the resources available to each party.[33]

In the watershed *Zubulake v. UBS Warburg LLC*[34] case, the court drew a distinction

between the relative accessibility and/or inaccessibility of information sought in discovery. It concluded courts should consider shifting the costs of production to requesting parties when the requested information is "inaccessible" and it used the term to describe information that must be restored or reconstructed before it can be used or reviewed.[35] Once a court determines that the information sought is inaccessible, it must, for cost-shifting purposes weigh the following seven factors to determine whether it is appropriate to shift the costs of producing the requested information to the requesting party:

a. The extent to which the request is specifically tailored to discover relevant information;
b. The availability of such information from other sources;
c. The total cost of production, compared to the amount in controversy;
d. The total cost of production, compared to the resources available to each party;
e. The relative ability of each party to control costs and its incentive to do so;
f. The importance of the issues at stake in the litigation; and
g. The relative benefits to the parties of obtaining the information.[36]

3. Rule 37(e): A "Safe Harbor" For Routine Destruction.

A common question for companies is how to manage all of the documents and data that their employees create and receive on a daily basis. Acutely aware of the sanctions that can accompany the destruction of relevant evidence, some companies have adopted a "keep everything" approach to their documents and ESI. Others have adopted the same policy by default; *i.e.*, they do not have a policy for destroying documents that no longer serve a business purpose. A major problem with this approach is that the costs of storing so many documents and ESI can be enormous. The practice can also affect litigation costs. If a company saves literally everything, it can be asked to search every possible source for documents or information relevant to any pending litigation or "reasonably calculated to lead to the discovery of admissible evidence."[37] For these reasons, companies need document retention policies that allow them to destroy paper documents and ESI that no longer serve the company's business needs. Rule 37 of the Federal Rules of Civil Procedure seeks to balance those needs against litigants' duties to preserve relevant information.

Rule 37(e) provides: "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."[38] "Good faith is generally understood to be the absence of bad faith, so if a spoliating party can show that its actions were not in bad faith, it will have met the state of mind standard required by Rule 37(e)."[39] This rule has been described as providing a "safe harbor" for litigants, who destroy documents in the routine course of electronic data management.[40] But a document retention program that is the product of evolution of informal company practices rather than intentional

design that addresses legitimate business needs is likely not a "good-faith" electronic information system.[41] Consequently, parties who destroy relevant documents pursuant to such a "system" may not be entitled to Rule 37's safe harbor.

"SIR, YOU CAN'T LET HIM IN HERE. HE'LL SEE EVERYTHING. HE'LL SEE THE BIG BOARD!"

D. Addressing Privilege Concerns

One major component of the cost of e-discovery is the review a party must undertake before production to ensure it is not disclosing privileged documents or information. The Federal Rules seek to limit those costs by endorsing what are commonly known as "claw-back" and "quick peek" arrangements. In theory, a producing party can skip the privilege review (and its attendant costs) and produce documents to an opposing party without waiving the privilege associated with any of the documents produced.

1. Rule 26(b)(5)(B): The Claw-Back and Quick Peek Provisions

"Claw-back" and "Quick-peek" agreements are similar. Rule 26(b)(5)(B) describes what is typically referred to as the 'claw-back' agreement:

> [i]f information produced in discovery is subject to a claim of privilege or of protection as trial-preparation material, the party making the claim may notify any party that received the information of the claim and the basis for it. After being notified, a party must promptly return, sequester, or destroy the specified information and any copies it has; must not use or disclose the information until the claim is resolved; must take reasonable steps to retrieve the information if the party disclosed it before being notified; and may promptly present the information to the court under seal for a determination of the claim. The producing party must preserve the information until the claim is resolved.[42]

In a "quick peek" agreement, parties "agree that the responding party will provide certain requested materials for initial examination without waiving any privilege or protection," thus, the quick peek.[43] Claw back and quick peek agreements did not gain much traction as parties were concerned that the non-waiver agreements would not apply as to third parties in the same or later litigation.[44] In response to that concern, Congress enacted Federal Rule of Evidence 502.

2. Federal Rule of Evidence 502

Rule 502 of the Federal Rules of Evidence[45] makes orders directing that a privilege has not been waived binding on non-parties as well as other federal and state courts. The operative sections of Rule 502 are summarized below.

a. Subject-Matter Waiver.

Federal Rule of Evidence 502(a) provides that the disclosure and resulting waiver of an attorney-client privilege or work-product protection will only result in a waiver of all such privileges and protections concerning the same subject matter in certain circumstances. Thus, "[i]n effect, an inadvertent disclosure, even if it constitutes a waiver, will act as a waiver only as to the materials disclosed, not to other materials regarding the same subject matter."[46]

b. Requirements For Avoiding Waiver Of Privilege In Context Of Inadvertent Disclosure.

Rule 502(b) limits the potential effect of an inadvertent disclosure of privileged or work-product material on a claim of privilege.

> (b) Inadvertent disclosure.- - When made in a Federal proceeding or to a Federal office or agency, the disclosure does not operate as a waiver in a Federal or State proceeding if: (1) the disclosure is inadvertent; (2) the holder of the privilege or protection took reasonable steps to prevent disclosure; and (3) the holder promptly took reasonable steps to rectify the error, including (if applicable) following Federal Rule of Civil Procedure 26(b)(5)(B).[47]

Rule 502(e) also tries to clear the way for claw-back and quick-peek agreements by making them binding on other parties and courts when made part of a court order. "An agreement on the effect of disclosure in a Federal proceeding is binding only on the parties to the agreement, *unless it is incorporated into a court order*."[48] Thus, to enjoy the benefits of Rule 502, parties who enter into non-waiver agreements should ask the court to memorialize their agreement in a Rule 16(b) scheduling order.

Before Rule 502 was enacted, federal courts generally protected parties from waiving a privilege due to an inadvertent disclosure "unless the disclosing party was negligent in producing the information or failed to take reasonable steps seeking its return."[49] Some courts, however, held that any inadvertent disclosure of privileged material constituted a waiver of the privilege.[50] Others required that the disclosure be intentional in order to result in a waiver.[51] As stated in the Explanatory Note, Rule 502(b) "opts for the middle ground: inadvertent disclosure of protected communications or information in connection with a federal proceeding or to a federal office or agency does not constitute a waiver if the holder took reasonable steps to prevent disclosure and also promptly took reasonable steps to rectify the error. This position is in accord with the majority view on whether inadvertent disclosure is a waiver."[52]

c. Reasonable Steps To Prevent Inadvertent Disclosure

Not all inadvertent disclosures of material will be exempt from a waiver of privilege. Satisfying the court that a party has taken reasonable steps both to avoid the disclosure and to correct the mistake is crucial. Rule 502(b) does not define what the "reasonable steps" are, but

"[b]ecause the reasonableness test adopted in Rule 502 is taken from the majority rule developed over many years, many courts have already addressed whether a party took reasonable steps to avoid inadvertent waivers."[53] The Advisory Committee Notes provide only a limited list of reasonableness factors, such as "'the number of documents to be reviewed and the time constraints for production,'" using "'software applications and linguistic tools in screening for privilege,'" and "'an efficient system of records management.'"[54]

In any event, some common-sense approaches during the search for and production of documents will help to avoid the inadvertent production of privileged materials in the first place. An obvious step is to carefully review *all* documents and materials before producing them. In one case, for example, a party produced a privileged document from a database it thought contained only non-privileged materials. Despite an applicable "claw-back" provision, the court held the party waived the privilege because it did not review the database for privilege before producing the material.[55] The most cautious (and perhaps most costly) approach is to make sure attorneys review all materials for privilege. "Even relatively tolerant courts have demonstrated their disapproval of nonlawyers handling privileged documents."[56] One commentator asserted, "there must be a final review of documents before they are produced to opposing counsel … consist[ing] of a face check of each document to make sure that counsel is not producing privileged material."[57] In addition, the review process should require that "all privileged documents [including electronically produced documents] be clearly labeled and adequately separated from nonprivileged responsive documents."[58] The type and reliability of the search conducted are other important factors. For instance, parties must pay close attention to the effectiveness of their keyword searches for privileged material.[59] *See Section III., E. below.*

An additional factor to consider is the time within which a party seeks to rectify its error after discovering it. One court agreed the privilege was not waived where attorneys took steps to correct the inadvertent disclosure "immediately" after realizing the disclosure.[60] Another court found that the plaintiff's delay in reacting after learning of the inadvertent disclosure, including taking two weeks to determine how the disclosure occurred, was not reasonable.[61]

The parties may define for themselves at their Rule 26(f) conference what conduct constitutes "reasonable steps."[62] For example, the parties could agree to specific time periods within which they could seek to recover inadvertently disclosed materials. In addition to removing as much ambiguity as possible, defining "reasonableness" for these purposes would provide a "checklist" of steps that counsel could circulate to the individuals involved in the search for and production of materials, helping ensure the parties do not inadvertently waive their privileges by acting "unreasonably."

d. Federalism and Rule 502

The orders entered under Rule 502 bind non-parties and other courts, including state courts. Section (d) of the rule provides that "[a] Federal court may order that the privilege or protection is not waived by disclosure connected with the litigation pending before the court—in which event the disclosure is also not a waiver in any other Federal or State proceeding."[63] This has been described as "the 'most critical piece' of the legislation," because the contemplated

court orders "bind[] all other courts, as well as nonparties."[64] Some commentators have noted, however, that Rule 502's attempt to bind state courts is ripe for a constitutional challenge.

> There may be serious constitutional questions as to the ability of Congress to enact such a law merely by asserting that the interest in the federal objective of limiting the costs of production requires such a rule. In *Erie Railroad Co. v. Tompkins*, Justice Brandeis wrote, 'Congress has no power to declare substantive rules of common law applicable in a state .... And no clause in the Constitution purports to confer such a power upon the federal courts.' ... To the extent that Rule 502 may overrule the *Erie* doctrine by encroaching on substantive privilege law that has traditionally been left to the states, the rule as drafted poses difficult constitutional questions ....[65]

Further, "[t]he legitimacy of a rule that would bind states or federal agencies in subsequent litigation may ultimately depend on Congress's power under the Commerce Clause."[66] A full examination of these issues is well beyond the scope of this paper. We simply note them to illustrate that even with the enactment of Rule 502, parties should not become complacent and assume that inadvertent disclosures of privileged materials will not adversely affect them in subsequent litigation.

"WHAT JEFFERSON WAS SAYING WAS, HEY! YOU KNOW, WE LEFT THIS ENGLAND PLACE 'CAUSE IT WAS BOGUS; SO IF WE DON'T GET SOME COOL RULES OURSELVES – PRONTO – WE'LL JUST BE BOGUS TOO."

E. State Laws Addressing E-Discovery Concerns

States have begun to address e-discovery as well. This paper focuses on federal e-discovery rules and case law largely because state law has not developed as quickly as federal law. In October 2007, the National Conference of Commissioners on Uniform State Laws issued its draft of uniform rules relating to the discovery of ESI.[67] Rather than "reinvent the wheel," the Committee's proposal "mirrors the spirit and direction of the ... Federal Rules of Civil Procedure," and "freely adopted, often verbatim, language from both the Federal Rules and comments it deemed valuable." Thus, federal law provides the clearest guidance on what the present state of the law is or should be concerning e-discovery. Indeed, federal law is strongly influencing the development of state law in this area as thirty-two states have now enacted e-discovery rules, many of which are patterned after the e-discovery provisions in the Federal Rules of Civil Procedure.[68]

"ALL RIGHT, MR. DEMILLE, I'M READY FOR MY CLOSE UP."

III. Courts And Commentators Take A Closer Look At E-Discovery Issues

"HOLD ... HOLD ... HOLD!"

A. Establishing a Litigation or Legal Hold.

Virtually all e-discovery risk is concentrated in the litigation-hold process.[69] Identifying the individuals with knowledge of the dispute, conducting reasonable searches of a party's ESI and paper documents to identify materials that must be preserved, and communicating the hold requirements to others in an organization are critical to ensuring a party is protected against liability or even sanctions for spoliation. As discussed below, the failure to sufficiently create, apply, and enforce a litigation hold can lead to claims of spoliation of evidence and severe sanctions.

"HOUSTON, WE HAVE A PROBLEM."

1. What Triggers the Need for a Litigation Hold?

The litigation hold is triggered by a party's duty to preserve relevant evidence once "litigation is reasonably anticipated, threatened or pending against" a party. The evidence that a party is required to preserve includes information that is: (i) relevant to the action/anticipated action; (ii) reasonably calculated to lead to the discovery of admissible evidence; and (iii) reasonably likely to be requested during discovery. As part of the duty to preserve, a party must "suspend, as to documents that may be relevant to anticipated litigation, any routine document purging system that might be in effect."[70] The failure to suspend destruction of that evidence constitutes spoliation.[71] This, of course, means "routine email and e-document destruction is required to cease,"[72] and, generally, that "relevant ... databases, spreadsheets, hard drive data, and data on a server, including all metadata" must be preserved.[73]

Precisely when the duty to preserve is triggered is not always obvious. Generally, "[t]he duty to preserve commences when litigation is likely or probable, not when litigation is merely possible."[74] One clear trigger of the duty to preserve is the "receipt of a demand letter."[75] Informal complaints, especially in employment cases, can also trigger the duty to preserve evidence, but the "receipt of a letter merely addressing a dispute without threatening litigation may not" signal that litigation is sufficiently likely to trigger the duty to preserve.[76]

Other factors, like the type of threat or complaint made, the position of the party making the threat or complaint, the parties' business relationship, the specificity of the threat or complaint, and whether the other party has a litigious reputation all bear on whether the duty to preserve has arisen.[77] Some courts "have found a duty to preserve if 'lawsuits or complaints have been filed frequently concerning the type of records at issue' and questioned the reasonableness of applying routine destruction policies to those records, even in the absence of a specific litigation threat."[78] In one case, the court found a defendant's duty to preserve

information concerning the development of software was triggered five years before suit was filed based on the existence of litigation in the defendant's industry concerning the same or similar issues.[79] As with any test that depends on "reasonableness," determining whether the duty to preserve has been triggered is a judgment call. Companies, therefore, must be vigilant in monitoring their business transactions for any potential indicators of anticipated litigation.

"ROUND UP THE USUAL SUSPECTS."

2. Identify and Interview Key Players in the Dispute

Oftentimes, the best place to start looking for information is with the "key players" in the dispute; *i.e.*, those persons likely to have information the party will rely on to support its claims or defenses.[80] Depending on the nature of the case, the "key players" could include, for example, claims examiners, underwriting department employees, various department managers and IT employees. One commentator has suggested five "areas of responsibility; the Internal Corporate Counsel, the legal department Paralegal or Litigation Specialist, the IT department[,] … the employee [and] … depending on your company culture … the employee's manager."[81] concerning electronically stored information, in particular, a litigation hold notice should be communicated to data users, records management personnel, IT personnel, and other potentially knowledgeable personnel, as well as those identified as document custodians.[82]

Counsel should interview the key players to identify: (i) an information timeline for the dispute; (ii) what type of relevant information is likely to exist; (iii) where the person stored the information she created and/or received; (iv) what her information and data storage habits are, *e.g.*, whether she stores information on the company's servers, a laptop, thumb drive, home computer, PDA, or one or more of the foregoing; (v) what other types of relevant information might exist concerning the dispute; (vi) who else might be a key player; and (vii) what types of information those individuals might have.[83]

"YOU ARE NOW INSIDE WHAT I LIKE TO CALL 'THE BYRNES FAMILY CIRCLE OF TRUST.' I KEEP NOTHING FROM YOU, YOU KEEP NOTHING FROM ME."

3. Communicate The Litigation Hold To The Circle Of Employees And Third Parties Likely To Posses ESI

In order to be most effective, the litigation hold notice should be written, "conspicuously labeled and dated," and clearly describe its purpose, as well as the lawsuit or investigation involved.[84] The notice (and later notices and reminders) should be given to each person or entity believed to have documents and ESI that the company is required to preserve. The notice must further "inform recipients of their legal obligations, including the potential penalties for noncompliance."[85] The notices and reminders should provide guidelines for the types of materials to preserve and "describe the actual steps that a recipient must take to verify preservation of materials.[86] Further, they should provide the name and contact information of the person "overseeing the litigation or investigation" and request that the recipients inform the contact person of other individuals who might have relevant materials.[87] "Companies should

resist the temptation to craft a 'form' letter to be used in all circumstances with a mere modification of the subject line. The letters must be read and understood not only by employees but perhaps adversaries and the court when the matter evolves into litigation. … The litigation hold letter itself, while arguably a privileged document, may itself be discoverable."[88]

Counsel must do more than "instruct a client to preserve email and other relevant evidence once litigation is reasonably anticipated."[89] One commentator has noted that "[s]ome corporate legal departments treat a litigation hold as a one-time communication (usually an email) to employees, requesting that all information relating to specific content be held and protected for possible production in an anticipated or pending legal case. Many companies wrongly believe an email message to the employee base removes responsibility from the company."[90] With an eye toward being able to prove the litigation hold was properly distributed, a hard copy should be delivered to the recipients.[91] If, however, "email is used to disseminate the litigation-hold notice, then counsel must ensure that all of the intended recipients … have email accounts," and "[r]ecipients of hold notices via email should be advised to file the notice so that it is protected from automatic deletion in their inbox."[92] Requiring each email recipient to send a response email acknowledging receipt of the notice and his duty to preserve the relevant information is an easy way to ensure proper distribution of the litigation hold.

Counsel must also keep track of the receipt and implementation of the litigation hold.[93] One court, for example, "found fault with counsel's failure to 'request retained information from one key employee' and 'safeguard backup tapes that might have contained some of the deleted emails, and which would have mitigated the damage done by [the client's] destruction of those emails.'"[94] That court also found the attorney's "duty extended to supplemental responses under" Rule 26, noting that counsel "'must periodically recheck all interrogatories and canvass all new information.'"[95]

Finally, a litigation hold should clearly communicate how the relevant ESI should be preserved. An understanding of how electronic information is stored and preserved is crucial because miscommunications between counsel, "key players," and IT personnel can result in additional search and retrieval costs. As one commentator has noted, "[c]ounsel must fully understand what is requested and question how the IT personnel will go about meeting that request."[96] The following examples show the importance of such an understanding.

> Suppose counsel requests a 'mirror image backup' of an employee's hard drive. Counsel's intention is to have an exact copy (a mirror image) of the hard drive made in order to ensure the integrity of the data – but that intention is never communicated to the IT personnel who is working on the project. Instead of making a mirror image copy of the hard drive, the IT personnel preserve the data by placing it on backup tape media. When the technicians heard 'backup,' they assumed the attorney meant a backup tape. Since backup tapes can be difficult to read, the actions of the IT personnel will inevitably increase the costs of extracting and producing the responsive dat[a] and could lead to claims that counsel was trying to hide evidence on inaccessible media.[97]

Similarly,

> suppose that counsel notifies the IT department to preserve the company's emails and other electronic data for a legal matter. The IT department, having received no input from counsel, copies the native files to an external hard disk drive (thus changing the metadata), places the company's emails and databases on backup tapes (making the data inaccessible) and fails to segregate and protect the original data. As a result of this miscommunication and lack of understanding, the preserved data resides on separate media formats, increasing the search and retrieval costs, and the original data is still exposed to change or deletion.[98]

"OVER? DID YOU SAY 'OVER?' NOTHING IS OVER UNTIL WE DECIDE IT IS! WAS IT OVER WHEN THE GERMANS BOMBED PEARL HARBOR?"

4. Terminating A Litigation Hold Notice.

Best practices require that "litigation-hold notices should remain in effect until a matter is ultimately concluded."[99] Accordingly, a "Release of Hold" notice is appropriate when "a final settlement agreement and release" has been executed, the court enters an order dismissing the case with prejudice, or when all appeals have been exhausted and the judgment is final.[100] Heeding a termination notice is as important as complying with a litigation hold notice because the unnecessary retention of documents and electronically stored information can create additional costs and waste resources.[101]

"ONE MILLION DOLLARS!"

B. Sanctions Due To Spoliation Of Evidence.

An incomplete litigation hold or an ineffective hold process can result in the spoliation of relevant evidence and a variety of different sanctions against a party. "Spoliation is the 'destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation.'"[102] Potential sanctions for spoliation of evidence include the dismissal of a claim or the granting of summary judgment in favor of the party who is prejudiced, an adverse inference jury instruction, fines, and attorney's fees and costs.[103] The following cases are examples of what awaits parties who fail to preserve ESI.

"WHAT WE'VE GOT HERE IS FAILURE TO COMMUNICATE."

1. The *Zubulake* Decisions: Backup Tapes and Litigation Holds

The United Stated District Court for the Southern District of New York issued five decisions in one case that, collectively, served as a wake-up call to parties and practitioners concerning the dangers of lax oversight of the preservation and production of electronic