

Summer 2009

Sponsor



Economic Damages & Regulatory Analysis

Economic & Financial Analysis of damage claims in Personal Injury, Commercial, and Healthcare Litigation

Loss of Earnings Analysis
Life Care Planning
Vocational Assessment
Business Valuation

Topics

Letter from the Editor

Feature Articles

From the Editor

From the Editor-in-Chief

by John D. Martin

In this edition of *E-Discovery Connection*, the authors cover many important electronic discovery topics. Joseph Valentine discusses the potential adverse effects of preservation orders and ways to manage these issues when such orders are unavoidable. Nicole Boehler and Marla Weston explain the gap between data privacy laws in Europe and United States litigation obligations and suggest potential methods for complying with both. Additionally, Sandra Stevens discusses two recent English e-discovery cases and the similarity of the principles followed to those in the United States.

Todd Nunn also provides detailed insight into methods for protecting the attorney-client privilege throughout the various steps of the e-discovery process and Alison Grounds discusses the issue of when the duty to preserve electronically stored information ends.

Finally, Hunter McMahon discusses the shortcomings of the Federal Rules of Civil Procedure and makes the case for amendments to Rule 26(f)(3) to require a cost-benefit discussion during the meet and confer process.

Please let us know if you would like to contribute to a future edition of this newsletter, as we always welcome submissions on emerging issues in the area of electronic discovery.

John D. Martin
Editor-in-Chief
Nelson Mullins Riley & Scarborough LLP
john.martin@nelsonmullins.com

John Martin is a partner at Nelson Mullins Riley & Scarborough LLP where he practices products liability, business, pharmaceutical, and medical device litigation. Mr. Martin is routinely called on by his clients to consult on electronic discovery preparedness and case-specific

Feature Articles

E-Discovery Preservation Orders—Exception or Rule?

by Joseph Valentine

The Federal Rules of Civil Procedure present an apparent tension regarding preservation orders. On one hand, Rule 26(f) explicitly requires the parties to discuss preservation of electronic data, and Rule 16 provides for a court order incorporating the parties' discussions. On the other hand, the official commentary makes it clear that the rules do not anticipate routine entry of preservation orders.

The jury is still out on how this tension will be resolved in practice. A party with voluminous electronic data should carefully consider how best to protect vital interests in this evolving arena. For companies with electronic data practices typical in today's business environment, broad preservation orders could result in significant additional expenditures, in some cases more than one million dollars per month.

I. Grounds to Oppose Entry of a Preservation Order

Implementation of the 2006 federal electronic discovery rules has dramatically increased many parties' litigation expenses. In addressing preservation orders, however, it remains appropriate to re-emphasize the dual objective of the new rules to maximize efficiencies in discovery and to minimize unreasonable burdens on the parties.

Consistent with that fundamental objective, preservation orders ought not to be routinely entered, but instead should be entered, if at all, only upon a showing of case-specific reasons supporting such an order and specific terms of the order. *See Ellington Credit Fund, Ltd. v. Select Portfolio Servs., Inc.*, No. 08 Cir. 2437 (RJS), 2009 WL 274483 (S.D.N.Y. Feb. 3, 2009) (denying motion for a preservation order in the circumstances of the case, in which the defendants, having submitted uncontested evidence of reasonable preservation steps, were fully aware of their common law preservation obligations, and the plaintiff had not provided reasonable terms for any such order).

The federal electronic discovery rules represent "intensive work" since 2000 by "bar organizations, attorneys, computer specialists, and members of the public [to] address the serious problems arising from discovery of electronically stored information." *Excerpt from the Report of the Judicial Conference, Committee on Rules of Practice and Procedure*, Sept. 2005, at 3, available at www.uscourts.gov/rules/supct1105/Excerpt_STReport_CV.pdf ("Judicial Conf. Report"). The discovery rules had been amended "in 1980, 1983, 1993, and 2000 . . . to provide more effective means for controlling overuse and occasional misuse of the discovery devices." *Id.* at 5. The amendments promulgated in 2006 "to make the rules apply better to electronic discovery problems have the same focus." *Report of the Civil Rules Advisory Committee, Advisory Committee on the Federal Rules of Civil Procedure*, May 27, 2005 (revised July 25, 2005), at 13, available at www.uscourts.gov/rules/supct1105/Excerpt_CV_Report.pdf ("Advisory Comm. Report").

None of this "intensive work" on the rules required routine entry of preservation orders. On the contrary, it is beyond dispute that Rule 26(f), which requires the parties in certain circumstances to address preservation issues, is not intended to result in a preservation order:

The requirement that the parties discuss preservation does not imply that courts should routinely enter preservation orders. A preservation order entered over objections should be narrowly tailored. Ex parte preservation

orders should issue only in exceptional circumstances. Fed. R. Civ. P. 26(f) advisory committee's note (2006).

Under the amended rules, whether or not "a preservation obligation arises depends on the substantive law of each jurisdiction, which is not affected by the proposed rule." *Judicial Conf. Report*, at 15 (referring to Rule 37). Indeed, because of a concern that an inaccurate interpretation of the rules could improperly "promote early applications for preservation orders," the final advisory committee's note was revised "to state that preservation orders entered over objections should be narrowly tailored and that preservation orders should rarely be issued on ex parte applications." *Advisory Comm. Report*, at 16.

II. Negotiating a Reasonable Preservation Order

Of course, there will be circumstances in which a focused preservation order will be appropriate. In such circumstances, there are many points to address to minimize any unfair burden or prejudice that could result from an overly broad order. The often under-utilized "legislative history" for the electronic discovery rules cited above can help in this context. Even in non-complex cases, the helpful commentary in section 11.442 of the *Manual for Complex Litigation* (4th ed.) identifies important and concrete reasons for limiting any preservation order to the maximum appropriate extent.

A. Continuation of Routine Operations

Under the letter and spirit of the electronic discovery rules, all parties must act reasonably in addressing the scope and effect of preservation of electronic data. Consistent with the obligation to identify "reasonable preservation steps," the "parties' discussion should pay particular attention to the balance between the competing needs to preserve relevant evidence and *to continue routine operations critical to ongoing activities.*" Fed. R. Civ. P. 26(f) advisory committee's note (2006) (emphasis added).

Indeed, the rules recognize "that all electronic information systems are designed to recycle, overwrite, and change information in routine operation, not because of any relationship between the content of particular information and litigation, but because they are necessary functions of regular business operations." *Judicial Conf. Report*, at 14.

In that specific context, it would be reasonable that any preservation order contain a "general obligations" section that sets out the following points or their equivalent:

- The parties shall be obligated to take reasonable steps to preserve documents and electronically stored information relevant to claims and defenses. (This paragraph should define those claims and defenses as specifically and narrowly as feasible.)
- "Document" and "electronically stored information" shall have the meaning set out in Rule 34(a) of the Federal Rules of Civil Procedure, namely, "writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations."
- Regarding electronically stored information specifically, complete or broad cessation of routine computer operations could paralyze the parties' activities. Accordingly, in identifying reasonable steps to preserve electronically stored information, and after taking account of specific requirements set out in the order below, each of the parties should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations

critical to ongoing activities. Except as specifically set out below, and emphasizing the good-faith obligation of the parties to avoid intentional destruction of relevant electronically stored information through routine operation of computers, nothing in this order shall prohibit continued good-faith implementation of a distinctive and necessary feature of computer systems—*i.e.*, the recycling, overwriting, and alteration of electronically stored information that are necessary functions of regular business operations and that attend normal use and routine operation of such systems in good faith.

- The parties shall meet and confer before bringing to the court's attention any additional preservation matters not encompassed by this order. Preservation obligations, if any, beyond those set out in this order shall be governed by the law of the applicable jurisdiction.

It is vital to become familiar in detail with the defensible rationales for each of the suggestions. The third point, in particular, takes language almost verbatim from Rule 26(f) advisory committee's note (2006), and from the *Judicial Conf. Report*, at 13-14.

In referring to the law of the applicable jurisdiction, the fourth suggestion emphasizes that the order should be narrowly tailored to deal with only those preservation obligations identified specifically in the order.

B. Particular Provisions

Although it is not possible to anticipate all electronic data practices that would have to be accounted for in a preservation order governing particular computer systems, several topics are likely to be in play in most cases once a preservation order becomes anticipated. In addition, depending on particular circumstances, it may be appropriate for the order to provide for the shifting of costs to implement any ordered steps.

1. Recycling (or Not) of Disaster-Recovery Tapes

Depending on the particular facts, it may be reasonable for the order to provide simply that recycling of disaster-recovery tapes (or other media) does not have to be suspended. On the other hand, when a party can make a concrete demonstration of a particular need, the proposed order should set out precise steps preserving some or all disaster-recovery tapes on a going-forward basis. "[A] data-preservation order that requires the accumulation of such backups beyond their usual short retention period may needlessly increase the scope and cost of discovery." *Manual for Complex Litigation* § 11.442 (4th ed.) Thus, counsel for the affected party must be familiar with all the details of the party's disaster-recovery system, because inattention to detail could result in costs exceeding tens-of-thousands of dollars *per day*.

In most circumstances, any order requiring preservation of disaster-recovery tapes should not also determine the reasonable accessibility of the data on any such tapes. The order should provide, instead, that the court will address any issue as to accessibility only if and when raised by the parties in connection with an actual discovery dispute.

2. Suspension (or Not) of E-Mail Auto-Deletion Functions

For important cost-management reasons, many companies arrange for automatic deletion of e-mails that are older than (for example) thirty days. Unless properly worded, a preservation order could require a company to suspend that practice company-wide, with

possibly devastating financial consequences. Although the issues in a particular case must be addressed uniquely, it may be possible to articulate reasons why no suspension is necessary. Alternatively, a potential solution could be to identify a manageable number of “key” personnel (with particularly relevant knowledge) whose e-mail files could be suspended from auto-deletion. Such a compromise would reasonably satisfy the opponent’s need for evidence while maintaining the additional costs to some reasonable level. Any such discussion should include the issue of cost-shifting.

3. Ongoing Software and Hardware Changes (“Legacy” Issues)

Depending on the circumstances of the case, the preservation order could protect one or both parties by addressing how “legacy” issues will be resolved. An incomplete or inartfully phrased preservation order could inhibit a party’s plans to improve or change its software or hardware. In some instances, such plans could result in a set of data that is accessible in the older system but that would not be reasonably accessible in the newer system. If a party currently has concrete plans for such changes, the order should explicitly account for those plans. In addition, if a party can anticipate the likelihood of making such changes during the litigation, the order should set out procedures that would require the parties to work cooperatively to determine the extent to which (and at whose cost) software and hardware to be replaced in the future must be preserved.

4. Requirements regarding Litigation Hold Notices

The law on litigation hold notices to representatives of the parties is evolving, and issues such as periodic updated notices and monitoring of compliance with the preservation instructions are rising in significance. In some circumstances, a party must be ready—based on comprehensive knowledge of its electronic data systems—to identify and propose concrete steps pertaining to the issuance and content of, and any required monitoring of compliance with, litigation hold notices. In addition, it could be valuable to include a provision that nothing in the order waives any privilege or work-product immunity applicable to preservation instructions. See *Muro v. Target Corp.*, No. 04 C6267 2007 WL 3254463 (N.D. Ill. Nov. 2, 2007) (holding litigation hold notice protected by the work-product doctrine).

III. Conclusion

In many circumstances, a party that could be adversely affected by a preservation order may demonstrate reasons, under the case law and the “legislative history” of the electronic discovery rules, why such an order should not be entered. In circumstances where a preservation order must be negotiated and entered, the party should anticipate and fully address concrete and potentially devastating pitfalls in the terms of such an order.

Joseph Valentine is Of Counsel with the Denver-based litigation firm of Wheeler Trigg Kennedy LLP. Mr. Valentine focuses his practice on advising major corporations regarding discovery of electronic data and protection of privileged and work-product data.

The European Union is Not “Getting Over” Data Privacy: the Data Protection Gulf Between the European Union and the United States

by Nicole B. Boehler and Marla R. Weston

The chairman of Sun Microsystems said in 1999, “You have zero privacy anyway. . . . Get over it.” Polly Sprenger, Sun on Privacy: ‘Get Over It’, Jan. 26, 1999, <http://www.wired.com/politics/law/news/1999/01/17538>. Although recent trends show that this may indeed be the case for individuals in the United States, European Union citizens find otherwise. The talks at the DRI Europe data protection conference in April 2009 brought home the tremendous difference between Americans’ and E.U. citizens’ respective sensibilities about data privacy. Truth be told, Europeans do have comparatively stronger expectations of data privacy, even in the workplace.

In the context of electronic discovery in particular, attention should be paid to the various data protection rights enjoyed by citizens of particular Member States. For example, under the French implementation of Directive 95/46/EC (the E.U. directive regarding data protection), it has been suggested that data privacy rights may be violated at the moment the litigation hold notice is distributed. If so, a litigant, or its representative, may inadvertently violate multiple individuals’ data privacy rights simply by fulfilling its duty in U.S. litigation to preserve electronically stored information by sending notification that it must be preserved. This potential for inadvertent encroachment upon privacy rights is enhanced in the e-discovery context, because the potential data subjects are often numerous and could be of diverse nationalities.

In determining the circumstances under which issuance of a litigation hold notice would violate the French Act implementing the Directive—Law No. 78-17 of Jan. 6, 1978 on Data Processing, Data Files and Individual Liberties (as amended by the Act of Aug. 6, 2004)—it is necessary to examine several provisions. First, the Act defines the “processing” of data to include “obtaining” the data (Law No. 78-17, art. 2), which may be interpreted broadly to include all acts taken by a litigant or practitioner in furtherance of responding to a request for discoverable information. Second, the Act requires,

For the purposes of the processing mentioned in [the Act], the data controller shall notify the ‘Commission nationale de l’informatique et des libertés’ (CNIL) of the appointment of a representative established on French territory who shall represent him for the fulfilment of the duties required by this Act.

Law No. 78-17, art. 5, § II. Thus, a litigant or its representative may have a duty to inform the CNIL *before* distributing a litigation hold notice.

A related blocking statute comports with the theory that liability can attach at the time a litigation notice is implemented:

Subject to treaties or international agreements and the laws and regulations in force, it is prohibited for any person to *request*, seek or disclose, in writing, orally or otherwise, economic, commercial, industrial, financial or technical documents or information leading to the constitution of evidence with a view to foreign judicial or administrative proceedings or in connection therewith.

C. Pen. Law No. 80-538, art. 1A (emphasis added).

E.U. Member States had leeway in implementing the data protection Directive, leading to differences in implementation—as well as interpretation—among laws of the various Member States. Therefore, the best practice in cross-border discovery is to review the implementations of the Directive, both in the jurisdictions where the data resides and the

jurisdictions where the data processors reside. In addition, it is advisable (and, in some cases, perhaps mandatory) to contact those countries' respective data protection authorities regarding the specific data processing and transfer plans, even before sending the litigation hold notice.

On the other hand, practitioners must balance E.U. Member States' requirements, such as contacting the data protection authorities prior to issuance of a litigation hold, with the requirement under U.S. law to implement the litigation hold promptly upon becoming aware of the potential for litigation. Since data protection authorities may significantly affect the discovery process, it is important that they recognize the potential need for haste in informing the data controller of their decisions concerning the need to block implementation of the subject litigation hold.

Contacting the CNIL might have prevented the unfortunate fate of "Christopher X," a French attorney employed by a U.S. law firm. Christopher X was criminally prosecuted under a French blocking statute for attempting to informally collect data in France for purposes of U.S. litigation. See *In re Advocat "Christopher X"*, Chambre Criminelle [Cass. Crim.] [highest court of ordinary jurisdiction] Paris, Dec. 12, 2007, Juris-Data [No. 2007-332254]. The blocking statute provides for the imposition of monetary penalties or imprisonment or both. Christopher X was sentenced to a € 10,000 criminal penalty. His crime consisted of telephoning an individual at a French company seeking to discover information for use in U.S. litigation. The French court held that by doing so, Christopher X infringed data protection rights. Contacting the CNIL before conducting discovery might have prevented such a result.

Consider another possible scenario: If a litigant or practitioner violates the Directive (or a law implementing it) at an early stage by issuing a litigation hold notice prior to contacting the data protection authority, and then later attempts to argue to a U.S. court that transferring data to the U.S. would violate the Directive, the argument against data transfer for fear of prosecution may be considerably weakened—even though the litigant may still face prosecution in the Member State for the violation.

That being the said, the CNIL has signaled a willingness to assist data processors in navigating its requirements as applied to particular data processing situations. In fact, this summer, the CNIL plans to publish recommendations to help businesses comply with both E.U. and U.S. laws in responding to international discovery requests.

We can also expect a summary of data protection rules for all of the G20 countries from the Sedona Conference.

Finally, on February 11, 2009, the E.U.'s Article 29 Data Protection Working Party published its "Working Document 1/2009 on Pre-trial Discovery for Cross Border Civil Litigation" (available at http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm). That document makes frequent reference to the similarly-titled Sedona Conference report of August 2008 (available at http://www.thesedonaconference.org/dltForm?did=WG6_Cross_Border). The E.U. Working Document may be the E.U.'s attempt at seeking a solution for the conflicts between discovery requirements in the U.S. and data protection laws in the E.U. At the moment, the E.U. Working Party recommends using the procedures of the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (23 U.S.T. 2555, T.I.A.S. No. 7444, Mar. 18, 1970), codified at 28 U.S.C. § 1781) if applicable, but it invites comments and is sure to receive some. Although the acknowledgement of the problem will not close the gap, it is possible that cooperation among data protection

authorities and the various working groups may eventually result in a safer way to bridge it.

Nicole B. Boehler and Marla R. Weston are both partners in the Stuttgart office of Carroll, Burdick & McDonough international (formerly Smith & Partners). Both are litigators with particular experience regarding the discovery of electronic information. Marla is a member of the California Bar and the Stuttgart RAK (Attorney-at-Law). Nicole is a member of the Bars of Virginia and Washington D.C. and of the Stuttgart RAK (Attorney-at-Law).

A Brief Look at How E-Discovery in the United States Compares With E-Discovery Across the Pond

by Sandra Tvarian Stevens

Two recent English decisions—*Digicel (St. Lucia) Ltd. v. Cable & Wireless PLC* and *Abela v. Hammond Suddards*—contain several well-established e-discovery principles that should be familiar to litigants in the United States. Importantly, both *Digicel* and *Abela* recognize that the need for discovery is subject to reasonable limitations.

In *Digicel (St. Lucia) Ltd. v. Cable & Wireless PLC*, [2008] EWCH (Ch) 2522, 2008 WL 4698881, mobile telephone companies applied for specific disclosure of certain electronic documents from the defendant telecommunication companies. In their response, the defendants indicated that their attorneys had performed “targeted keyword electronic searches” of electronic documents. The plaintiffs argued that the search was inadequate and requested that back-up tapes for the e-mail accounts of key former employees be restored and that various electronic searches then be performed. The England and Wales Chancery Division court identified the issues before it as (1) whether the defendants had performed a reasonable search for electronic documents; and (2) whether the defendants should be required to take additional steps to comply with e-discovery obligations. The court found that the search had not been reasonable because it had not included a search of the e-mail accounts of the specified employees and because an adequate keyword search had not been performed. The court concluded that it would be inappropriate “to make a simple order that D[efendants] restore the back-up tapes” because such an order would not address the possibilities that restoration might not be possible, or that if restoration was possible, that it would be cost prohibitive. Therefore, the court ordered counsel to meet and confer regarding how best to restore the back-up tapes and further ordered that the tapes be restored “as soon as was reasonably practicable.”

Digicel was soon followed by *Abela v. Hammond Suddards*, [Dec. 2, 2008] 2008 WL 5130206 (Ch), which involved a corporate acquisition dispute and related claims of negligence and breach of fiduciary duty. A request was made for disclosure of certain e-mails and electronic records. Citing *Digicel*, the court found that “[r]ecognition had to be given to the potential value of electronic searches in identifying important documents which might otherwise be missed.” The court explained that while no requirement existed that “no stone should be left unturned,” a reasonable search was necessary. The court invited counsel to make further submissions addressing how electronic disclosure was to be approached.

Digicel and *Abela* are consistent in several respects with U.S. law governing e-discovery. For example, both decisions implicitly recognize that parties have a duty to preserve information. U.S. courts have long imposed certain preservation obligations on litigants. See, e.g., *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (“The obligation to preserve evidence arises when the party has notice that the evidence is

relevant to litigation or when a party should have known that the evidence may be relevant to future litigation." (citations omitted)); *see also Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001) ("The duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation."). However, *Digicel* and *Abela* further recognize, as U.S. courts have, that the need for information is subject to reasonable limitations. *See, e.g., Zubulake*, 220 F.R.D. at 217 (finding that while litigants are "under no duty to keep or retain every document in [their] possession . . . [they are] under a duty to preserve what [they] know, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request." (citation omitted)) .

Both *Digicel* and *Abela* also required the litigants to meet and confer about how to best conduct the search for responsive information. This practice has been mandated in the United States since the Federal Rules of Civil Procedure with respect to e-discovery were amended in December 2006. *See, e.g., Am. Family Mut. Ins. Co. v. Gustafson*, No. 08-2772, 2009 WL 641297 (D. Colo. Mar. 10, 2009) (requiring parties to meet and confer and agree upon the electronic search terms to be used); *Bray & Gillespie Mgmt. LLC v. Lexington Ins. Co.*, No. 07-222, 2009 WL 546429, at *3 n.6 (M.D. Fla. Mar. 4, 2009) (noting that Fed. R. Civ. P. 26(f)(3)(C) "requires parties to confer and indicate their views and proposals regarding 'any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced'"). Some courts have denied requests for electronic discovery where the parties have failed to meet and confer. *See, e.g., Emmerick v. Penley*, No. 07-13, 2007 WL 2257646 (E.D. Tenn. Aug. 6, 2007) (denying motion to compel electronic discovery where parties had failed to meet and confer about the requested discovery); *In re Presto*, 358 B.R. 290, 293 (Bankr. S.D. Tex. 2006) (denying motion to compel where counsel had "pointed out" flaws in written deposition question answers to opposing counsel, but had failed to meet and confer with opposing counsel prior to filing the motion).

Thus, while it remains to be seen what future impact *Digicel* and *Abela* will have on e-discovery across the pond, if nothing else, U.S. litigants will recognize that the e-discovery principles identified in those cases are not very different from those they may encounter in the U.S.

Sandra Tvarian Stevens is a partner with the law firm of Wiley Rein LLP in Washington, DC, and a member of the firm's insurance and litigation practice groups.

Holistic Privilege Protection: Protecting Privilege by Taking "Reasonable Steps" Throughout the Process of Production

by Todd Nunn

There are now rules specifically designed to protect the attorney-client privilege during document production: Federal Rule of Civil Procedure 26(b)(5) and Federal Rule of Evidence 502. These rules provide a procedure for clawing back inadvertently produced attorney-client privilege and work product documents and a consistent framework for determining whether the privilege was waived. However, protection of privilege remains one of the primary concerns, and cost drivers, of parties producing documents in discovery.

The goals of the holistic approach to privilege protection are to protect attorney-client privilege and work product documents from being produced. Further, in the event of production, the goal is to have taken “reasonable steps” to protect the privilege from waiver under Federal Rule of Evidence 502(b). The goal is to do this while also producing documents that are responsive to discovery requests in a timely and economical way. This is made more challenging by the increasing volumes of electronically stored information (“ESI”) that must be screened for privilege.

Rule 502(b) states,

[T]he disclosure [of a communication or information covered by the attorney-client privilege or work product protection] 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).

The advisory committee’s note to Rule 502(b) states that generally a non-dispositive set of factors are applied to determine if there is waiver under the rule: “the reasonableness of precautions taken, the time taken to rectify the error, the scope of discovery, the extent of disclosure and the overriding issue of fairness.” Fed. R. Evid. 502(b) advisory committee’s note.

The note indicates that precautions taken at each phase of the lifecycle of the review and production of the documents, what this article calls the “process of production,” will be taken into account to determine “reasonable precautions.” This includes the beginning (“[t]he implementation of an efficient system of records management before litigation may also be relevant”), the middle (“a party that uses advanced analytical software applications and linguistic tools in screening for privilege and work product may be found to have taken ‘reasonable steps’ to prevent inadvertent disclosure”), to the end (“[o]ther considerations bearing on the reasonableness of a producing party’s efforts include the number of documents to be reviewed and the time constraints for production”) of the process. See *id.* The “holistic” approach to privilege protection advocates consciousness of privilege issues, and taking “reasonable precautions,” at each step of the process of production.

The process of production is broken down roughly into the following steps:

- Client’s communication and document management policy;
- Discovery planning/Rule 26(f) conference;
- Collection of ESI;
- Deduplication strategy;
- Search;
- Review strategy;
- Production/Privilege Log;

Preliminary Questions

In evaluating the process of production, a party must decide what is necessary for the particular case. What are the time frames involved for production of documents? What are the issues at stake, and what is the money value of the case? Is there a need for e-discovery, to what extent, and what types and volume of ESI are implicated? A party needs to decide whether it can do what is needed for each step of the process, or whether

it needs help for all or part of the process. Then, it must decide who can help at each step: e-discovery counsel, an e-discovery vendor, or in-house tools?

Client's Communication and Document Management Policy

Privilege protection begins with client policy. As the advisory committee note to Rule 502(b) states,

[T]he implementation of an efficient system of records management before litigation may also be relevant" to determining "reasonable steps" taken to protect privilege under the rule. An efficient communication and records management policy is the key first step in preventing disclosure of privilege. First, a document management policy that encourages keeping volumes of e-mail and other ESI low when there is no obligation to retain it will help mitigate the main cause of the privilege review problem, high volumes of ESI. Second, a communication policy that enforces certain practices around electronic communication relating to privilege can further reduce problems.

The biggest cost driver for privilege review is e-mail. When a client is casual about e-mail interactions with attorneys and legal departments, it can greatly increase both the cost of review and the likelihood of an inadvertent disclosure. The following are suggested policies and practices for making privilege protection easier:

- Address all legal e-mail only to the lawyer from whom advice is sought and limit recipients to those who "need to know." This keeps the volume of privileged ESI low and makes review, logging, and redaction consistency much easier. It will also be easier to determine the purpose of e-mail with fewer recipients.
- Clients should carefully limit distribution of documents, and be wary of large e-mail distribution lists. Again, this keeps the volume of privileged ESI lower (as it is sent to fewer people in the first instance). Further, large aliases increase the chance that the communication will fall outside the group of people covered by the privilege.
- Clients should consider adding "Legal" or some other clear designation to the legal department e-mail alias to aid in identification (by search term or otherwise) of mail with potential legal content.
- If e-mails with legal content are sent to non-legal corporate recipients, they should be marked clearly as containing legal content and marked "do not forward."
- If in-house counsel wears more than one hat (business advice and legal advice), legal communication should be plainly marked as such. This will make it easier for search and review to identify truly privileged communications.
- When legal advice is requested or given, the communication should do that specifically so it is clear that there is legal content.
- Do not put "privileged" in regular signature lines.
- Keep a centralized list of outside counsel names and the cases they have worked on. This will be needed for developing search terms and for the reviewers to identify potentially privileged communications.
- Identify work product communications clearly. Work product protected documents can be the most difficult to identify because there is not necessarily an attorney on the communication, and there isn't necessarily any request or provision of legal advice. More context may be necessary to identify work

product in ESI. The clearer it is that certain work or communications are work product, the better.

- Consider technology that can tag privileged communications for automatic identification.

In addition to e-mail policies, clients should consider other ESI policies relating to privilege protection. For example, policies controlling the use of instant messaging (“IM”) for privileged communications (given the inherently casual nature of the chats and the ephemeral quality of the chat logs) and clear identification of any databases that can contain privileged communications, and the fields that could contain that information. Some of the above policies and practices are basic and well understood by clients, but are easier to conceptualize than to enforce on a day-to-day basis. And while perfect compliance is not realistic with any communication policy, a policy that encourages consciousness of privilege issues in handling ESI will aid in protection of the privilege during discovery.

Discovery Planning and the Rule 26(f) Conference

Privilege protection is one of the most important issues to address as part of discovery planning. Federal Rule of Civil Procedure 26(f) expressly requires it as a subject of the discovery plan. See Fed. R. Civ. P. 26(f)(3)(D) (requiring discussions regarding “any issues about claims of privilege or of protection as trial-preparation materials, including – if the parties agree on a procedure to assert these claims after the production – whether to ask the court to include their agreement in an order”). During the Rule 26(f) conference, or more likely during a series of conferences, there are a number of issues relating to privilege that can be discussed (and potentially agreed upon):

- **Scope of discovery.** The parties can seek to establish an appropriate scope of discovery so that each has a better idea of the type of privilege issues and the volume of review that will be needed.
- **Timing of production.** Given the volume of ESI and other material the party must review, the party can make sure that there is an understanding of the amount of time needed to prepare for production, and whether a rolling production will allow for more time.
- **Timing of privilege log.** Timing of the privilege log is a frequent source of dispute and waiver arguments. A party should seek to agree on the timing of the log. The timing that a party should seek (and on which the party will be able to get agreement) will differ from case to case, but thirty days after the final production is a good rule of thumb.
- **Form of the privilege log.** The amount and type of information provided in a privilege log is frequently a subject of dispute and arguments of waiver. Seeking to agree in advance to the information provided in the log can avoid the “gotcha” tactics of some parties. Even if there is no agreement, it may be prudent for a party to submit a sample of a log the party is comfortable with to the court for pre-approval.
- **Redactions.** How redactions will be done and logged is a basic concept, but one that, if discussed in advance, can avoid trouble.
- **Problematic ESI.** Some types of ESI will require unusual efforts to protect privilege. Voicemail, database reports, and IMs are some examples. There may be a need to discuss timing or form of production for this ESI.
- **Form of production.** A discussion of the form of production is another subject that is expressly required by Rule 26(f). See Fed. R. Civ. P. 26(f)(3)(C). The form

of production can implicate privilege protection. For example, production of native format documents can expose privilege information in metadata or tracked changes. Converting native files into images and providing load files can maintain the “reasonably useable” nature of the documents, but may cause issues for some types of ESI. Spreadsheets do not image well, for instance, but they may also be less likely to convert to privileged information. Some types of ESI may be produced natively while others are imaged. Discussion in advance can avoid problems.

While the above discussions may not result in agreement, the proposing party can document the discussions and raise the issues with the court as part of the scheduling conference or in a motion for protective order. Simply flagging the issue for the court may be useful later, particularly on issues relating to privilege logs and redaction. The Rule 26(f) conference is also an opportunity to agree to a protective order. While it might seem that clawback and non-waiver agreements are less necessary because of Rules 26(b)(5)(B) and 502(b), they are still very useful tools in privilege protection. Waiver of privilege is still possible under Rule 502(b) depending on the circumstances. *See Rhoads Ind. v. Bldg. Materials Corp.*, 254 F.R.D. 216 (E.D. Pa. 2008). A non-waiver clause can provide greater protection than Rule 502(b). *See Alcon Mfg. Ltd. v. Apotex Inc.*, No. 1:06-cv-1642-RLY-TAB, 2008 WL 5070465 (S.D. Ind. Nov. 26, 2008). Federal Rule of Evidence 502(d) states, “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.” A non-waiver clause can simply state that no inadvertent production can result in waiver, allowing the party to avoid having to meet the Rule 502(b) test. *Alcon*, 2008 WL 5070465, at *6; Fed. R. Evid. 502(d) advisory committee’s note (“[T]he court order may provide for return of documents without waiver irrespective of the care taken by the disclosing party.”).

The Advisory Committee note to Rule 502(d) states the policy, “The rule provides a party with a predictable protection from a court order – predictability that is needed to allow the party to plan in advance to limit the prohibitive costs of privilege and work product review and retention.”

Although it is not generally a good practice to make no effort to remove privileged documents (because there are other reasons to protect privileged information than just waiver protection), a non-waiver order can provide considerable back-up protection. Additionally, while it is more common for such orders to be entered by agreement between the parties, there is no requirement of an agreement. Indeed, as Rule 502(d) Advisory Committee note makes clear, “Under the rule, a confidentiality order is enforceable whether or not it memorializes an agreement among the parties to the litigation. Party agreement should not be a condition of enforceability of a federal court’s order.” If no agreement can be reached with opposing counsel, it may be prudent to seek a protective order on privilege by motion to the court based on the protective policy expressed under Rule 502.

Collection of ESI

Parties should keep privilege protection in mind when collecting ESI. If collecting by custodian, a party should be aware of what each custodian’s involvement with legal issues is likely to be. A custodian questionnaire or interview can help in identifying privilege issues, as well as determining where and what ESI the custodian has. The custodian should be questioned about (1) what issues the custodian works on with the legal department or outside lawyers (or what cases or legal projects), (2) the lawyers with whom that person specifically works or has communicated, (3) during what time periods, (4) whether the custodian has ever been directed to assist with legal issues in any way,

and (5) what specific documents or types of documents that person can identify as potentially containing privileged or work product communications. Knowing the custodians' involvement with legal issues will allow that material to be handled differently during search and review if there is an indication of heavy legal involvement. The lawyer names and legal projects will help with developing effective search terms and help the review attorneys effectively identify privileged and work product communications.

Understanding the type of ESI that is being collected is also important. For example, are there PDFs, TIFFS, other image files, WAV files or other file types that are not easily searchable with key words? If so, is there likely to be responsive material in those file types? And if so, is there likely to be privileged information in those file types? If the answer to all of these questions is yes, a strategy for screening that material for privilege should be developed.

It is also important to collect documents in such a way that the metadata, and therefore robust searchability, is maintained. The party should work with its vendor to understand how collection is being done, what is being collected, and to direct how the ESI should be handled based on the information gathered.

Deduplication Strategy

How is deduplication relevant to protection of privilege? Very simply, fewer documents to search, review, redact, log, and ultimately, to inadvertently produce means there is less likelihood of privileged material being disclosed. For example, the more duplicate lesser included e-mail strings there are with identical content at various places in the string, the harder it is to make redactions consistent. If there is a team of attorneys doing privilege review and applying redactions, and they are all redacting the same parts of different e-mail strings, consistency becomes a real issue. Also, it is important to remember that the number of privileged documents inadvertently produced is a factor for a court to consider when deciding waiver. *Rhoads Ind. v. Bldg. Materials Corp.*, 254 F.R.D. 216, 219 (E.D. Pa. 2008).

There are different deduplication strategies. The party should talk to its vendor to determine the vendor's approach and ability to deduplicate. Most vendors can suppress exact duplicates, but can the vendor also suppress lesser included e-mail strings (leaving only the longest string with a unique top communication) or "near duplicates"? Most vendors can deduplicate within each custodians' material, but can they also deduplicate across custodians, providing an even more drastic volume reduction? The vendor should also be able to track what is deduplicated across custodians so that the opposing party can be provided with a log, or a load file, that identifies all custodians who had each duplicate file. The timing of deduplication is also important. Deduplication before review is vital to reduce the volume of review and redactions. A deduplication process that is run after review and redaction does not save any effort for the reviewing party, although it could reduce the amount that needs to be logged.

Search Strategy/Review

The party should discuss search strategy options with its vendor. There are many options for searching ESI. The Advisory Committee note to Rule 502(b) states that the use of "advanced analytical software" and "linguistic tools" to screen for privilege may constitute "reasonable steps" under the rule. That statement encompasses a wide range of possible search tools and strategies. Courts are focusing more attention on the use of search to screen for privilege. See *Victor Stanley v. Creative Pipe, Inc.*, 250 F.R.D. 251 (D. Md.

2008) (determining waiver based on privilege search approach before implementation of Rule 502). Courts will consider the search terms used and other aspects of the search strategy to determine whether “reasonable steps” were taken as part of deciding waiver under Rule 502(b). *Rhoads*, 254 F.R.D. at 224. While there are many options and technologies for search strategy, any of them will make use of the privilege information gathered during collection of ESI (as discussed above).

Search can be used in a number of ways to assist with privilege screening. Search terms alone can be used to screen for relevance and privilege under the right circumstances. Relevance terms can be run to determine the universe of responsive documents and then privilege search terms can be run to screen out privileged material. If this approach is taken, it is a good idea to agree on the particulars of this process with the opposing party in advance, and to enter into a clawback and non-waiver agreement to mitigate the risk of missed privilege.

Search can also be used to better organize a manual review. Some parts of the documents can be screened by search terms and others by manual review. For example, known third party (outside any possible privilege group) e-mail aliases can be run against the to, from, cc, and bcc metadata of a set of relevant documents to screen out ESI that will not be privileged because of its transmission to third parties. That material could comfortably be produced without further review. Then, a set of specific legal search terms (consisting of the names of in-house and outside counsel, the e-mail aliases for particular law firms, and known case and legal project names), can be used to create a set of material that is highly likely to contain legal communications, and will be reviewed further. Another review set can be created by more general privilege terms (“legal,” “attorney,” and “privileged”) and be staged for a different level of scrutiny. And material not hit by specific or general privilege terms, but also not sent to a third party, can be subject to another level of scrutiny. The information gathered from custodians (discussed above) may be used to design the searches and can be used in other ways to organize and inform the review.

The specific type of review to which material is subjected depends on the circumstances of the case, the issues involved, and the agreements in place. If there will be manual review of all or a portion of the material, the review team should be trained on the facts of the case, on privilege review generally, and be informed about the specific privilege issues for the custodians’ ESI they will review. The team should understand all of the information gathered from the custodians about each custodian’s involvement with legal issues. The review team should have the names of in-house and outside attorneys, and as much information as possible about their role in the legal issues of the client and their role in the case. There should be clear rules for how reviewers make privilege decisions. There should also be clear communication between the review team and the client to allow for questions relating to particular circumstances of privilege. As the review team works its way through the material, there may be additional attorney names and privileged projects identified, and this may require an adjustment of search terms and search strategy to capture additional potentially privileged material.

Production/Privilege Log

Assuming that the issues regarding form of production have been worked out as discussed above, with thought given to the privilege implications of the chosen form, the remaining issues for production relate to quality control. A final set of checks should be done. The final production should be checked to make sure that it contains the intended ESI. The images should be checked to make sure they display correctly and that redactions that

were applied (usually in a litigation support tool) remain in the image when put in final production format. Checking the number of responsive images in the production against reports from the litigation support tool can help ensure no additional privileged material has been included. The native files, or the load files that accompany images (depending on the form produced), should be searched for privilege terms and those responsive documents checked to make sure that privileged material was not missed in the first instance, or inadvertently re-introduced to the production set. Also, a party should check the load files for redacted images to make sure the OCR or extracted text does not reveal the redacted content of the image. The text from these load files should be removed or separately redacted.

The Advisory Committee note to Rule 502(b) discusses post production obligations:

The rule does not require the producing party to engage in a post-production review to determine whether any protected communication or information has been produced by mistake. But the rule does require the producing party to follow up on any obvious indications that a protected communication or information has been produced inadvertently.

Fed. R. Evid. 502(b). Thus, once the documents are produced, there must be notice of an inadvertent production to obligate a party to check for privileged material in the production. When the party receives notice, it will want to have the material in a litigation support tool that is searchable in both the full text and the metadata of the ESI. The tool should also preserve any tags or other coding that was put on the documents during the review. It should clearly identify what material was produced, withheld as fully privileged, and produced with redactions. Robust searchability will allow the party to quickly assess the scope of any inadvertent production and promptly take reasonable steps to rectify the error. The party should talk to its vendor and determine what information about each document is maintained or created during the review and whether it is accessible and searchable in the litigation support tool that will be used.

The privilege log will be produced at the time of or, more likely, sometime after, the production. If there was discussion and agreement on the timing and the content of the privilege log during the Rule 26(f) conference(s) (as suggested above), there should be no surprises. If not, the party should check the local rules, the judge's rules and any reported opinions because the standards for privilege logs can vary widely by jurisdiction. A party should talk to its vendor in advance of production about what log generating capabilities the review tool or litigation support tool offers. A lot of information needed for the privilege log can be generated automatically. The party should have a plan for how it will create the privilege log in the time allowed and in the form that is required.

Conclusion

Following the holistic approach and taking reasonable precautions at each step of the process of production will better and more efficiently protect attorney-client privilege and work product communications from disclosure. It also helps to better build a record that reasonable steps were taken to protect privilege to avoid waiver under Federal Rule of Evidence 502(b) in the event of disclosure. The suggestions above are not exhaustive, but illustrate a philosophy and approach that can help protect privilege in civil discovery.

Todd Nunn is a partner in K&L Gates' Seattle office and a member of the e-Discovery Analysis and Technology (e-DAT) Group, which provides electronic discovery and

document review legal services. Todd advises clients on e-discovery issues, document preservation, and discovery response planning.

When Does the Duty to Preserve End?

by Alison Grounds

The duty to preserve electronically stored information (“ESI”) potentially relevant to litigation and the penalties for failing to properly and timely comply with this duty are well-documented. We have all heard the horror stories, read the ever-evolving body of cases, and been bombarded by cautionary White Papers from vendors and service providers. Parties in both state and federal courts frequently argue about when the duty to preserve attaches in a particular case, and judges regularly sanction parties who fail to take reasonable steps to preserve relevant information after the duty arises.

However, one important question is not often addressed by the courts or commentators: “When does the duty to preserve end?” The answer to this question is significant for a number of reasons that relate to the larger issues associated with defensible, cost-effective practices regarding the management, collection, review, and production of ESI.

Why Does It Matter?

Prematurely releasing a litigation hold and allowing potentially relevant ESI to be lost or destroyed can lead to sanctions in the same manner as failing to properly implement the hold in the first place. On the other hand, failing to timely release a litigation hold can increase the burdens and costs associated with managing the massive amount of ESI generated every day by businesses of all sizes.

The burdens and costs associated with maintaining ESI, including ESI that was taken out of the normal data management and destruction lifecycle for a litigation hold, can, and often do, far outweigh the cost savings and risk aversion that come with following a defensible, consistent process for managing ESI. Recognition of the risks and costs associated with maintaining ESI beyond its useful life is inspiring many companies that have not already done so to create or revise data management policies and litigation readiness plans. If implemented and followed consistently, such plans can significantly reduce the costs and risks associated with amassing stockpiles of e-mails, PowerPoint presentations, and company retreat photos. Any effective data management or litigation readiness policy should include defensible procedures for releasing ESI from a litigation hold.

Why Is This a Difficult Question?

The timing of when to release ESI from a litigation hold may seem as simple as “when the case ends.” Unfortunately, many situations which trigger a preservation obligation do not have an easily identifiable trigger for its release. For example, even a lawsuit that results in a settlement may not trigger a release if there are other similarly situated plaintiffs who are likely to file suit. No existing rule or case law provides a convenient checklist for when the duty to preserve ESI expires, and courts will likely assess these issues on a case-specific basis using the same inquiry they use to assess when the preservation obligation is triggered.

Courts have held that the obligation to preserve evidence is triggered “when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.” *Cache La Poudre Feeds, LLC v. Land*

O'Lakes, Inc., 244 F.R.D. 614, 620 (D. Colo. 2007) (quoting *Zubulake v. UBS Warburg, LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003)). Recognizing that "litigation is an ever-present possibility in our society," the duty to preserve requires that future litigation is not merely possible, but probable. *UMG Recordings, Inc. v. Hummer Winblad Venture Partners*, 462 F. Supp. 2d 1060, 1068 (N.D. Cal. 2006); *Cache La Poudre Feeds*, 244 F.R.D. at 621.

As illustrated by the case law in this area, determining when future litigation goes from possible to probable is a fact-specific inquiry that illustrates the difficulty in knowing when the duty to preserve has ended. A few examples and the dilemmas they create include the following:

- Company A receives a preservation notice and a clear threat of future patent infringement litigation. Assuming the letter is sufficient to trigger the duty to preserve, how long does the obligation last? What if the lawsuit is not filed for a year, or two, or three, or ten? Does the trigger ever expire?
- What if the patent infringement lawsuit is actually filed against Company A along with several other similar companies, but then Company A gets dismissed from the lawsuit without prejudice? Does the resolution of the underlying case end Company A's preservation obligation or is Company A required to continue to preserve and wait to see if the claimant decides to refile?
- What if Company A never receives any preservation notice, is not sued, but is in a similar position to other companies who are sued? Should Company A anticipate that future litigation is probable?

The patent infringement aspect of the hypothetical examples above adds the complicating factor of a relatively long statute of limitations period which makes the option of triggering a release based on the date when the statute of limitations expires less viable. Unfortunately, companies will have to take a case-specific approach, guided by established protocols and guidelines, to determine when a particular hold can be released. Absent a clear directive from the courts on when a duty to preserve expires, the best guidance comes from the cases addressing when the hold is triggered.

For example, *UMG Recordings, Inc. v. Hummer Winblad Venture Partners*, 462 F. Supp. 2d 1060 (N.D. Cal. 2006) illustrates the risks associated with failing to issue and maintain a litigation hold during a series of related lawsuits, including after a company has been dismissed from a lawsuit. *UMG Recordings* is one of a series of related cases involving claims of copyright infringement against Napster brought by recording industry plaintiffs. Hummer Winblad Venture Partners ("Hummer") became an investor in Napster in May 2000—when Napster was involved in several pending lawsuits (collectively "*Napster I* litigation"). One month later, on June 1, 2000, Hummer was served with deposition and document subpoenas requesting communications related to Napster in the *Napster I* litigation. Two days after receiving the subpoenas, a Hummer executive sent an e-mail out to all Hummer employees which the court later found instructed employees to delete all Napster-related e-mails going forward in order to avoid producing them ("June 3, 2000 E-mail"). Later that same month, an officer of Hummer was advised by the CEO of Universal Music Corporation that the recording companies intended to sue Napster's investment firms if the alleged copyright infringement continued. In July 2000, a lawsuit was filed against Napster and other defendants, including Hummer ("*Katz* lawsuit").

The *Katz* lawsuit was subsequently dismissed in July 2001, but the *Napster I* litigation remained ongoing. In August 2001, as part of the settlement negotiations in *Napster I*, counsel for plaintiffs sent Hummer a letter threatening litigation. Hummer acknowledged

that it knew it was going to be sued in an April 2002 e-mail sent to a potential purchaser of Hummer, and, one year later, in April 2003, the instant lawsuit was filed.

When Hummer produced the June 3, 2000 e-mail as part of the *UMG Recordings* litigation, the plaintiffs sought sanctions against Hummer for failing to preserve relevant ESI. The court had to determine not only when the duty to preserve was triggered, but whether, as Hummer argued, Hummer's preservation obligation ended after the *Katz* lawsuit was dismissed. Hummer argued that the dismissal of the *Katz* case in July 2001, to which it was a named party, terminated any preservation obligation and no new obligation to preserve was triggered until Hummer was served with the *UMG Recordings* complaint in August 2003. The plaintiffs argued that the preservation obligation was triggered in May 2000, when Hummer invested in Napster, and remained in effect through the current litigation.

The court held that the initial preservation trigger occurred in June 2000 when the CEO of Universal Music told an executive at Hummer that it planned to sue the company. The court held that this clear statement of intent to sue coupled with the existing related litigation was sufficient to trigger a preservation obligation. The court also held that Hummer's duty to preserve was not released upon dismissal of the *Katz* lawsuit because Hummer was aware "there was a reasonable probability of litigation against Hummer during the period following the *Katz* lawsuit." *UMG Recordings*, 462 F. Supp. 2d at 1069-70. Notably, the court held that Hummer's status as an investor in Napster and Hummer's receipt of a third-party subpoena in the *Napster I* litigation were **not** enough alone to create a reasonable expectation that litigation against Hummer was probable rather than just possible.

The additional surrounding circumstances that elevated the threat of litigation against Hummer from possible to probable included (1) Hummer's receipt of a letter threatening suit in August 2001, one month after the *Katz* litigation was dismissed; (2) John Hummer's admission to a potential purchaser in April 2002 that he knew Hummer would be sued; (3) Hummer's past status as a party in the *Katz* lawsuit; and (4) Napster's bankruptcy and the plaintiffs' litigation strategy to pursue solvent investors.

Accordingly, the court found that Hummer had at worst "mounted a knowing and concerted effort to destroy Napster-related e-mails that it had a duty to preserve and produce" and at best had been "grossly negligent in executing its duties to preserve evidence" *Id.* at 1074. The court concluded that an adverse inference instruction and monetary sanctions were warranted.

The court's fact-specific holding does not provide a clear test for when a preservation obligation expires, but it does offer some additional factors to consider when assessing when to release legal holds, including the following:

- Whether similarly situated parties have been sued in other litigation;
- Whether the company has been involved in similar litigation in the past; and
- Whether plaintiffs or potential plaintiffs have communicated an intention to sue (or refile).

Companies balancing the costs and burdens of preservation against the risks associated with failing to preserve potentially relevant information must carefully weigh the risks and burdens and evaluate the specific circumstances that triggered the hold in the first instance. Companies may want to consider adding certain factors or timelines into their

own policies that show a good faith and consistent approach to making these determinations.

The general guiding theme in determining when a litigation hold can be released is the same as whether it has been triggered: Does litigation continue to be probable rather than merely possible? The fact-specific answer to that question requires careful assessment of the particular circumstances of the case in light of the company's established practices and procedures for management of ESI. A consistent approach that considers such factors as those identified in *UMG Recordings* reduces the costs and burdens associated with keeping the preserved ESI out of the regular data management lifecycle while providing a defensible process in the event that the timing of a litigation hold release is ever called into question.

Alison Grounds is a litigation associate at Troutman Sanders LLP and serves as co-leader of the firm's Electronic Discovery and Data Management Team. Alison focuses her practice on advising clients on the efficient management, production, and use of electronically stored information in litigation, regulatory proceedings, and government investigations.

Shortcomings of the Federal Rules of Civil Procedure

by Hunter McMahon

Within a company's business plan, it is not common to include large contingency funds for settling frivolous claims out of pure financial necessity due to the possible exorbitant litigation costs that may be associated with electronic discovery. There are such things as the Rule 26(f) conference that requires counsel to meet and confer prior to conducting discovery, which can help minimize costs; however, the cost implications of producing even readily accessible data should be of more concern to both parties. Businesses in the current economy are struggling enough without the rising costs of litigation. The lack of specificity in the Federal Rules of Civil Procedure regarding grievous costs that can be associated with e-discovery should be remedied.

Rule 26(f)(3), "Discovery Plan," requires parties to submit their plans and views on several different facets of discovery; yet it fails to specifically include a required analysis of the costs. The rule covers such issues as (1) things as timing, form, or requirements for disclosures; (2) subjects on which discovery may be needed, when discovery should be completed, and whether discovery should be conducted in phases or be limited to or focused on particular issues; (3) disclosure or discovery of electronically stored information, including the form or forms in which it should be produced; (4) claims of privilege or protection as trial-preparation materials, including—if the parties agree on a procedure to assert these claims after production—whether to ask the court to include their agreement in an order; (5) what changes should be made in the limitations on discovery imposed under these rules or by local rule, and what other limitations should be imposed; and (6) any other orders that the court should issue. Should the rule not require a *cost-benefit analysis*? Sure, the notion of "reasonably calculated to lead to the discovery of admissible evidence" (See Fed. R. Evid. 26(b)(1)) is still in play, but at what cost?

Dating back to 1947 with the Learned Hand formula for negligence, the courts have imposed a cost-benefit analysis. *United States v. Carroll Towing Co.*, 159 F.2d 169 (2nd Cir. 1947). If the cost of the precautionary measure is greater than the likelihood of injury multiplied by the severity of said injury, then there is no negligence. How has that reasoning not translated to preventative measures regarding the rising costs of e-

discovery? Simply put, the Federal Rules have failed to establish fixed guidelines regarding excessive costs of litigation and the alleged injustices that have occurred.

Amending Rule 26 to include subsection (G) of (f)(3), with such language that would require parties to bring *at minimum, two estimates of associated costs and a breakdown thereof for the execution of the proposed discovery plan*, would at the very least bring the costs to the court's attention. It is unlikely that parties' are not already discussing costs, but to bring estimates of the overall costs to the court's attention would allow the court to compare the cost of the discovery with the damages sought. This would further support Rule 26(b)(2)(C) that allows the court to consider

[W]hether the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' respective resources, the importance of the issues at stake in the litigation, and whether the discovery sought will resolve those issues.

For example, an employment case poses a claim for \$100,000 in damages, but due to the size of the company and complexity of the IT infrastructure, it will cost at minimum \$20,000 to produce the e-discovery. The value of this suit is, thus, diminished by 20%.

Most attorneys will agree that the only truly effective way to minimize costs is to work with opposing parties to avoid such cumbersome costs. There are several reasons that cooperation between parties may be difficult—ranging from *just cause* to *strategy*. Either way, it is because such cooperation is not required, that one party (generally the plaintiff) continues to take advantage of the other by using the threat of costly e-discovery.

Yet, if Congress amends the Federal Rules of Civil Procedure to include a formula, similar to Learned Hand's negligence formula, it would allow courts to find the costs of e-discovery to *per se* outweigh the alleged injustice sought to be remedied and would help reduce the unneeded rise in litigation costs. Such a formula may present itself as follows: *if the cost of production is greater than 15% of the claimed damages minus shared costs, there is a presumption of overly burdensome discovery and therefore, requires a court appointed discovery referee whose fees and costs will be shared equally by all parties involved.*

The cost of litigation as a whole, but more specifically the cost of e-discovery, would be reduced because the imposition of a formula will force counsel to either cooperate or find more cost effective ways for handling e-discovery. Use of a *per se* formula that may render high cost e-discovery overly burdensome and inequitable, may also allow parties to initially limit their scope of discovery and more effectively cooperate during the Rule 26(f) conference.

There is a concern that having a *per se* formula in place would inadvertently encourage defendants to submit abnormally high budgets and/or estimates in an unjust attempt to reach the limit. However, this issue is no different from the current battles regarding what is "reasonably accessible" and the validity of document retention policies. Regardless, imposition of a formula could be met with force on several fronts. In addition to the above amendments, Congress could include such language as, *If a party is found to have submitted false or bad faith estimates, that party is subject to sanctions and will be financially responsible for all production costs relating to electronically stored information.* Also, it must be remembered that this not an irrefutable rule. There is still judicial discretion to allow the discovery; the formula simply gives more guidance to the courts as to what discovery presumptively fails the cost-benefit analysis.

In any event, the rising costs of e-discovery should be addressed by the Federal Rules of Civil Procedure or injustice will continue to occur. The current rules allow for too much judicial discretion and must be amended.

Hunter McMahon is a candidate for a Juris Doctorate from the University of La Verne College of Law, 2011; candidate for a Masters in Business Administration from the University of La Verne College of Business and Public Management, 2012. He is also the Administrative Systems Manager at P.K. Schrieffer LLP, an insurance defense firm in California. Mr. McMahon is a member of the DRI Electronic Discovery Committee.

NFJE



The National Foundation for Judicial Excellence is a 501(c)(3) charitable foundation dedicated to supporting an independent, well-informed judiciary in order to preserve excellence and fairness in the civil justice system. It is the only organization of its kind led by the Defense Bar. NFJE -- promoting excellence; affirming justice.