Nicole
Boehler,
Smith &
Partners

(13 Março 09)

This article was first published in *The International Comparative Legal Guide to Product Liability 2008*. To read country-by-country chapters, please click here.

At a glance

1. Introduction

The discovery of electronic evidence or e-Discovery has become a key focus in product liability litigation both in courts in the US and around the world. Recent amendments to and the creation of e-Discovery law in the form of statutes, cases, and court rules shows that the law is finally catching up with the realities of the Information Age.

e-Discovery or the discovery of electronically stored information (ESI) is generally understood as the act of preserving, collecting, preparing, reviewing, and producing electronic documents and data during civil litigation. Since the vast majority of corporate documents now are kept in electronic form, e-Discovery may very well soon overtake "traditional discovery" in terms of importance, volume and cost to the parties and the courts. The practitioner not only needs to be aware of the applicable rules governing e-Discovery, but also needs to be able to implement best practices when conducting e-Discovery and avoid its pitfalls.

This article will provide the reader with a very brief, summary overview of e-Discovery laws, cases, and principles and describe the current trends and outer boundaries of the major points of the law in this rapidly changing element of the discovery process.[1] In addition, this article will offer the reader practical tips in dealing with e-Discovery on a global scale.

2. e-Discovery is here and here to stay

Pre-trial discovery is an important process in a product liability case in any jurisdiction, but perhaps nowhere more so than in the US where broad discovery demands, loose standards of discoverability, strict time limits for production, and "person most knowledgeable" depositions on factual and now corporate IT issues, etc. can and do dramatically affect the conduct and outcome of any litigation. Until a dispute arises between the parties, discovery in the US remains largely unsupervised by the courts.

a. Discoverability of ESI in the US

In the US, the standard for discoverability is generally that the discovery must be "reasonably calculated to lead to the discovery of admissible evidence" – the information sought need not itself be admissible to be discoverable. *Fed.R.Civ.P. 26(b)(1)*. Parties may seek discovery of all information "relevant" to the subject matter of the litigation – a process that has often been described as "casting a fishing net" to see what you "catch." In addition to the broad discoverability standards, a company also faces short and strict time limits for production, generally between only 15–45 days within which to search, organise, evaluate, object to and produce all materials relevant to the discovery requests and demands. In addition to rights of written discovery, US discovery rules give litigants a right to conduct oral questioning under oath of company representatives who have knowledge of the subject matter of the litigation and/or the subject matter of the discovery. Increasingly, this means depositions of "persons most knowledgeable" in corporate IT departments, who are subpoenaed to testify about and explain corporate electronic document retention means and methods, policies and procedures.

Given the adversarial nature of US litigation, many cases are also fraught with discovery disputes that have to be carefully prepared by the parties and decided by the courts. Until the revisions to the US Federal Rules of Civil Procedure came into force on December 1, 2006, binding rules and helpful guidelines regarding e-Discovery practice were few and far between, and e-Discovery was – and in many US state courts

still is – often regulated only by case law, which necessarily led to more such disputes arising. This is beginning to change – in the US and elsewhere.

b. e-Discovery rules in the US federal courts

On April 12, 2006, The US Supreme Court unanimously approved e-Discovery amendments to the Federal Rules of Civil Procedure that had been under debate in the US since September 2005. These rules came into force on December 1, 2006. The amendments affect Rules 16, 26, 33, 34, 37 and 45.[2]

In the context of global products litigation in US federal courts, counsel must now meet and confer to resolve e-Discovery issues, including the scope of preservation, the types of technologies involved, and the form of production, in every lawsuit. This means that counsel has an affirmative duty to become intimately familiar with each and every client's manner, methods, processes and procedures for storing and maintaining electronic documents – a trend present in all e-Discovery regulations.

e-Discovery best-practices also require the creation and maintenance of an "electronic information system" – primarily via an ongoing document retention policy capable of being suspended on short notice via an appropriate litigation hold.

In addition to the US Federal Rules of Civil Procedure, many US federal courts have enacted local rules specifically governing the discovery of ESI, and others are considering them. Of the 94 US District Courts, at least 38 presently have specific local e-Discovery rules in effect[3] or "Default Standards for ESI". In addition, certain individual courts and judges have their own e-Discovery rules and forms. In 2007, the Federal Judicial Center released its "Managing Discovery of Electronic Information: A Pocket Guide for Judges".

c. e-Discovery rules in US state courts

In addition to amendments to the US Federal Rules of Civil Procedure, many US state courts have enacted or are considering e-Discovery statutes, rules and guidelines. As of February 2008, Arizona, California, Connecticut, Idaho, Illinois, Indiana, Louisiana, Maryland, Minnesota, Mississippi, Montana, New Hampshire, New Jersey, New York, North Carolina, Texas and Utah state courts all have either court rules or statutes affecting e-Discovery. Arkansas, California, the District of Columbia, Nebraska, New Mexico, Ohio and Washington are evaluating proposed rules. In August 2006, the Conference of Chief Justices of the US state courts issued an updated and detailed "Guidelines for State Trial Courts Regarding Discovery of ESI." In December 2007, the National Conference of Commissioners on Uniform State Laws approved its "Uniform Rules Relating to the Discovery of Electronically Stored Information", which advocates the adoption of e-Discovery rules in all US state courts.

d. e-Discovery outside of the US

Courts and entities outside of the US have also issued rules and guidelines related to e-Discovery. To date, all common law countries have some form of e-Discovery regulations and provisions. For example in the UK, the October 2005 amendments to the Practice Direction to UK Civil Procedure Rules r31 brought e-Discovery and

electronic disclosure to the fore for UK companies involved in litigation and those conducting discovery in the UK. Companies and their legal advisers not only have to examine how electronic documents are created, stored, searched and retrieved in litigation, but they also have to be aware of and follow the guidelines for e-Discovery at the very earliest stages of litigation. UK courts have even interpreted the e-Discovery rules to include the creation and production of reports on ESI.

The Supreme Court of Ireland reached a similar result in *Dome Telecom, Ltd. v. Eircom, Ltd.* (2007) IESC 59. In this competition case which alleged discriminatory phone charges, Dome sought discovery of the total minutes of calls to certain toll-free numbers from Eircom. While the court refused to order the creation of the report in this case, holding the discovery unnecessary and disproportionate, it did hold that "[i]t may … be necessary to direct a party to create documents even if such documents do not exist at the time the order is made."

UK and Irish treatment of a litigant's e-Discovery duties are clearly more expansive than US e-Discovery jurisprudence to date: in the US a litigant need only produce responsive documents and things in its custody and control and need not create evidence for production.

In Canada, the Province of Ontario issued its "Guidelines for the Discovery of Electronic Documents in Ontario" in November 1995 in response to a Report of the Task Force on the Discovery Process in Ontario. Though these Guidelines are not enforceable directly, they "may aid in the enforcement of agreements between parties or provide the basis for court orders."

In Australia, the Federal Practice Note on Document Management, Discovery and Electronic Trials will come into effect on July 1, 2008. The Practice Note will apply to all cases where the volume of discovery is reasonably anticipated to exceed 200 documents. Its purpose is to provide a framework for discovery of both paper and electronic documents and to facilitate the use of technology to increase litigation efficiency. In addition to the Practice Note, the Court also issued the following Related Materials: (a) the Pre-Discovery Conference Checklist (PDCC); (b) the Default Document Management Protocol (DDMP); (c) the Sample Advanced Document Management Protocol; (d) the Pre-Trial Conference Checklist (PTCC); and (e) the On-line feedback forum and email distribution list.

Other – primarily civil law – jurisdictions and the EU have on the books either legislation, binding court rules or guidelines to address the maintenance, storage, transfer and use of ESI in civil litigation. Most limit the information available to parties seeking discovery in litigation, including to protect personal privacy.[4]

Upon examination of the rules and guidelines, some common themes emerge: (1) the duty of counsel to become familiar with a client's electronic management system; (2) the client's duty to preserve electronic documents, where the term "documents" has a broad definition; (3) how one should go about ensuring preservation; and (4) the necessary balancing in assessing proportionality and costs in the e-Discovery process. In addition, the failure to properly provide e-Discovery often leads to severe sanctions, and there are significant privacy and other considerations that all counsel need to take into consideration in the face of international e-Discovery.

3. Counsel's duty to know: what are we even dealing with here?

The e-Discovery rules, laws, and court decisions handed down to date either expressly or implicitly impose a clear, affirmative duty on the part of counsel to research and understand the details of the corporate client's records management and IT systems as they relate to e-Discovery demands.

For example, the US District Court for the District of Kansas Electronic Discovery Guidelines state that "counsel should become knowledgeable about their clients' information management systems and their operation, including how information is stored and retrieved. In addition, counsel should make a reasonable attempt to review their clients' electronic information files to ascertain their contents, including archival, backup, and legacy data (outdated formats or media)." Ideally, all of this should occur prior to the beginning of the traditional discovery process, and perhaps even prior to any litigation, especially for in-house counsel.

Counsel's duty to be familiar with their clients' information management systems is a common theme in the rules and guidelines because electronic information is, by its very nature, fragile and transient – merely clicking on a document can lead to data alteration or destruction. In order for counsel to ensure that the company can properly preserve electronic information for production in litigation, counsel must know what the company has, where it is stored, how it is stored, and who is responsible for it.

4. Document preservation: okay, but can a company ever destroy anything?

One very hotly contested e-Discovery issue is exactly when a duty to preserve ESI arises and under what circumstances a company can destroy potentially relevant and discoverable business records.

The US Court of Appeals for the Fourth Circuit has explained that "[t]he duty to preserve material evidence arises not only during litigation but also extends to that period before litigation when a party reasonably should know that evidence may be relevant to anticipated litigation." *Silvestri v. General Motors Corp.*, 271 F.3d 583, 591 (4th Cir. 2001). This principle also clearly applies to ESI. In one recent case, *Doe v. Norwalk Community College*, 2007 WL 2066497 (D.Conn. Jul. 16, 2007), the court held that the duty to preserve arose at the latest when the defendant received the plaintiff's demand letter from her attorney, over two months prior to the plaintiff filing her complaint.

The court indicated that the duty to preserve and the attendant duty to issue a litigation hold may even have arisen seven months' prior thereto, when the parties first met to discuss the issues related to the lawsuit – the alleged sexual assault of the plaintiff by the defendant's employee, a professor at the College. In the *Doe* case, the defendant had, pursuant to its "normal practices", "scrubbed" the professor's hard drive after he left the College. In addition, a later forensic search of certain other employee's hard

drives revealed that pre-incident e-mails, which the plaintiff alleged would have shown the defendant's actual knowledge of the professor's conduct prior to her incident, had been altered or destroyed – also pursuant to College policy.

The College had not issued a litigation hold, nor had it directed key players to search for and/or preserve records relating to the case. The court ultimately granted the plaintiff's request for an adverse inference instruction with respect to the destroyed evidence and awarded Doe her reasonable attorneys' and experts' fees and costs for pursuing the motion and investigating the spoliation of evidence.

Outside of the US, the same principles apply. For example, the Ontario Guidelines provide: "As soon as litigation is contemplated or threatened, parties should immediately take reasonable and good faith steps to preserve relevant electronic documents." The duty to preserve, however, is not absolute. The Guidelines recognise that "it is unreasonable to expect parties to take every conceivable step to preserve all documents that may be potentially relevant." US courts have agreed:

A California court laid down some well-reasoned, common-sense rules regarding the destruction of corporate records for business reasons. In *Hynix Semiconductor, Inc. v. Rambus, Inc.*, No. C-00-20905 RMW (N.D.Cal. Jan. 4, 2006), Hynix sought terminating sanctions in a patent infringement suit because Rambus had in place a document retention policy that resulted in the destruction of potentially relevant and discoverable electronic and paper documents.

Prior to the case being filed, Rambus developed and began implementing a company-wide, written document retention policy. Under the policy, Rambus destroyed e-mail preserved on backup tapes after three months. Rambus also held several "Shred Days" to enforce compliance with its document retention policy. During the "Shred Days", Rambus instructed its employees to follow the retention policy guidelines and determine what information they should keep and what they should destroy.

Rejecting Hynix's arguments against such a document lifecycle management programme, the court stated: "Rambus' adoption and implementation of its content-neutral Document Retention Policy in mid-1998 was a permissible business decision… [made before reasonably anticipated litigation and] did not constitute unlawful spoliation." The court noted that the document retention and destruction policy and its implementation did not target any specific documents or category of relevant documents. Nor did the court find an intent to prevent the production of relevant documents in the lawsuit.

The court noted specifically that one "legitimate consequence of a document retention policy is that relevant information may be kept out of the hands of adverse parties." The court therefore refused Hynix's request for terminating sanctions and held that this destruction of even admittedly highly relevant information during an established, ongoing records retention and destruction programme was permissible absent notice to the company of potential litigation which would involve that specific information.

But not all courts have agreed. In a later patent infringement suit, also involving alleged spoliation by Rambus, the court undertook a detailed analysis of when and under what circumstances the implementation of the same document retention and destruction

policy may constitute spoliation, though the court ultimately did not impose sanctions. In *Samsung Elecs. Co., Ltd. v. Rambus, Inc.*, 439 F.Supp.2d 524, 565-74 (E.D. Va. 2006), the court relied on substantial documentation of Rambus's spoliation developed during the *Rambus, Inc. v. Infineon Tech. AG*, 220 F.R.D. 264 (E.D. Va. 2004) and *Hynix Semiconductor, Inc. v. Rambus,* Inc., *supra*, cases.

The court agreed with Samsung in this case and found that Rambus had engaged in the spoliation of evidence as part of its plans for litigation against the DRAM industry, including Samsung specifically. The court found that Rambus implemented its content-neutral document retention policy to justify destroying relevant and discoverable patent claims information when Rambus anticipated, or reasonably should have anticipated, litigation with Samsung.

The court assured, however, that "neither corporations nor individuals are at risk of a finding of spoliation merely because they adopt or implement a proper document retention policy." But the court also cautioned that "any company that implements a document retention policy during or in anticipation of litigation, and destroys documents relevant to the actual or anticipated litigation, will face and lose a spoliation charge." The court further found Rambus's litigation hold instructing its employees to "not destroy relevant documents" vague and insufficient to satisfy Rambus's preservation obligations in light of several factors, including: the volume of documents destroyed; the extent and types of evidence destroyed after the hold was issued; the failure to specify which documents were relevant to litigation; and the fact that Rambus maintained no records of which documents were destroyed.

The court went on to offer guidance on how companies can comply with their preservation duties by modifying document retention policies already in place. The court stated that in issuing a litigation hold, "the company must inform its officers and employees of the actual or anticipated litigation, and identify for them the kinds of documents that are thought to be relevant to it." The court also indicated that the collection and segregation of the relevant documents may also serve to comply with a corporation's duty to preserve. "It is not sufficient, however, for a company merely to tell employees to 'save relevant documents,' without defining what documents are relevant." The court observed that a company cannot "make a document retention programme an integral part of its litigation strategy and, pursuant thereto, target for destruction documents that are discoverable in litigation."

Similarly, in a case decided in late 2005, *In re Old Banc One Shareholders Sec. Litig.*, 2005 WL 3372783 (N.D. Ill. Dec. 8, 2005), a defendant was sanctioned for destroying records under similar circumstances. In *Old Banc One Shareholders*, the plaintiffs alleged spoliation of evidence and sought "draconian" sanctions: default judgment; the striking of the defendant's affirmative defences; or an adverse inference jury instruction. The plaintiffs had requested documents and data relating to underlying data, calculations and drafts of relevant documents allegedly "essential" to proving their claims.

The plaintiffs argued that the defendant's written document retention policy allowed these allegedly essential documents and data to be deleted or destroyed. Although the defendant could not produce the information requested, the defendant claimed to have met its preservation burden. In evaluating the defendant's document retention policy,

the Old Banc One Shareholders court noted the defendant was not obligated to preserve "every scrap of paper." The court found, however, that the defendant failed to implement and enforce a "comprehensive" document retention policy and failed to properly disseminate the policy it had in place to its employees. The court ultimately issued an order precluding the defendant from cross-examining the plaintiffs' expert witness at trial.

What these cases show is that a coherent, pre-litigation document retention policy is one key aspect to winning an e-Discovery battle. Courts have expressly recognised that companies need not keep all documents forever. However, a reasonable, good faith records management programme that is widely and consistently followed, as well as a plan for stopping it when the duty to preserve arises (see below), establish current best practices in this area.

5. The litigation hold letter: how does a company ensure preservation?

Any document retention policy must be designed to account for the case where litigation is anticipated, threatened or filed. At this point, counsel must ensure that any records retention policy in place is stopped to a degree such that evidence and information relevant to the dispute or potential dispute is preserved. It is now widely accepted that in order to accomplish this task, counsel must issue a "litigation hold." But "stopping" an ongoing document destruction programme pursuant to the document retention plan alone may not suffice to meet the legal burden to preserve information under new e-Discovery rules, as we saw in the *Samsung* and *Old Banc One Shareholders* cases, above. So what is a "litigation hold" then?

A litigation hold is correspondence transmitted to all individuals likely to be in possession of relevant information asking them to preserve all such materials in exception to the company's otherwise applicable records destruction plan. The notice should contain a description of the litigation and the categories of documents that should be preserved, and it should provide instructions on how to preserve those documents.

It should also provide information necessary to contact the in-house or external attorney or e-Discovery liaison, who is the client's designated person responsible for managing document preservation in a particular case. The notice should be circulated in different formats and as widely as needed in order to meet the preservation goals, including sending the document by various means, both hard copy and electronic, and perhaps even posting it or publishing it in public company areas.

Best-practices and current case law and rules of court essentially require the issuance of a litigation hold. These documents are, due to notice pleading in the US, often overly-inclusive and must be relatively detailed in order to serve their intended purpose.

a. Sanctions for failure to issue a litigation hold

In fact, the failure to issue a litigation hold by itself can lead to sanctions – both for the client and counsel. In *Tantivy Communications, Inc. v. Lucent Techs. Inc.*, 2005 WL 2860976 (E.D.Tex. Nov. 1, 2005.), the plaintiff accused the defendant of "hide the ball" discovery abuse during a patent infringement suit. The plaintiff petitioned the court to exclude certain defence evidence as a sanction for this alleged abuse. Specifically, the plaintiff had requested documents and data regarding interoperability testing, including information from the defendant's website.

The defendant had responded time and again in written discovery that it knew of no documents in its possession responsive to the plaintiff's requests. The plaintiff discovered during a later employee deposition, however, that the defendant had destroyed arguably responsive documents, including test plans and interoperability contracts - both in paper in electronic form - pursuant to its document destruction policy.

Citing the *Zubulake* line of cases, the court stated, "[the defendant] and its counsel are well aware that a party in litigation must suspend its routine document retention/destruction policy and establish a 'litigation hold' to ensure the preservation of relevant documents." Though the court preliminarily withheld ruling on the imposition of specific sanctions, it stressed in its ruling that it would not allow "lawyers or their clients to lay behind the log and disregard their discovery obligations."

Other court decisions indicate that merely sending a litigation hold may not be enough to meet current preservation obligations, i.e. more action may be required of counsel. In a decision known as *Zubulake V (Zubulake v. UBS Warburg LLC*, 229 F.R.D. 422 (S.D. N.Y. 2004)), the court held that it is both the in-house and outside counsels' duty to ensure that relevant information is preserved by giving clear instructions to the client to save it and – more importantly – to take affirmative steps to ensure the client is actually heeding those instructions.

At the outset of the litigation, counsel for the defendants instructed UBS personnel to retain relevant electronic information. Despite those orders, some UBS employees deleted relevant e-mails and destroyed electronic backup material in the corporate network. Some other employees never produced relevant information to counsel. As a result, many discoverable e-mails were not produced to the plaintiff until two years into the litigation – and some were lost forever.

The *Zubulake* court sanctioned the defendant specifically for the failure of its lawyers in: (1) not specifically giving "litigation hold" instructions and personally requesting retained information from a key employee involved in the dispute; (2) not adequately communicating personally with the employees about what electronic information they retained and how they maintained their computer files; and finally (3) not safeguarding backup material which could have contained deleted e-mails. The very serious discovery sanctions included both monetary fines and a ruling that the jury would be given an adverse inference instruction with respect to deleted e-mails.

More recently, in *Disability Rights Council of Greater Washington v. Washington Metropolitan Area Transit Authority*, 2007 WL 1585452 (D.D.C. Jun. 1, 2007), the court ordered the production of e-mail from backup tapes following the defendant's failure to preserve e-mails and halt its routine document destruction policy. In the

Disability Rights Council case, the plaintiffs claimed that the defendant unlawfully discriminated against the disabled by offering materially inferior service to patrons with disabilities.

During the prolonged discovery battle, the court determined that the defendant failed to halt its automatic e-mail deletion system, under which e-mails were automatically deleted after a period of 60 days unless the individual user saved the e-mail elsewhere. Apparently, the majority of system users never saved the e-mails to an alternate location. This destruction of potentially material evidence went on for a period of over two years after the complaint was filed.

The defendant attempted to invoke the Rule 37 safe harbour provision, but the court rejected this argument, noting that Rule 37 does not provide safe harbour to a culpable party. The court then applied the seven factors found in the Advisory Committee Notes to Rule 26(b)(2)(B)[5] to the facts in this case and ordered the defendant to restore and produce the relevant materials requested from the backup tapes.[6]

In addition to requiring the restoration and search of backup tapes, the court in *Treppel v. Biovail Corp.*, 2008 WL 866594 (S.D.N.Y. Apr. 2, 2008), also allowed the plaintiff to search the defendant's CEO's laptop. In *Treppel*, the plaintiff alleged that the defendant corporation and its employees were engaged in a "smear campaign" to defame him and destroy his career. During the course of the litigation, the plaintiff moved to compel the defendants to preserve ESI and respond to discovery regarding those preservation efforts and document management procedures.

Following the close of discovery and a protracted discovery battle, the court found that, despite assurances to the contrary, the defendants had not taken adequate measures to preserve ESI. The court stated that the defendants were tardy in instituting a comprehensive preservation plan, finding that Biovail had knowledge of the lawsuit even prior to service of the complaint. The court also took issue with the defendant's general counsel's efforts – or lack thereof – to instruct key players to preserve ESI, especially e-mails that were downloaded only to the CEO's laptop.

The defendant's general counsel was not able to show that he actually instructed the key players to preserve the ESI at issue, nor was he able to show that he followed up with the key players to ensure that they were in fact preserving the materials. While the court declined to issue an adverse inference jury instruction, it did order the defendants to restore and search five of 18 backup tapes and also allowed a forensic search of the CEO's laptop at the defendants' expense.

In fact, courts have gone so far as to order a party to issue a litigation hold. In *Board of Regents of University of Nebraska v. BASF Corp.*, 2007 WL 3342423 (D. Neb. Nov. 5, 2007), the defendants moved the court to compel the plaintiffs to produce all "development" documents. In this patent and licensing litigation, the court had previously ordered the plaintiffs to produce certain development documents as requested by the defendants. The plaintiffs produced nearly 13,000 pages of documents in response thereto, 11,000 of which were produced shortly before the close of discovery.

This led the defendants to renew their motion to compel. The e-Discovery violation came to light when one witness testified at deposition that his original search had only covered his hard copy and not his electronic files. This witness also revealed that during and independent of the litigation, the plaintiff had switched from a central archiving system to an "individual user" archiving system for ESI, including e-mail, under which the individual user determined which materials to keep and which to delete. At no point during the litigation did the plaintiff or its counsel explicitly instruct the key players to preserve or search for ESI, nor did they issue a litigation hold. The court found that counsel have a duty to direct their client to conduct a thorough search and to follow up to ensure that all relevant materials in the client's custody and control are produced.

The court went on to state that this duty is heightened when under court order to search for and produce discovery. The court issued remedial sanctions, which included re-searching "all of the files, including electronic files" pursuant to the court's orders, having employees and counsel swear to the methods, means and completeness of the searches, offering certain key players for re-deposition, and immediately issuing a litigation hold – all at the plaintiff's sole expense. The court also awarded attorney's fees and costs associated with the discovery dispute.

Based upon the e-Discovery jurisprudence to date, best practices dictate that counsel issue a litigation hold and supervise the discovery process. This means that counsel for corporate litigants should also personally and physically follow-up with affected personnel to ensure that they comply with the litigation hold and save and produce all discoverable data. In addition, counsel must obviously work with corporate IT personnel to ensure that electronic documents are not destroyed and that they are properly preserved.

b. Production or discovery of the litigation hold

The fear of having the client be required to produce the actual litigation hold letter during discovery should not deter counsel from issuing the hold. In a recent automotive product liability case, *Capitano v. Ford Motor Co.*, 831 N.Y.S.2d 687 (N.Y. Sup. Ct. 2007), the plaintiffs sought production of defendant's "suspension orders" – the defendant's version of a litigation hold – after determining through other means that the defendant had not produced certain documents during discovery. The plaintiffs claimed that if they had access to the "suspension orders" they would be able to determine if the missing documents in question were intentionally or negligently destroyed, or perhaps secure information which may lead to the discovery of the missing documents.

The defendant argued that the suspension orders were not relevant, and even if they were, that they were protected from discovery by the attorney-client privilege and/or attorney work product doctrine. The defendant submitted an Affidavit from an attorney in its legal department who explained that the suspension orders were "communications (a) that are issued by attorneys in Ford's Office of the General Counsel in connection with certain anticipated or pending litigation or administrative proceedings and (b) that identify attorney-selected categories of documents required to be maintained beyond periods set out pursuant to Ford's records management programme."

The attorney further explained that the suspension orders were confidential communications between the attorneys and Ford's representatives, were disseminated to

only those employees who deal with Ford's record management programme, and contained the warning that the "suspension orders" were privileged and confidential and that dissemination should be limited to persons working at Ford on a need-to-know basis. The plaintiffs countered by offering the deposition testimony of another Ford attorney who, in an unrelated case, stated that Ford's suspension orders were posted on Ford's intranet communications system and were available to all employees. Based thereupon, the plaintiffs argued that the defendant had waived any attorney-client privilege.

Although the court agreed with the plaintiffs that the requested "suspension orders" may lead to the production of admissible evidence and were, therefore, relevant, it denied the motion. The court concluded that the suspension orders were attorney-client privileged communications protected from discovery under N.Y. Civil Practice Law § 4503 (2007). It did not reach the issue of whether the "suspension order" constituted attorney work product.

In another case, a court reached the same result, though it found the "litigation hold" irrelevant but protected. In *Gibson v. Ford Motor Co.*, 2007 WL 41954 (N.D. Ga. Jan. 4, 2007), the plaintiff moved to compel the production of the defendant's "suspension order." The court found that the document did not have to be produced since litigation holds likely constitute attorney work product, often are overly inclusive, and the documents they list do not necessarily bear a reasonable relationship to the issues in litigation.

The court also feared that compelled production could have a chilling effect and "dissuade other businesses from issuing such instructions in the event of litigation" and that "[i]nstructions like the one that appears to have been issued here insure the availability of information during litigation. Parties should be encouraged, not discouraged, to issue such directives."

As e-Discovery jurisprudence develops, however, not all courts are convinced of the privileged nature of "litigation hold" letters. In any case, these privileges are not absolute. In the case *In re eBay Seller Antitrust Lit.*, 2007 WL 2852364 (N.D. Cal. Oct. 2, 2007), the court held that though the defendant need not produce copies of its "document retention notices" (DRNs), the plaintiffs were entitled to inquire into the *facts* as to what the employees who had received the DRNs had done in response. The court found that the defendant met its burden of showing that the contents of the DRNs may be protected by either the attorney-client privilege or the attorney work product doctrine.

In this case, the parties had previously agreed to conduct a corporate witness deposition to clarify the defendant's ESI preservation and collection efforts. Nonetheless, the court allowed further discovery on exactly that issue and as to the DRNs. The court ordered the defendant to reveal the names and job titles of the 600 employees who had received the DRNs and found that the plaintiffs were entitled to know what the defendant's employees were doing with respect to collecting and preserving ESI. The court also found it appropriate to discover what those employees were *supposed* to be doing.

Ultimately, the court held that the plaintiffs were entitled to know what kinds and categories of ESI the defendant's employees were instructed to preserve and collect, and

what specific actions they were instructed to undertake to that end. In fact, the court expressed hearty scepticism that the DRNs were privileged at all. In light of its other rulings to conduct further discovery, however, it ultimately did not reach the privilege issue. It remains to be seen how other courts will balance and weigh the privilege issues surrounding the litigation hold letter.

As shown above, the failure to implement proper document retention procedures and programmes can have drastic consequences in litigation in the e-Discovery context. However, the exact scope of the duty to preserve is not entirely clear. Courts and others differ on the types of information subject to preservation and potential production.

6. Data, data everywhere: what is a "document" in e-Discovery?

A "document" in the e-Discovery context clearly includes an e-mail or a word processing document – but what about the associated document properties, i.e. drafts and various versions of the document? The terms active data, ambient data, archival data, backup data, deleted data, distributed data, fragmented data, legacy data, metadata, migrated data, near-line data, off-line data, and residual data are all used to describe ESI or certain aspects of ESI. Some of the above may be discoverable; some may not.

For example, in *In re Vioxx Prods. Liab. Litig.*, 2005 WL 756742 (E.D. La. Feb 18, 2005), the court in a multi-district litigation ordered all parties to preserve relevant evidence, including "writings, records, files, correspondence, reports, memoranda, calendars, diaries, minutes, electronic messages, voice mail, e-mail, telephone message records or logs, computer and network activity logs, hard drives, backup data, removable computer storage media such as tapes, discs and cards, printouts, document image files, Web pages, databases, spreadsheets, software, books, ledgers, journals, orders, invoices, bills, vouchers, checks statements, worksheets, summaries, compilations, computations, charts, diagrams, graphic presentations, drawings, films, charts, digital or chemical process photographs, video, phonographic, tape or digital recordings or transcripts thereof, drafts, jottings and notes, studies or drafts of studies or other similar such material."

The court also ordered the preservation of "[i]nformation that serves to identify, locate, or link such material, such as file inventories, file folders, indices, and metadata." The *Vioxx* court noted that the parties had to take reasonable steps to preserve the relevant information until they agreed to a preservation plan or until the court ordered otherwise.

In the UK, pursuant to the UK Practice Direction 2A1, the definition of a document "extends to electronic documents, including e-mail and other electronic communications, word processed documents and databases. In addition to documents that are readily accessible from computer systems and other electronic devices and media, the definition covers those documents that are stored on servers and backup systems and electronic documents that have been ‘deleted’. It also extends to additional information stored and associated with electronic documents known as metadata."

Though the Practice Direction includes a list of factors relevant to determine the final scope of e-Discovery, the definition of "document" under the Civil Procedure Rules has arguably been expanded to include as discoverable information that would not commonly be referred to as a "document": Metadata is fair game[7] – or so it would seem.

But what is metadata? Metadata is fundamentally different from electronic and printed documents. All the information in a paper document is displayed on its face, which is not the case for electronic documents where its history is preserved in metadata. Paper shows what a document says or looks like; metadata can reveal where the documents went and what was done to it there – and by whom. Clients and counsel must be aware of and prepared to confront any embedded information and they must do so in a timely fashion. While metadata may arguably be relevant in some cases, in most cases it is not.

The seminal metadata production case remains *Williams v. Sprint/United Mgmt Co.*, 230 F.R.D. 640 (D. Kan. 2005) (*Williams I*). In *Williams I*, the court held that "[w]hen the Court orders a party to produce an electronic document in the form in which it is regularly maintained, i.e. in its native format or as an active file, that production must include all metadata unless that party timely objects to production of the metadata, the parties agree that the metadata should not be produced, or the producing party requests a protective order." *Williams I* was an employment class action involving alleged age discrimination.

The plaintiffs had requested "active" electronic versions of Microsoft Excel spreadsheets so that they would be able to determine if the documents "had any actual other columns or types of information available on a spreadsheet." After a protracted discovery battle, the defendant produced electronic versions of the spreadsheets. After reviewing the spreadsheets, the plaintiffs claimed that the defendant "scrubbed" the spreadsheet files to remove metadata, failed to produce a log of the information scrubbed, and "locked cells" and data on the spreadsheets, which prevented the plaintiffs from accessing those cells and electronically searching and sorting the data in them.

The defendant in *Williams I* admitted that it had scrubbed metadata and either redacted or locked certain cells and data, but argued that not only was the metadata irrelevant and certain redacted information privileged, but it also argued that the plaintiffs had never requested production of the metadata. In addition, the defendant claimed that it had acted in good faith, that its modifications were designed to prevent the plaintiffs from discovering information that the Magistrate judge had ruled undiscoverable, and that the modifications served to maintain data integrity. The court ultimately chose not to sanction the defendant, but it ordered the defendant to produce "unlocked" versions of the spreadsheets with the metadata intact.

The metadata discovery battle continued in *Williams v. Sprint/United Management Company*, 2006 WL 3691604 (D.Kan. Dec. 12, 2006) (*Williams II*). The defendant eventually produced the unlocked spreadsheets in native format, but the plaintiffs returned to the court a year later and argued that they could not match the over 11,000 e-mails produced with the respective spreadsheet. They moved to compel the production in native format of all 11,000 e-mails produced that transmitted spreadsheets.

The Magistrate judge ultimately held that since the plaintiffs had already received the e-mail production in one format (paper), the amended Federal Rule 34(b)(iii) protected the defendant from having to produce them again in another format (native).[8]

Further cases to date tend to affirm the notion that absent a showing of a compelling need and/or a timely agreement to the contrary, a court will not order the regular production of metadata.[9] As the courts gain further experience with ESI, they are beginning to deal with its varied forms and complexities.

Text messages. In *Flagg v. City of Detroit*, 2008 WL 787061 (E.D. Mich. Mar. 20, 2008), the court allowed the discovery of certain text messages exchanged between defendant's employees who the plaintiff accused of delaying the investigation into his mother's murder and concealment of evidence. In its opinion, the court set forth a detailed protocol for preserving, retrieving and reviewing the text messages for discoverability prior to production to the plaintiff.

RAM. In *Columbia Pictures, Inc. v. Bunnel*l, 245 F.R.D. 443 (C.D. Cal. 2007), the court ruled that Random Access Memory is "stored", no matter how briefly, and therefore ESI under the plain meaning of Rule 34 and ordered the production of information held in RAM on the defendant's servers. The court cited the Advisory Committee's Notes to Rule 34, which call for an expansive reading of ESI, intending it to cover data stored "in any medium from which information can be obtained". The court also rejected the defendant's invocation of international law in this copyright infringement action. In this case, the servers were situated in the Netherlands, where EU and Dutch national law purportedly prohibit US courts from ordering discovery.

The court held that Dutch law cited by the defendants, The Netherlands Personal Data Protection Act and the case *BREIN Foundation v. UPC Nederland B. V.*, only prohibit the production of "identifying information", not all information and not the information sought in that case – anonymous Server Log Data, including IP addresses. The District Court further agreed with the Magistrate Judge's finding that "foreign blocking statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce (let alone preserve) evidence even though the act of production may violate that statute."[10]

Cache. Finally, in *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey*, 497 F.Supp.2d 627 (E.D. Pa. 2007), the court rejected the plaintiff's claim that the defendant law firm spoliated ESI when it failed to preserve its computer's cache containing the "screen shots" of the plaintiff's archived webpage that the law firm had pulled up using the "Wayback Machine" in its defense of one of its clients. The court found the preservation of information stored in a computer's temporary cache files "impractical" and rejected the request for sanctions. The defendants prevailed in that case and were ultimately awarded US$ 9,000 in costs.

The international practitioner can expect further rulings on these and other matters of first impression as courts continue to confront with these and other novel e-Discovery issues. But not only must courts confront these issues, but companies, their counsel and their service providers must continue to do so as well.

7. e-Discovery vendors: so who can we count on to help us get through e-Discovery?

As the discovery practices evolve with technology and e-Discovery becomes more prevalent, the effective practice of e-Discovery often requires the services of an e-Discovery vendor. In the past few years, the legal community has seen a rapid proliferation of e-Discovery vendors and service providers that assist counsel and clients in obtaining and managing electronic data prior to and during litigation. The vendor works with the client's counsel and IT staff to ascertain where documents are stored, in what format they are stored and how the data can be retrieved in a way that does not change it.

In addition, the vendor generally has access to equipment and personnel that allow legacy data from dormant e-mail, word processing and other systems to be read and retrieved. Vendors convert the data into a format that allows attorneys to review and produce it. Many vendors and service providers often provide additional consulting services and even assist in selecting search terms or perform the first review and filtering of documents. Often an e-Discovery vendor is essential to properly assess and budget, harvest, filter and format ESI for production.

The production of electronic documents and data is now part of the US litigation culture. Cost-effective managing of the harvesting, review and production of such information requires careful selection of e-Discovery vendors. Failure to do so can lead to costly and time-consuming conflicts between lawyer and client.

In the recent past, marquee law firms, vendors and clients have become embroiled in public finger-pointing and even litigation regarding the services rendered. Often the allegations include trading blame for the under- or over-inclusive production of ESI, delays leading to the inability to comply with court deadlines, and allegations of overcharging. Technical glitches in e-Discovery software have cost attorneys, clients and the courts hours of valuable time and thousands in resources.[11]

In litigation today, e-Discovery vendors are performing services that go beyond mere litigation support. External lawyers and clients ultimately need to keep in mind that they will often be held responsible for mistakes by third-party vendors.

8. Proportionality and costs: shifting and sharing the benefits and burdens

The burden of preserving, collecting, preparing, reviewing, and producing electronic documents and data during civil litigation is clearly immense. Traditionally, discovery rules outside of the US foresee that the party seeking the discovery bears the cost of production. In the US, the costs are presumed to fall on the producing party.

The e-Discovery amendments to the US Federal Rules do not change that regime, but instead rely on a two-tiered approach to the production of electronic information: Under

Rule 26(b)(2)(B) "[a] party need not provide discovery" of ESI "from sources that the party identifies as not reasonably accessible because of undue burden or cost." The burden is on the producing party to show that it falls into this category. Otherwise, case law continues to govern cost-shifting in US e-Discovery.

Increasingly, courts are showing a willingness to pass to the requesting party the burdensome costs of producing e-Discovery.

In Australia, for example, prior to the 1998 Federal Court judgment by Justice Sackville in the case *BT (Australasia) Pty Ltd v. State of New South Wales & Anor* (No. 9) [1998] 363 FCA, the retrieval and analysis of electronic files was accepted as being too costly and challenging a task for Australian litigants to be required to undertake. In his finding that Telstra failed to comply fully with its electronic data discovery obligations, the judge scathingly rejected that view.

Justice Sackville stated that "[he] accept[ed] and appreciate[ed] that the purpose of making and retaining the backup was essentially disaster recovery, rather than archival. Nonetheless, as subsequent events have demonstrated, it is feasible, albeit difficult and expensive, for the tapes to be restored and a review process set in place to identify discoverable material. The fact is that the tapes do contain much material that is relevant to the issues in the proceedings, even though it is technically difficult to retrieve and the task of review is time consuming."

The message to Australian lawyers was clear: electronic document discovery may be onerous, costly and time consuming, but there is no excuse for not doing it. Since that time, electronic discovery in Australia has become widely accepted, with the Australian Federal Court Rules now defining document to include any material data or information stored by mechanical or electronic means.[12] Clearly, Australian litigants are expected to bear and have borne significant costs related to e-Discovery and can, as is the case in traditional discovery, seek a cost order from the court to shift the burden of producing electronically stored information.

In cost-shifting cases in the US, courts routinely relied on the eight factor test articulated in *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*, 205 FRD 421 (2002), or the seven factor test from *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309 (S.D.N.Y. 2003) (*Zubulake III*). More recently, courts are tending to employ the Advisory Committee Notes to the US Federal Rules e-Discovery amendments.

In *Rowe*, the court shifted all e-Discovery production costs to the plaintiff, except the defendants' search of their own materials for privileged e-mails, finding that although the plaintiff could not obtain the information by other means, the plaintiff's discovery requests were very broad and the plaintiff had not been able to prove that the discovery of e-mail would be a "gold mine" of relevant information. In Rowe, a group of concert promoters had sued several talent agencies for allegedly freezing them out of the market for promoting certain events.

The plaintiffs had moved to compel the production of all documents, including e-mail, concerning any communication between any of the defendants relating to the selection of concert promoters in the course of its business. The William Morris agency alone estimated that it would cost approximately US$ 9,750,000 to fulfil the plaintiffs'

discovery request. In reaching its decision, the court employed an eight-factor balancing test.[13]

The test set forth in *Zubulake III* makes it more difficult to shift costs to the requesting party than under Rowe. The court in *Zubulake III* even criticised the approach set forth in Rowe for making it too easy to shift costs back to the requesting party, asserting that "there is little doubt that the *Rowe* factors will generally favour cost-shifting" and called the Rowe approach "incomplete."

Zubulake III adopted a three-step analysis, which incorporated some of *Rowe*'s eight factors. Step #1 is to determine whether cost-shifting is even an appropriate consideration. Step #2 requires a factual showing to support shifting the cost of production to the requesting party. Specifically, the responding party must restore and produce a sampling of responsive documents from the inaccessible media.[14] The final step #3 in the *Zubulake III* analysis takes us to the seven enumerated factors.[15]

In addition to courts generally applying the Rowe and *Zubulake III* factors to determine accessibility and proportionality, another court relied on the Advisory Committee's Notes to Rule 26(b)(2)(B)[16] to conduct the balancing test and find the database in question not "reasonably accessible" under the rules. In *Best Buy Stores L.P. v. Developers Diversified Realty Corp.*, 247 F.R.D. 567 (D. Minn. 2007), a magistrate judge had ordered the plaintiff to restore and provide discovery from a database that the plaintiff had created for a prior case.

The database contained nearly all of the plaintiffs' existing ESI stored outside of its e-mail system and had been "downgraded" at some point during that litigation. In the case at issue, the defendants sought discovery from that database and the magistrate judge agreed, finding estimated restoration costs of US$124,000 and monthly maintenance costs of ca. US$27,800 – nearly one quarter of the total amount in controversy – "reasonable".

The district court, employing the Advisory Committee factors, disagreed and sustained the plaintiff's objection to restoring, maintaining and searching the database in the present litigation. Though the court agreed that the database would likely contain discoverable and relevant information, it nonetheless concluded that absent specific discovery requests or additional facts suggesting that the database was of particular relevance to the litigation, the plaintiff did not have a duty to continue to maintain the database. The plaintiff did not destroy potentially relevant evidence but merely "removed it from a searchable format", and since the defendant was not able to show good cause, the plaintiff need not restore and maintain the database.

Litigants, however, continue to seek access to electronic databases.

9. Direct access to corporate databases

Recently, plaintiffs and their counsel – especially those in product liability cases – ask that courts order corporate defendants to allow the plaintiff (and their expert IT and

other litigation consultants) direct access to corporate servers, databases and other electronic information. Some US trial courts – in unpublished decisions – have ordered corporate defendants to give a plaintiff direct, searchable access to certain databases on a case-by-case basis. However, to date, absent agreement from a corporate defendant or a showing of prior discovery violations, US courts have been very wary of giving a claimant such unfettered, unrestricted "live" access to a company's electronic servers.

For example, in *In re Ford Motor Co.*, 345 F.3d 1315 (11th Cir. 2003), a plaintiff alleged that a defectively designed seatbelt buckle caused her injuries. After serving extensive written discovery, the plaintiff filed a motion to compel to obtain direct access to two Ford databases in order to search for related claims; one database contained records of all customer contacts with Ford and the other contained records of contacts by dealers, personnel and other sources. After the trial court granted the motion, Ford sought review by the Court of Appeal. In rejecting the trial court's grant of direct access, the court stated: "Like the other discovery rules, Rule 34(a) allows the responding party to search his records to produce the required, relevant data.

Rule 34(a) does not give the requesting party the right to conduct the actual search. While at times – perhaps due to improper conduct on the part of the responding party – the requesting party itself may need to check the data compilation, the district court must 'protect respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs'".[17]

10. Sanctions for failures and non-compliance

Under Federal Rule 37(e), a party is exempt from sanctions for the failure to provide electronically stored information lost as a result of the "routine, good-faith operation of an electronic information system" – "[a]bsent exceptional circumstances." It remains to be seen exactly what those circumstances are, but past cases can provide guidance.

Even prior to the amendments to the Federal Rules, a variety of sanctions were and continue to be available for the failure to comply with e-Discovery, both against the non-responsive party and its counsel. Courts have issued sanctions for the failure to have a document retention policy, the failure to issue a litigation hold, the failure to enforce the retention policy or litigation hold, and the failure to produce e-Discovery, including in the form requested or agreed to.

The following are examples of the sanctions issued in recent e-Discovery disputes.[18]

At the first trial of this product liability case, Hyundai Motor America v. Magana, 170 P.3d 1165, (Wash. App. Oct. 30, 2007), the jury awarded plaintiff over US$ 8 million in damages for injuries sustained after being ejected out of the hatchback of a 1996 Hyundai Accent during a 1997 accident. The defendant appealed liability but not damages, and the case was remanded for a second trial on the issue of liability. During preparations for the second trial, the plaintiff filed a motion to compel the production of documents relating to "other similar incidents".

The court granted the motion, and ordered the defendant to produce "Police Reports, legal claims, consumer Complaints and Expert Reports or Depositions and Exhibits and photographs thereto with respect to all consumer complaints and lawsuits involving allegations of seatback failure on all Hyundai vehicles with single recliner mechanisms regardless of incident date and regardless of model year".

At the deadline for complying, the defendant motioned the court for relief from the order, requesting that it be permitted to produce only those responsive consumer complaints that were maintained on its current computer system, and that it not be required to restore some 96 backup tapes which were believed to contain original data from its old mainframe computer. The defendant explained that its Consumer Affairs Department was responsible for handling consumer contacts and inquiries, and that prior to its conversion to a new computer system, Consumer Affairs files were kept on the mainframe for 12 months.

If there was no activity on the file for 12 months, it was moved to an "inactive" table, but still on the mainframe. If there was then no activity for 12 months thereafter, the file would be converted to a backup tape. The defendant stated it had located a total of 96 backup tapes dating from mid-1995. The defendant further explained that existing backup tapes were not converted into the new computer system; thus, they would need to restore the tapes and then access the data – at an estimated cost of at least US$ 24,000. The plaintiff opposed the motion and argued that the defendant's failure to convert the tapes containing consumer complaints amounted to spoliation, and that an adverse inference instruction should be given to the jury.

The court denied the defendant's motion for relief and also denied the plaintiff's motion for spoliation sanctions. Two months later, however, the court granted the plaintiff's motion for default judgment based upon the defendant's failure to produce the evidence regarding other similar claims and incidents as ordered. The court had held a four-day evidentiary hearing on the motion for default judgment and concluded that the defendant and its counsel committed numerous discovery violations, "which were wilful, deliberate, direct and egregious".

The defendant apparently had not searched its Consumer Affairs Department's electronic records for responsive documents; its search was limited to the legal department's records and no effort was made to search beyond the legal department, as this would have required an "extensive computer search" and presumably a search of the 96 backup tapes. The court found no legal basis for limiting the search for responsive documents to those available in the legal department, noting that the legal department worked closely with the Consumer Affairs Department to handle customer complaints and claims, including product liability claims.

In some instances, the Consumer Affairs Department would even refer a claim to the legal department, which directed an investigation of the claim and/or provided direction to Consumer Affairs regarding the claim. All such records were maintained in the Consumer Affairs Department. The defendant's attorney in charge of the products liability section of the legal department testified that he was familiar with this process and supervised attorneys involved in this process. The court found that a search limited to the corporate legal office, which did not seek or disclose records from claims which

originated with the Consumer Affairs Department, even though many of the claims involved the legal department, was not a diligent search.

The defendant had the obligation not only to diligently and in good faith respond to discovery efforts, but to maintain a document retrieval system that would enable the corporation to respond to the plaintiff's requests. The court noted that the defendant is a sophisticated multinational corporation and experienced in litigation. It found that a search of computer records for documents requested by the plaintiff, even if voluminous in nature, is standard operating procedure for attorneys practicing in the products liability field. In fact, the defendant did not object to the request as burdensome. The false answers given due to the failure to search the Consumer Affairs Department were without reasonable excuse or explanation. The defendant and its counsel knew that there had been customer complaints and claims of incidents of seat back failure.

The defendant knew that these happened in the Accent and Elantra, as well as other vehicles. Some of these complaints had been litigated and most involved personal injuries. It was the defendant's duty to establish an adequate system to respond to discovery requests. The defendant failed to establish such a system and failed to respond accurately to discovery requests. The defendant unreasonably limited its search, and failed to supplement those answers that were incorrect. The court discussed the other sanctions available, and concluded that nothing short of default judgment was appropriate. The court entering default judgment reinstated the jury's damage award of US$8,064,055. In a separate opinion, the court also awarded the plaintiff the attorneys' fees and costs occasioned by the discovery violations.

The defendant appealed. On appeal, the court agreed that the manufacturer wilfully violated the plaintiff's discovery requests, but that the trial court abused its discretion in granting the default judgment. The court cited the plaintiff's tactics and strategy in preparing for the second trial, including the plaintiff's request to supplement discovery four months prior to the hearing date and five months after the remand and its request to amend its pleadings one week prior to the hearing date, as indicia that it did not suffer prejudice – claiming that the plaintiff himself argued that he could not proceed to trial without further examining and exploring other materials recently produced. Stating that "the purpose of the trial process is to uncover the truth", the court reversed the default judgment and remanded the case for trial, or further discovery as necessary.

In *In re Seroquel Prods. Liab. Litig.*, 2007 WL 2412946 (M.D. Fla. Aug. 21, 2007), the plaintiffs motioned the court to impose sanctions on the defendant for failing to timely comply with discovery obligations, even after the entry of an agreed case management order and a stern warning from the court to comply with it. The plaintiffs pointed out at least four instances where the defendant failed to produce documents in an accessible or useable format, in addition to missing numerous deadlines. While the court found two of those instances to be excusably negligent, the court found the defendant's failure to adequately identify relevant databases and persons knowledgeable about the databases in violation of the CMO and sanctionable under Rule 37.

The court stated that "[i]dentifying relevant records and working out technical methods for their production is a cooperative undertaking, not part of the adversarial give and take. … It is not appropriate to see an advantage in the litigation by failing to cooperate in the identification of basic evidence". The court found the defendant's actions in this

multidistrict product liability litigation "purposely sluggish" and cited a number of specific failings by the defendant, including: the use of a plainly inadequate key word search, the failure to provide attachments, and the omission of relevant emails, and what it described as "woefully deficient" efforts to prevent and solve technical problems – which included the production of a large number of blank pages, load files that were not searchable, and the absence of page breaks arguable required by the order.

While the defendant blamed many of the technical problems on errors made by its e-Discovery vendor, the court, citing the Sedona Principles, stated that a party is responsible for the errors of its vendors. The court also concluded that the defendant did not perform the requisite quality control oversight to ensure that such problems with the production did not occur.

The court found that the defendant should have allowed the parties' respective technical staffs to consult to resolve the issues sooner and at less expense. The court concluded by finding the defendant's failure to timely produce "usable" or "reasonably accessible" documents sanctionable, stayed the determination of which sanctions to impose to allow the plaintiffs an opportunity to present evidence as to their damages or prejudice.

In a recent case involving a claim of wrongful termination of disability benefits, *Finley v. Hartford Life and Acc. Ins. Co.*, 2008 WL 509084 (N.D. Cal. Feb. 22, 2008), the plaintiff sought sanctions against the defendant and its counsel for the untimely production of a surveillance video, arguing that the delay in production required additional expert and deposition expenditures. The defendant had produced certain electronic surveillance materials in its initial disclosures, but failed, due to an "administrative oversight", to produce a video of the plaintiff in her kitchen.

Upon discovery of the oversight, the defendant produced the video and argued that its initial search was reasonable. In collating the initial disclosures, the responsible administrative assistant failed to search the "old database", as the defendant's policy required, so the video was not discovered, even though it was not lost or misplaced. The court found it "unreasonable for the defendant to rely on a system which contained so few checks and balances that the mere fact that an administrative assistant did not look for a file, in the filing cabinet where that file was normally kept, could undermine the entire initial disclosure apparatus. The file was where it was supposed to be.

It was unreasonable for the defendant not to find it there at the point of its initial disclosures." The defendant failed to make a "reasonable inquiry" as required by Rule 26(g), and thus the court sanction the defendant, but did not sanction its outside attorneys. Since the defendant's attorneys relied, however erroneously, on the defendant's defective search methods, the court found that they were negligent but did not act in bad faith in certifying the discovery. The court ordered the defendant to pay US$9,000.

In the patent infringement suit, *Qualcomm Inc. v. Broadcom Corp.*, 2008 WL 638108 (S.D.Cal. Mar 05, 2008), during one of the last days of trial, the plaintiff's employee mentioned certain potentially relevant and discoverable e-mails during cross-examination. A junior associate working for the plaintiff's outside counsel had recently discovered these e-mails during search of the employee's laptop. He had conducted the search during trial ten days prior to the witness' testimony and apparently found 21 e-

mails from the relevant time period during the search. Apparently, in consultation with more senior trial counsel, the attorney deemed the e-mails not "relevant" and did not produce them to the defendant.

They also allegedly neither informed lead trial counsel, nor the plaintiff of the discovery of the e-mails. During the trial, the lead trial counsel consistently insisted to the court, also pursuant to the witness' earlier deposition testimony, that no further relevant, discoverable e-mails were available. Once revealed during the trial, the defendant sought discovery of these and other e-mails and documents. The plaintiff conducted a search and produced 46,000 additional documents (which amounted to over 200,000 pages of new materials), leading the court to call the 21 e-mails "the tip of the iceberg" in the plaintiff's attempt to conceal hundreds of thousands of relevant and exculpating documents – documents that ultimately defeated the plaintiff's case.

The defendant sought sanctions. The court agreed that sanctions were warranted, finding that the defendant's failure to conduct basic searches prior to trial amounted to the intentional withholding of documents. The court denied the plaintiff's claim that outside counsel should have given more guidance and should have more closely supervised the scope of the pre-trial searches, though it still found fault with external counsel's behaviour. The court stated: "Qualcomm is a large corporation with an extensive legal staff; it clearly had the ability to identify the correct witnesses and determine the correct computers to search and search terms to use. Qualcomm just lacked the desire to do so."

The court found that the plaintiffs committed "monumental and intentional" discovery violations for failing to produce thousands of documents requested in discovery. The court ordered fourteen internal and external counsel to appear at a hearing to show cause as to why sanctions should not be imposed. The court imposed monetary sanctions of US$8,568,633.24 on the defendant, but did not impose monetary sanctions on outside counsel. Stating, however, that "[a]ttorneys must take responsibility for ensuring that their clients conduct a comprehensive and appropriate document search", the court referred six of the defendant's outside lawyers to the California Bar for investigation of ethical violations.

The court also ordered the outside attorneys and the defendant's employees and in-house counsel to participate in a "Case Review and Enforcement of Discovery Obligations" or CREDO programme. The court believed that participation in this programme may deter future discovery misconduct by providing a "road map" to assist in understanding ethical obligations during the discovery process as well as establish a turning point for increased ethical conduct in the practice of law. In April 2008, the attorneys were still conducting the CREDO programme.

Initially, the magistrate judge had refused to pierce the client's attorney-client privilege based on the self-defense exception, as the outside attorneys requested. However, during the many hearings and the court's many attempts to resolve these issues and this case, the plaintiff paid the entire amount of sanctions, and in defending its own conduct, made declarations creating an adversarial relationship between the client and its former attorney. The court reversed the magistrate's judgment in part and remanded it, instructing the court to allow the outside attorneys to fully defend themselves against their (former) client.[19]

Finally, further developments in the well-known *Morgan Stanley* case are worth mentioning. Please recall that in Coleman (Parent) *Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 679071 (Fla. Cir. Ct. Mar. 1, 2005), a jury awarded the plaintiff more than US 1.5 billion following an adverse inference jury instruction based on Morgan Stanley's practice of overwriting e-mails every 12 months (in violation of federal regulations that required the firm to retain e-mails for two years). In addition to overwriting e-mails, the defendant failed to produce backup tapes, failed to conduct court ordered searches for documents, and failed to produce responsive documents in a timely fashion – all of this after having served a sworn notice of compliance with the court's e-Discovery Order.

At the time of issuing its certification of compliance, the defendant was still in possession of more than 1,400 backup tapes containing data not yet processed or produced.[20] In March 2007, the Florida state appellate court reversed the US$1.58 billion judgment against Morgan Stanley, in Morgan Stanley & Co., Inc. v. Coleman (Parent) Holdings, Inc., 2007 WL 837221 (Fla. App. 4th Dist. Mar. 21, 2007), on the grounds that the plaintiff failed to prove compensatory damages. In December 2007, the Florida Supreme Court denied review and indicated that no motion for rehearing would be entertained. The appellate courts never reached the e-Discovery issues in their review of the case.

As can be seen from the above examples, the law on sanctions for e-Discovery abuse continues to develop and warrants close monitoring and consideration of internal policies before and during the conduct of litigation.

11. International aspects of e-Discovery

Though not as fully developed, the jurisprudence on the international aspects of e-Discovery is gaining in practical importance. Not only can US e-Discovery potentially reach international corporations when the entity is a direct party to an action, but it can also in theory reach non-US parent and subsidiary corporations and affiliates not directly involved in the litigation. Though international choice of law and evidence-gathering treaty restrictions apply, some attorneys are arguing (sometimes successfully) that e-Discovery requests can and do reach beyond US borders.

For example, a federal magistrate judge invited the imposition of discovery sanctions against the Kingdom of Spain, holding that it had failed to meet its obligations under the US Federal Rules to preserve and produce electronic documents and e-mail. *See Reino de Espana v. Am. Bureau of Shipping*, 2006 WL 3208579 (S.D.N.Y. Nov. 3, 2006). The *Reino De Espana* decision shows that litigants – even foreign governments – must be prepared to address the preservation and potential discovery of e-mail and other ESI, not just during discovery, but perhaps well before litigation actually commences, regardless of where the discoverable information might be found.

The case arose from the casualty of the ship *Prestige* and the resulting oil spill off the coast of Spain. Initially, the defendant served a wide-ranging document request on the plaintiff, the Spanish government, requesting the production of e-mail and other ESI

created around the time of the accident from over a dozen different Spanish government agencies. After the defendant complained that the plaintiff's initial production of electronic documents was deficient, the plaintiff promised to produce all non-privileged responsive electronic records.

Thereafter, the defendant narrowed its request, requesting production of e-mail and electronic documents from 98 individuals and fifteen government e-mail addresses. In response, the plaintiff produced only 62 e-mails. The defendant filed a motion to compel, asserting that the plaintiff had either destroyed or failed to adequately preserve relevant electronic information. The plaintiff countered that the electronic records sought by the defendant simply did not exist.

The court held an extensive evidentiary hearing regarding the plaintiff's e-mail systems before ruling that the electronic records at issue had likely existed at one point, but that the lack of electronic document production resulted from the plaintiff's failure to locate, preserve, and produce electronic evidence in accordance with its obligations under the US Federal Rules even prior to the e-Discovery amendments coming into force. The court granted the defendant's motion to compel and directed the defendant to apply for an appropriate sanction.

The court's key rulings included the following:

- The court rejected the plaintiff's argument that the document request was overbroad and described the defendant's narrowed request for a search of 98 individual e-mail accounts and 15 government e-mail addresses as "targeted and focused." The plaintiff had proposed a limitation of discovery to two specific agencies, but the court rejected this proposal and took a very broad view of the proper scope of discovery. The Spanish agencies were apparently not connected to a single, centralised server, meaning that a search for discoverable records would require the plaintiff to search individual computers and e-mail accounts. Still, the court found that such efforts were required under the US Federal Rules.
- The court also appeared to require a prompt and proactive approach to document preservation in the international context. According to the court, the Spanish Merchant Marine should have conducted "a diligent discovery search of all possible sources from the onset," instead of relying upon voluntary disclosure and production of electronic documents by employees. The court described another Spanish agency's notice directing employees to voluntarily preserve records as "untimely," and noted with disapproval that the agency had failed to actively oversee the process. Moreover, the court indicated that the agency's normal document retention policy was insufficient to fulfil its discovery obligations, where under that policy "[i]ndividual users determine how long e-mails are preserved" and "[i]ndividual users are responsible for downloading their e-mails and electronic records, and storing them."
- The court also implied that a litigant – even a foreign one – should bear in mind its potential document retention obligations under the US Federal Rules, perhaps even before litigation actually commences. The court asserted that under the US Federal Rules, a litigant "is obliged to preserve relevant records" even in the absence of a document request specifically addressing the issues for preservation.

- Notably, the court disregarded the plaintiff's argument that Spanish and EU privacy laws prevented disclosure of the electronic documents at issue, stating that the litigation was brought in the Southern District of New York rather than Spain and noting that under the US Federal Rules it was "incumbent upon [the plaintiff] to identify and preserve relevant documentation related to its claims."

Regardless of whether or not sanctions for e-Discovery violations are ultimately imposed in the above case involving a foreign plaintiff, non-US companies doing business in the US as well as overseas dependencies of US corporations may well be subject to the new e-Discovery rules and standards should they be hailed in front of US courts. In the past, US courts have actively imposed the burden of global discovery on international litigants coming before them, despite fundamental opposition from both governments outside the US and their constituent companies.

On the other hand, for the foreign corporate defendant, ensuring that day-to-day business can continue uninterrupted and without undue burden is necessarily tantamount to their obligations related to discovery in a US product liability case. Unfortunately, international corporations would be ill-advised to simply ignore this new challenge.

Generally, opposition to global discovery is often based on legal and cultural differences that global practitioners and clients faced with the new, even more intrusive US e-Discovery regime must take into consideration. For example, the role of the judge and lawyer are often starkly different in common law versus civil law jurisdictions.

In common law jurisdictions, the judge acts as a neutral referee, and the attorneys take a more adversarial and proactive role in developing the case and moving it forward. In civil law countries, by contrast, one or more judges are often active in a case, determining what is discoverable and necessary for the prosecution of that particular case.

In addition, a number of civil law jurisdictions have privacy laws or even specific blocking statutes that prevent the transfer of certain information out of the jurisdiction – and to the US. Regardless of these statutes, many US courts will still expect and demand global discovery from internationally-acting parties to US litigation. The practitioner must therefore attempt the often difficult task of ensuring that US obligations are met in a product liability claim while at the same time not violating the laws of the place the discovery is sought.

This may require the personal consent of the author of e-mails, for example, or extensive filing and liaising with governmental agencies to ensure the proper and confidential treatment of "personal" data – which is, for example, often liberally construed by non-US courts to include any data identifying the person or his location.

Presently, no concrete, binding methods exist for obtaining e-Discovery outside of the US for use in US litigation. One method for obtaining discovery internationally is via the Hague Convention of March 18, 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, which provides the rules and procedures for obtaining evidence outside of one's home jurisdiction. A threshold questions is, of course, whether the country from which you are seeking discovery is a signatory to the Convention.

If so, the requesting party must strictly follow the specific procedures provided in order to request discovery via diplomatic channels. In addition, the requests must also strictly comply with local discovery rules, which may limit the information available, regardless of whether or not the country is a signatory. Further, there are no direct methods of enforcement.

In addition to the Hague Convention on Evidence, the international practitioner must also take into consideration privacy issues. For example, European Directive 95/46/EC prohibits the transfer of personal information outside of the EU unless the country receiving the information provides an "adequate level of protection" for individuals in the processing of personal information. The US is presently not considered to provide adequate privacy protections. These and other regulations may bar making a mirror-image of your non-US client's ESI and taking it to the US for segregation, preservation, review, and production. Often times, offering redaction *may* overcome privacy issues – but, for example, only if the affected party and your opponent agree.[21]

Though incumbent upon any practitioner, practitioners with a multi-jurisdictional, international practice should take special care to alleviate any such concerns. An international discovery request is likely to meet with greater success if accompanied by a degree of specificity virtually unknown in the US: One should attempt to identify what documents one wants from whom or face rejection at the border and the door of the party.

Practitioners should also be aware that web-based e-Discovery platforms may already violate some non-US data privacy and transfer laws. It simply may be illegal to transfer data to the US under current international privacy laws – and random "fishing" for information to support a claim may already violate such international civil and criminal laws and customs.

In addition, the international litigator will often also face language and other cultural barriers, exacerbated by the "new" terminology associated with e-Discovery. Many international corporations find the US pre-trial discovery process intrusive and burdensome. Many are not familiar with or prepared to deal with the adversarial nature of proceedings or the large-scale of discovery.

Effective e-Discovery practice on an international scale will necessarily require more time and effort in explaining to non-US clients why they need to accept and support effective e-Discovery – especially with respect to the many foreign employees who counsel will need to assist them in this important process.

For example, in issuing an effective litigation hold, non-US entities must take into consideration not only vastly different legal frameworks and traditions, but also different cultural norms and expectations. Cultural sensitivity and awareness can be of critical importance. And it goes without saying that any litigation hold must follow local laws regarding document retention and destruction. Further, employees may have privacy rights – whether real or perceived – via local law, a specific employment contract or through the works council to information on their employer-issued technical equipment, especially if the employer expects mobile (i.e., which may include after-hours and private) communication from and with its employees.

For example in Australia, the Workplace Surveillance Act of 2005 makes it illegal to monitor employee e-mail activity without prior notice to the employee unless the employer has a strong suspicion of criminal activity. Such laws add a new wrinkle to issuing a global litigation hold or even implementing an effective document retention and destruction policy. In addition, the efficient and effective use of e-Discovery technologies will require early consultation with clients and vendors, especially in countries not using the Latin alphabet, and will likely require a vendor with Unicode deduplication and "near duplicate" comparison capabilities.

And finally, in our zeal to represent our clients, it's often the most basic things that we forget – the international practitioner should also take into consideration local customs and holidays. It's not just efficient, best practices for managing a case, it's also simply the right thing to do.

12. Conclusion

International Electronic Discovery remains an exciting and constantly evolving aspect of product liability litigation worldwide that the international practitioner must take into consideration. Often times, it will be necessary to cooperate with or even engage local counsel to assist in overcoming the hurdles and understanding the nuances incumbent to International Electronic Discovery.

Though courts and other entities continue to develop concrete rules, case law and guidance on e-Discovery practice, much of the law in this area remains to be developed. As such, clients and counsel have to actively remain abreast of this ever-changing aspect of the modern, high-tech practice of law.

Endnotes

[1] During 2003 and 2004, Judge Shira A. Scheindlin of the US District Court for the Southern District of New York issued a series of six groundbreaking opinions in the case of *Zubulake v UBS Warburg*. The *Zubulake* decisions were the seminal rulings in the US on a wide range of e-Discovery issues, including:

- the scope of a party's duty to preserve electronic evidence during the course of litigation;
- a lawyer's duty to monitor their clients' compliance with electronic data preservation and production;
- data sampling;
- the ability for the disclosing party to shift the costs of restoring "inaccessible" backup tapes to the requesting party; and
- the imposition of sanctions for the spoliation (or destruction) of electronic evidence.

This article will not extensively treat but instead will attempt to take the reader beyond the *Zubulake* decisions in an attempt to describe the current state-of-the-law in the US on key e-Discovery subjects. Full legal citations were omitted in this Chapter for the sake of brevity. All law as stated herein is believed by the author to be current as of May 1, 2008.

[2] The amendment to Rule 16 requires the court to regulate e-Discovery via scheduling order and include any agreements reached by the parties. The amendments to Rule 26 require counsel to confront e-Discovery issues at the very earliest stages of litigation during an early meet-and-confer process. The amendments to Rule 33 contemplate a new cost-shifting scheme away from the burden being placed only on the producing party toward the parties sharing the burdens of production.

Rule 34 was amended to create a new category of electronic discovery separate from the categories "documents" and "things," an amendment which recognises the unique nature of ESI. Under Rule 34, a requesting party may specify the form of production and a responding party may object to the same. Ultimately, the responding party may produce the information in the form in which it is ordinarily maintained or in a reasonably usable form, meaning that the responding party must provide the tools necessary for the information and data to be accessed. The amendments to Rule 37 provide somewhat of a safe-harbour for a responding party – absent special circumstances, the court may not impose sanctions for the failure to provide electronically stored in formation destroyed as a result of the routine, good-faith operation of an electronic information system.

Though often overlooked, Rule 37 also provides for sanctions for failing to participate in good faith in the Rule 26 and meet and confer conferences required under the rules. Finally, Rule 45 allows federal judges to issue subpoenas specifically for electronic documents.

Please also note that as of December 1, 2007, the US Supreme Court renumbered the Rule 37 (f) "safe harbour" provision to Rule 37(e). That renumbering was the result of a multi-year effort to rewrite the rules to improve their "style." The Court made the revisions to "clarify and simplify" the rules "without changing their substantive meaning." No matter the Court's purported intent to not change the rules' meaning, the perhaps unintended effect was to at least change their emphasis in parts. *See e.g.*, Rule 26(f), which now places a greater emphasis on meeting in good faith to agree on a discovery plan, which the failure to do can lead to sanctions under new Rule 37(f). *Cf. In re Seroquel Prods. Liab. Litig.*, 2007 WL 2412946 (M.D. Fla. Aug. 21, 2007) (indicating that "identifying relevant records and working out technical methods for their production is a *cooperative undertaking*, not part of the adversarial give and take...." (emph. added).

[3] The District of Alaska, Eastern and Western Districts of Arkansas, the Northern District of California, the District of Colorado, the District of Connecticut, the District of Delaware, the Middle and Southern Districts of Florida, the Southern District of Georgia, the Central District of Illinois, the Northern and Southern Districts of Indiana, the Northern and Southern Districts of Iowa, the District of Kansas, the District of Maryland, the District of Missouri, the District of New Hampshire, the District of New Jersey, the Southern and Eastern Districts of New York, the Western District of North Carolina, the Northern and Southern Districts of Ohio, the Eastern, Middle and Western Districts of Pennsylvania, the Eastern, Middle and Western Districts of Tennessee, the Eastern, Northern and Southern Districts of Texas, the District of Utah, the District of Vermont, the Southern District of West Virginia, and the District of Wyoming all have

enacted local rules and/or guidelines dealing with e-Discovery. The Court of Appeals for the Ninth Circuit is also considering e-Discovery local rules.

[4] In order to address data privacy issues, the US and EU agreed to a self-certification process by which companies handling ESI from the EU agree to abide by certain principles for handling personal information and data, including ESI. Organisations that participate in the safe harbour must comply with the its requirements and publicly declare in writing that they do so.

The organisation must state in its published privacy policy statement that it adheres to the safe harbour and its requirements, including its notice, choice, access and enforcement provisions. The US Department of Commerce maintains a list of all organisations that file self-certification letters and makes both the list and the self-certification letters publicly available. Many e-discovery vendors have self-certified under the safe harbour regime.

[5] The Advisory Committee factors cited by the court are: (1) the specificity of the discovery request; (2) the quantity of information available from other and more easily accessed sources; (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources; (4) the likelihood of finding relevant responsive information that cannot be obtained from other, more easily accessed sources; (5) predictions as to the importance and usefulness of the further information; (6) the importance of the issues at stake in the litigation; and (7) the parties' resources.

[6] *But see Clearone Communications, Inc. v. Chiang*, 2008 WL 704288 (D. Utah Mar. 10, 2008), (declining to sanction a technology company for its failure to produce a "smoking gun" e-mail, a copy of which was produced by a co-defendant during discovery, where the non-producing defendant's regular e-mail system did not save copies of sent mail).

[7] In fact, readily-available on-line products such as Metadata Scrubber™, Doc Scrubber™, Metadata Assistant™, and Evidence Eliminator™ can be purchased and used to "cleanse" electronic documents of metadata. While the scrubbing of metadata is generally permissible outside of the context of a specific litigation, the scrubbing of metadata can constitute spoliation if the metadata is the subject of a litigation hold or otherwise discoverable in litigation. *See, e.g., Arista Records, LLC v. Tschirhart*, 2006 WL 2728927 (W.D. Tex. Aug. 23, 2006). *See also Elec. Funds Solutions v. Murphy*, 134 Cal. App. 4th 1161 (2005) (finding default judgment proper after a showing that defendants ran data scrubbing software during discovery).

[8] *Cf. PSEG Power New York, Inc. v. Alberici Constructors, Inc.*, 2007 WL 2687670 (N.D.N.Y. Sep. 7, 2007), infra at Endnote 11. In January 2007, the Magistrate judge explained his reasoning in not awarding sanctions against the defendant in the Williams case. *See Williams v. Sprint/United Mgmt. Co., 2007 WL 214320 (D. Kan. Jan. 23, 2007).*

[9] *See Autotech Techs. Ltd. v. Automationdirect.com, Inc.*, 2008 WL 902957 (N.D. Ill. Apr. 2, 2008) (holding that the plaintiff need not produce a word processing document in its "native format" with the metadata intact, where the plaintiff had produced the

document as a PDF and in hard copy and the face of the document itself included a "Document Modification History" and where the defendant neither specified the form of production nor did it request the production of metadata at the time of its initial requests); *D'Onofrio v. SFX Sports Group, Inc.*, 247 F.R.D. 43, 48 (D.D.C.2008) (holding that metadata need not be produced since the requesting party failed to specifically mention metadata in its original requests); *Kentucky Speedway, LLC v. Nat'l Ass'n of Stock Car Auto Racing, Inc.*, 2006 US Dist. LEXIS 92028, at *21-23 (Dec. 18, 2006) (ruling that Rule 34(b) does not require the production of metadata absent a showing of a particularised need, and the failure to raise the issue prior to production waives the opportunity to object: "[T]he issue of whether metadata is relevant or should be produced is one which ordinarily should be addressed by the parties in a Rule 26(f) conference.").

See also Wyeth v. Impax Lab., 2006 WL 3091331, at *2 (D. Del. Oct. 26, 2006) (ruling that production in native format was not required in the absence of foreseeable or necessary requirement for accessing metadata); *accord,* THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION, Principle 12, (July 2005), available at http://www.thesedonaconference.org ("Unless it is material to resolving the dispute, there is no obligation to preserve and produce metadata absent agreement of the parties or order of the court.").

[10] *Richmark Corp. v. Timber Falling Consultants,* 959 F.2d 1468, 1474 (9th Cir.1992) (citations and internal quotations omitted). *See generally Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct for the S. Dist. of Iowa*, 482 U.S. 522(1987).

[11] *See, e.g., PSEG Power New York, Inc. v. Alberici Constructors, Inc.*, 2007 WL 2687670 (N.D.N.Y. Sep. 7, 2007) (holding the plaintiff and counsel responsible for a software glitch that led to the "divorce" of e-mails and attachments in a production of ESI and ordering the re-production of the documents with the e-mails and attachments "married" – at an estimated cost of between US$37,500 and US$206,000).

[12] Australian Federal Court Rules O1, r4.

[13] The factors are: (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 purpose 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 the 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. Each factor was weighted, with factors 1-3 carrying more influence than the other factors, even though all factors were deemed important.

[14] In formulating this factor, the court followed *McPeek v. Ashcroft*, 202 F.R.D. 31 (D.D.C. 2001), where the court ordered the producing party to restore the electronic data at issue, to "carefully document the time and money spent," in doing so, to search the restored data for responsive documents, and to "file a comprehensive, sworn certification of the time and money spent and the results of the search."

[15] The factors are, in order of weight given: (1) the extent to which the request is specifically tailored to discover relevant information; (2) the availability of such information from other sources; (3) the total cost of production, compared to the amount in controversy; (4) the total cost of production, compared to the resources available to each party; (5) the relative ability of each party to control costs and its incentive to do so; (6) the importance of the issues at stake in the litigation; and (7) the relative benefits to the parties of obtaining the information.

[16] *See* Endnote 5, *supra*, for the Advisory Committee factors.

[17] Likewise, in *Lytle v. Ford Motor Co.*, 2003 WL 23855089 (Ind. Cir. Ct. Apr. 19, 2003) (unpublished), the court denied a plaintiff's request "to go into Ford's databases and look for any relevant information that might be there," finding the request for production to be overbroad and unduly burdensome. *But see, e.g.*, *GTFM, Inc. v. Wal-Mart*, 2000 WL 1693615 (S.D.N.Y. Nov. 09, 2000) (the defendant's failure to produce data or provide and accurate description of the computer system led to an order allowing the plaintiff's lawyer and expert to examine the defendant's computer system to look for the requested information at the defendant's expense).

[18] For cases prior to February 1, 2007, please refer to the 2007 "International Electronic Discovery" chapter in *The International Comparative Legal Guide to: Product Liability 2007*, published by Global Legal Group Ltd, London. For cases prior to June 1, 2006, please refer to the 2006 "International Electronic Discovery" chapter in *The International Comparative Legal Guide to: Product Liability 2006*, published by Global Legal Group Ltd, London.

[19] See also *Qualcomm Inc. v. Broadcom Corp.*, 2006 WL 5201392 (S.D.Cal. Dec 14, 2006); Qualcomm Inc. v. Broadcom Corp., 2006 WL 5410361 (S.D.Cal. Dec 20, 2006); *Qualcomm, Inc. v. Broadcom Corp.*, 2007 WL 1031373 (S.D.Cal. Mar. 21, 2007); *Qualcomm, Inc. v. Broadcom Corp.*, 2007 WL 2261799 (S.D.Cal. Aug. 6, 2007); *Qualcomm, Inc. v. Broadcom Corp.*, 2007 WL 2296441 (S.D.Cal. Aug. 6, 2007); *Qualcomm, Inc. v. Broadcom Corp.*, 2007 WL 2900537 (S.D.Cal Sept. 28, 2007); *Qualcomm Inc. v. Broadcom Corp.*, 2007 WL 4351017 (S.D.Cal. Dec 11, 2007); *Qualcomm, Inc. v. Broadcom Corp.*, 2008 WL 66932 (S.D.Cal. Jan. 7, 2008).

[20] See also *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, 2005 WL 674885 (Fla. Cir. Ct. Mar. 23, 2005); *Coleman (Parent) Holdings, Inc. v. Morgan Stanley & Co., Inc.*, No. CA 03-5045 AI (Fla. Cir. Ct. Jun. 23, 2005) (awarding prejudgment interest of US$ 207 million).