E-Discovery Obligations: a Comparative Analysis

By: Peter Pfeiffer[1]

Today large companies utilize computer networking systems to store vast quantities of electronic documents and media at relatively low cost. Many terabytes of data may be stored, and each terabyte may represent about three-hundred million typewritten pages, depending on file format. And all this electronically stored information ("ESI")[2] can be the target for opponents in litigation. E-Discovery[3] costs in large-scale litigation matters can exceed fifty percent of the litigation budget especially when there are contentious discovery disputes. The technology available to manage ESI for discovery in litigation is constantly evolving. Lawyers responsible for managing repositories of documents in discovery need to understand how technology is best able to serve client litigation needs. Moreover lawyers must have a good understanding of the rules as they relate to electronic discovery.

In an attempt to keep up with technological developments that corporations use to store and manage data, many countries are amending their rules, laws and procedures regarding electronic discovery. For example, in the United States the Federal Rules of Civil Procedure (the "Rule(s)") were amended in late 2006. In England Practice Direction 31B – Disclosure of Electronic Documents ("PD 31B"), which supplements Part 31 of the English Civil Procedure Rules ("CPR") was introduced to apply to electronic disclosure commencing on or after October 1, 2010. And in recent years many state courts and the federal courts in Australia have introduced rules and practice notes to give lawyers and their clients direction regarding the preferred court methodologies to

---

[1] Peter Pfeiffer is an associate at Hunton & Williams in Richmond, Va. Mr. Pfeiffer holds Masters of Laws degrees from Fordham University and The University of Sydney. He is admitted to practice in New York, Virginia, England & Wales and NSW Australia. He is a member of The Sedona Conference - Working Group 6 - International Electronic Information Management, Discovery and Disclosure. The views expressed in this article are those of the author and do not necessarily reflect the views of Hunton & Williams and are not intended to provide legal advice.

[2] In the US ESI includes all electronically stored data including but not limited to local drives, network drives, external drives, blackberries', blogs, e-mail servers, instant messaging, text messaging, voicemail, metadata, CDs, disks, back-up tapes and computer clouding etc. In other words, if you can store data on a computer or in some other electronic format it is likely to fall within the concept of ESI. In England an analogy may be drawn to PD 31B5 which defines "Electronic Document" as any document in electronic form. "It includes e-mail … text messages and voicemail, and word-processed documents and databases, and documents stored on portable devices … it includes documents stored on servers and backup systems… It also includes Metadata…" Similarly, Australia Federal Court Glossary to *Practice Note CM 6* effective September 2009, defines **"**Electronic Document" as "…a Document or component of information that was originally created using a computer system, software application or database. This is often referred to as Electronically Stored Information ('ESI'). The Metadata embedded within an Electronic Document is considered part of that Document. The definition of Electronic Document includes an email, email attachment …"

[3] "E-discovery" refers to electronic discovery. And the term "disclosure" or "e-disclosure" in England and Australia is similar to "discovery" or "e-discovery" in the US. However, England and Australia reference to disclose also refers to serving the "list of documents" whereas inspecting the documents is similar to reviewing documents in the US, see "ESI Collection and Word Searching" below.

adopt when addressing large scale electronic discovery.[4] This article discusses how the e-discovery or e-disclosure obligations of the United States, England and Australia have developed recently in contrast with one another.

A Comparison of the Duty to Preserve Documents and the Legal Hold Process

In the US when a party reasonably and in good faith anticipates litigation, the duty to preserve attaches. Some clear examples where the duty to preserve may attach include: when a party has served or received a complaint, when a party receives a demand letter threatening litigation or when a party receives notice from the government stipulating a civil or criminal investigation. Whether or not a duty to preserve documents has attached is a fact-intensive question, and each potential dispute should be assessed on its own merits. In *Zubulake IV* five months before Plaintiff filed an Equal Employment Opportunity Commission claim certain employees at the company reasonably believed Plaintiff would sue and thus the duty to preserve attached at that time. However, in *Cache la Poudre Fees v. Land O' Lakes*, a party wrote a letter implying a willingness to "explore a negotiated resolution" to their dispute without actually threatening litigation and thus the court found no obligation to preserve attached.[5] Preservation may be required well before litigation has commenced and it requires suspension of any document retention/destruction policy that might otherwise be in place.[6]

In *Zubulake v. UBS Warburg LLC*, Judge Shiendlin set out three steps to follow in meeting a company's preservation and legal hold obligations: (1) a litigation hold must be implemented as soon as litigation is "reasonably anticipated," and it should be re-issued periodically to refresh current employees and to ensure that new employees know what their obligations are; (2) counsel should identify the "key players" in the litigation regarding the litigation hold obligations; and (3) counsel should instruct all employees to

[4] In Australia, depending on where the action has commenced relevant state or federal rules apply. Often state courts rule on significant matters because the Australian federal system has not adopted an identical "diversity" procedure for removing a state court claim to federal court as that concept has evolved in US litigation. Australian Federal Court proceedings are governed by certain Commonwealth legislation such the *Federal Court Rules 1979* (Cth) and the *Evidence Act 1995* (Cth). Moreover, orders and rules promulgated under Federal Court Rules and relevant practice notes provide guidance to litigants. "Practice Notes" are not rules but are written by judges to provide litigant's direction regarding the court's process and procedures. This article assesses these enactments and Federal Court *Practice Note CM 5* – Discovery, *Practice Note CM 6* – Electronic Technology Litigation, both effective September 2009, Supreme of Victoria *Practice Note No. 1 of 2007* - Guidelines for the Use of Technology in any Civil Litigation, and the Supreme Court of New South Wales Equity Division *Practice Note SC Eq 3* - Commercial List and Technology and Construction List, commenced January 1, 2009. Any comprehensive "e-discovery" comparison with Australia would look at all states and territory courts, but in the interest of brevity this article focuses on the practice notes identified.

[5] 244 F.R.D. 614, 621 (D. Colorado 2007).

[6] *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 at 216-17 (S.D.N.Y. 2003) ("*Zubulake IV*").

produce electronic copies of the relevant files and make sure all relevant backup media is identified and stored in a safe place.[7]

A party who in good faith reasonably anticipates litigation must place a hold on all relevant documents.[8] As a practical matter this is usually done by sending an e-mail to appropriate personnel, and speaking to key players as necessary under the circumstances.

As recently as 2009, Brown J in *Earles v Barclays Bank* discussed preservation of documents under English law and explained there is a distinction between before and after commencement of legal proceedings. While a party should not deliberately destroy documents "…there is no duty to preserve documents prior to the commencement of proceedings…"[9] Brown J refers to *Documentary Evidence* as the leading text book in this area which mentions 'there might be cases where it was appropriate to draw adverse inferences from a party's conduct before the commencement of proceedings.'[10] However, the court found there "…would have to be some clear evidence of deliberate spoliation in anticipation of litigation before one could legitimately draw evidential 'adverse inferences' …[and] there is no such evidential basis in this case."[11] Note the consequences for deliberate destruction of evidence are discussed below in "Discovery Sanctions."

The recently-enacted PD 31B.7, entitled "Preservation of Documents," provides "as soon as litigation is contemplated, the parties' legal representatives must notify their clients of the need to preserve disclosable documents." It includes electronic documents that would otherwise be deleted pursuant to a document retention policy or in the ordinary course of business. Moreover, PD 31B 9.4 requires the parties to discuss before the first case management conference "the preservation of electronic documents, with a view to preventing loss of such documents before the trial."

In Australia the Supreme Court of Victoria in *British American Tobacco Australia Services Limited v. Cowell* discussed the duty to preserve documents before litigation has commenced, specifically, where documents were deleted pursuant to a document retention policy in the ordinary course of business. The court specifically compared the law of Australia to England and the US and stated "…much care is needed when seeking to apply [the learning of spoliation, as used in US proceedings] to the position in

---

[7] *Zubulake v UBS Warburg, LLC*, 229 F.R.D. 422, 433-34 (S.D.N.Y. 2004).

[8] *Id.* at 218.

[9] [2009] EWHC 2500 (Mercantile) at [28]; in Australia, see *British American Tobacco Australia Services Limited v. Cowell* [2002] V.S.C.A. 197, Para 175 (Unreported, Phillips, Batt and Buchanan JJA, December 6, 2002).

[10] Charles Hollander QC, *Documentary Evidence* Para 10-06, 10th Edition, Sweet & Maxwell, 2009.

[11] *Op. Cit.* [2009] EWHC 2500 (Mercantile) at [28].

Australia."[12] The court held the destruction of documents before proceeding have commenced "…was not shown to be a breach of any rules relating to discovery in this proceeding."[13] Victorian *Practice Note No. 1 of 2007* Para 6.2 discusses the retention and protection of electronic material. The accompanying "Frequently Asked Questions" discusses the need for lawyers to discuss with their clients' information management department issues concerning any automatic deletion policy and other document retention issues.

In NSW *Practice Note No. SC Eq 3* provides that at any hearing relating to discovery, the courts expect practitioners to have "ascertained the probable extent of discoverable documents" and under subparagraph 2 lawyers should discuss "…with their opponents about any issues concerning the preservation and production of discoverable documents including ESI."

Scope of Discovery

US Federal Rule 26(b)(1) entitled "Discovery Scope and Limits" provides the "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to a party's claim or defense." And "relevant" material can have a broad scope in US proceedings.

In England CPR 31.6(b) entitled "Standard disclosure – what documents are to be disclosed" requires a party to disclose documents which (i) adversely affect his own case; (ii) adversely affect another party's case; or (iii) support another party's case. And CPR 31.4 describes the "meaning of document" as "anything in which information is recorded" which read in context with CPR 31.6(b) is not as broad as the US. Note, CPR 31.6(c) also requires disclosure as required by a relevant practice direction. Practice Direction 31A Para 3.1 provides the form of disclosure is undertaken by a "list" of documents.[14]

In Australian Federal Court proceedings *Practice Note CM 6* - Pre-Discovery Conference Checklist, Para 2.1 provides that "… parties should agree on the scope of discovery having regard to: (b) the importance of limiting the scope of discovery as far as practicable in order minimize the time and costs … associated with … processing, analysis, review … of documents." And sub-paragraph (c) provides it is "the Court's view [that it is] inappropriate to require the production of more documents than are necessary for the fair conduct of the case." Federal Order 15 governs discovery and inspection of documents and rule 2(2) thereof provides a party must give discovery by

[12] *Cowell, Op. Cit.* Para 165.

[13] *Id.* at 175.

[14] Both England and Australia use the "list of documents" as the method for disclosure and this is described below at "ESI Collection and Word Searching." Briefly, the "list" identifies all disclosable documents and explains reasons for the absence of any document(s). The opposing party/counsel looks at the list to determine which documents they want to inspect (i.e. review). The list also identifies documents withheld on the basis of privilege. Thus, the list is central to procedural requirements in these jurisdictions.

serving the list of documents, unless otherwise directed to do so by the court. Note, rule 2(3) thereof requires a reasonable search for documents be conducted (discussed below). And rule 2(5) provides that in making a reasonable search a party may consider the complexity of the matter, the number of documents, the ease and cost of retrieving the document and the likely significance of the document.

As a practical matter scope of discovery is typically broader in the US because all "relevant" documents or materials may be discovered. In England or Australia the scope (or scale of discovery) tests are construed more narrowly.

Proportionality

In the US the term "proportionality" is not used in the Federal Rules of Civil Procedure but the concept is found in Rule 26(b)(2)(c), which provides that "[o]n motion or on its own the court must limit the frequency or extent of discovery" if "(i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source … less burdensome or less expensive" or subparagraph (iii) "the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties resources … and the importance of discovery in resolving the issues." Note, the language in this provision refers to a party making a motion and therefore assumes that ligation has commenced.

The concept of proportionality in term of costs is considered in Rule 26(b)(2) which makes a distinction between accessible and inaccessible ESI. Pursuant to 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." Rule 26(b)(2)(C)(iii) provides that by motion or on its own the court must limit discovery if the burden or expense of discovery outweighs the benefit of the evidence. Here the court will consider the needs of the case, the amount in controversy, the importance of the issues and the importance of discovery in resolving the issues.

In England the purpose of PD 31B is described in Para 2 as "to encourage … parties to reach agreement in relation to the disclosure of Electronic Documents in a proportionate and cost effective manner." In other words, the parties must weigh whether the costs of discovery are disproportionate to the claims in issue. This concept is emphasized in PD 31B.20 whereby parties ought perform a reasonable search for electronic documents "…in ways which are proportionate." The concept of proportionality in term of costs also appears in PD 31B.21(3)(d) and (e) whereby a litigant must consider costs of recovering the electronic document as well as the cost of making it available for inspection as part of the process when performing a reasonable search for electronic documents.

Australian Federal Court *Practice Note CM 5* Para 1 provides that when making discovery orders the court does so "with a view to eliminating or reducing the burden of discovery…" moreover Para 2 provides that the court considers "the likely cost of the discovery and its likely benefit." In *Practice Note CM6* Para 3.2 "[t]he court expects the

parties and their representatives to cooperate with and assist the Court … in identifying documents relevant to the dispute as early as possible and dealing with those documents in the most efficient way practicable." Similar to English requirements, NSW *Practice Note No. SC Eq 3* Para 30.4.1 states that the court expects practitioners to know "whether the burden and cost involved in discovering a particular document or class of documents is justified having regard to the cost of assessing the documents…" and the importance of the document(s) in the proceedings. Therefore, parties must be mindful of proportionality issues as a preliminary issue to discovery.

Although the concept of proportionality adopted in the subject countries have similarities, as a practical matter more documents tend to be subject to discovery in US litigation than in England or Australia. There are probably many reasons for this, but one important reason is that in England and Australia an order can be entered by a judge against the losing litigant requiring it to pay the winning litigant's court costs and attorney fees (which includes reasonable e-discovery costs).[15] So in England and Australia documents tend to be requested in a manner that considers costs should a party lose at trial.[16] In the US each litigant usually must bear its own costs notwithstanding the outcome of the trial, which is also referred to as the American Rule.[17]

Initial Disclosures and Conferences

In the United States once litigation has commenced the parties must consider document collection. Rule 26(1)(A)(i) (entitled "initial disclosures") requires a party to litigation, without awaiting a discovery request, to provide the other party: the name and if known, the address and telephone number of each individual likely to have discoverable information – along with the subject of that information … And (ii) requires a description by category and location of all documents, electronically stored information … in its possession, custody, or control and may use to support its claims or defenses…"

Also Rule 26(f)(2) provides that the parties must in the context of their claims and defenses consider the possibility for settling the matter and "discuss any issues about preserving discoverable information; and develop a proposed discovery plan." They must meet at the commencement of the litigation to confer about these matters. The Rule essentially requires the parties to develop and agree upon discovery plans in a cooperative manner. Even though it may be more work up front to address these "meet

[15] Note in England, PD 31B 9.7 requires parties to discuss "the basis of charging for or sharing the cost of the provision of electronic documents…" early on in the proceedings.

[16] In England costs must be "reasonably incurred and reasonable in amount," see CPR 44.4(1). In Australia Federal proceedings Order 62 Para 4(2)(c) provides the gross amount must be specified as well how it is justified so that a judge may consider costs.

[17] *Alyeska Pipeline Service Co. v. Wilderness Society*, 421 U.S. 240, 247 (1975).

& confer" obligations, it may save time and money in the long run by laying the path for discovery to proceed with fewer disputes, particularly in regards to e-discovery.[18]

England and Australia do not have "initial disclosures" as such. However, parties are required to consider early on in a matter how best to manage ESI, including use of technology (see discussion regarding requirements for "list of documents" in "ESI Collection and Word Searching" below). For example, in England PD 31B.8 requires parties to discuss the use of technology to manage electronic documents. In Australia *Practice Note CM 6* - Pre-Discovery Conference Checklist, Para 4 requires parties to consider strategies for the early management of electronic documents.

In England PD 31B.8 entitled "Discussion between the parties before the first Case Management Conference in relation to the use of technology and disclosure" requires parties and legal representatives to discuss the use of technology to manage electronic documents particularly with regard to creating lists. PD 31B.9(3) requires the parties to consider tools and techniques to reduce the cost of disclosure of electronic documents, including by considering categories of documents, date ranges, particular custodians or types of documents; key word searches; agreed software; methods to identify privileged documents; and use of data sampling. These issues are considerations similar to that required in US federal litigation.

PD 31B.10 provides parties may complete the "Electronic Document Questionnaire" which identifies the scope, extent and suitable format for disclosure of documents (which must be verified by a statement of truth). Completion of the questionnaire is not required. However, if the parties are unable to reach agreement regarding the management of electronic documents a court may well order them to complete the questionnaire (see PD 31B.15 and 31B.18). The questionnaire identifies in pertinent part custodian, date ranges, types of documents and communications, database and IT systems, key word searching and potential problems with accessing electronic documents. Moreover, PD 31B.14 requires certain preparation for the first Case Management Conference which is an informal meeting between all parties and the judge to review the case progress.[19] Many of the issues addressed are similar to the objectives of the US "meet and confer" process.

Australian Federal Court *Practice Note CM 6* Para 7.1 provides "[t]he Court expects the parties to meet and confer for the purpose of reaching an agreement about the protocols to be used for the electronic exchange of documents and other issues relating to efficient document management…" And Para 7.2 provides that "[t]he Court may require the parties to address these issues at a Directions Hearing or a case management conference."

[18] The Sedona Conference have produced a number of working group papers and best practices regarding discovery obligations, http://www.thesedonaconference.org. See generally, The Sedona Principles: Second Edition - *Best Practices Recommendations & Principles for Addressing Electronic Document Production*, June 2007.

[19] PD 31B.17 provides that where the parties are not able to reach agreement in relation to disclosure of Electronic Documents that they seek direction from the court at the earliest practical date.

NSW *Practice Note Sc Eq 3* Para 29 provides, "[p]ractitioners must advise their opponents at an early stage of the proceedings of potentially discoverable electronically stored information and meet and agree upon matters…" See also Victorian *Practice Note No 1 of 2007* Para 6 which contains similar objectives.

Moreover in Australia parties are expected to consider adopting certain protocols to manage their disclosure. *Practice note CM 6* Para 8 provides that parties should agree on whether they will use the "Default Document Management Protocol" when the number of documents subject to discovery is between 200 and 5,000. If the number is expected to exceed 5,000 documents then the "Advanced Document Management Protocol" is expected to be considered. The template protocols contain certain standardized formats for parties to follow for their disclosure obligations. These requirements are analogous to the US "meet and confer" obligations regarding discovery issues.

ESI Collection and Word Searching

In the US after litigation commences, the parties will exchange document requests for specific categories of documents. Pursuant to Rule 34(a) a party may request ESI in "the responding party's possession, custody, or control." In order to respond to such a request an attorney or experienced legal assistant together with a database specialist sometimes may visit their client and interview all appropriate persons likely to have relevant documents and ESI. Once the attorney interviews the custodians and determines where the responsive documents are located, a database specialist copies all identified relevant e-files. This may mean collecting relevant e-mail folders, Word files, Excel, Calendar, among other programs where relevant information may be stored.

Once documents are collected search terms may be identified to cull out irrelevant documents. Documents may be culled out by date range or alternatively include documents by agreed known key word searches. This process must be explained and/or performed co-operatively with opposing counsel to make it judicially defensible. As explained in *In re Seroquel Products Liability*, "…while key word searching is a recognized method to winnow relevant documents from large repositories, use of this technique must be a cooperative and informed process."[20]

Moreover, sampling and other quality assurance techniques should be employed in order to meet discovery obligations.[21]

In England, PD 31B.20 requires a party to perform a reasonable search for electronic documents and the factors to be considered are listed in PD 31B.21. They include but are not limited to: the number of documents; nature and complexity of proceedings; the cost of recovering any electronic document; and the significance of the documents. PD 31B.25 provides for the use of reasonable keyword searches and PD 31B.27 adds that it

[20] 244 F.R.D. 650, 662 (M.D. Fla. 2007).

[21] *Id.*, 662.

may be necessary to individually sample certain documents or review categories of documents. PD 31B.9(b) and (e) also provide for keyword searches to be utilized in case management in the context of data sampling to ensure quality.

In England parties initially prepare and exchange the *List of documents* on *Form N265* (CC) if in the Commercial Court (See PD 31B.30). The "list of documents" is used by an opponent to determine which documents they would like to inspect. Part one of the "list" requires parties to discloses all documents chronologically that are in the parties' control. Part two of the list requires parties to identify documents in their control but which will not be produced because of privilege or third party confidentiality. Part three requires parties to identify relevant documents that are relevant but no longer in a party's control. Parties can agree whether they will provide originals or copies for inspection. Pursuant to Rule 31.10(6) CPR a (a) party must certify the extent of searches conducted to locate documents; (b) that they understand the duty to disclose; and (c) certify to the best of their knowledge the duty to disclose has been carried out.

In Australian Federal Court proceedings parties may reach agreement regarding search terms and pursuant to *Practice Note CM 6* attach them to Schedule 2 - "Agreed strategies in relation to reasonable searches" and any "Agreed strategies for management of electronically stored information" may be attached to Schedule 3.

When litigating in Australian Federal Court a litigant is required to complete *Form 22 List of documents* pursuant to Federal Order 15, rule 6. An affidavit is sworn confirming that the list of documents is correct. In NSW similar requirements are found in Sections 21.3 and 21.4 of the *Uniform Civil Procedure Rules 2005* (NSW) and parties use the format provided by Form 11 for the list of documents.

In the US categories of documents are not listed; they are either copied for opposing counsel or the originals are provided for inspection as they kept in the ordinary course of business. So getting the documents in the first place is a less impeded process in the U.S.

Data Privacy Considerations

With any comparative analysis of e-discovery obligations it is helpful to consider briefly the implications of the *1995 EU Data Protection Directive* (the "Protection Directive") because many European countries have adopted data protection laws to implement privacy protection. Moreover data privacy has evolved in Europe and Australia more as a fundamental human right and in ways that may sometimes conflict with the US discovery process.

The Protection Directive generally applies when "personal data" (defined broadly as "relating to" an identifiable individual) is "processed" (including "collection, recording, organization, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available…") by an entity. To legally process personal data under the Protection Directive the grounds for doing so under Article 7 must be met, which include: (1) the data subject must consent; (2) when processing is necessary for a legal obligation; or (3) the processing must be necessary for

the performance of a legitimate interest. Moreover, Article 25(1) of the Protection Directive generally prohibits the "transfer" of personal data to any other country or territory outside the European Union.

Article 29 Working Party was formed as an independent European advisory body for data protection authorities from Europe pursuant to Article 29 of Directive 95/46/EC for the purpose of interpreting directive issues. Article 29 Working Party views the Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matter (the "Hague Convention") as the method by which cross-border e-discovery should proceed. This process requires that in order to obtain discovery the court in a country where a claim is being made issues "letters of request" or "letters rogatory" to the relevant authority in the country where the documents are located. As a practical matter the procedures of the Hague Convention can be time consuming, and requires redactions of personal information. Most European countries have adopted procedures from the Hague Convention.

England enacted the *Data Protection Act 1998* (the "*DPA 1998*") which incorporates certain objectives of the Data Directive.[22] These provisions are complicated and certainly require assistance from local counsel. The first data protection principle of *DPA 1998* provides that "personal data shall be processed fairly and lawfully and … shall not be processed unless (1) one of the conditions in Schedule 2 is met." Schedule 2 provides that:

> (1) The data subject has consented; (2) Processing is necessary for the performance of, or commencing a contract; (3) Processing required under a legal obligation; (4) Processing is necessary to protect the vital interests of the data subject; (5) Processing is necessary to carry out any public function; (6) Processing is necessary to in order to pursue the legitimate interests of the "data controller" or "third parties."

These requirements conflict with US litigation practice because "preserving" data under US rules falls within the concept of "processing" under the *DPA 1998*, which defined broadly in Section 1(1) to include, among other things obtaining, recording, holding, retrieving, disclosing or erasing or destroying data. However, England has adopted certain exemptions which make the discovery process easier to manage. Part IV-Exemptions of the *DPA 1998*, includes exemptions for national security, investigating crimes and other matters, including, especially Section 35(2) of the *DPA 1998* which provides an exemption for disclosure in connection with "any legal proceeding (including prospective proceeding)." Additionally, Schedule 4 to *DPA 1998* provides for the transfer of data for legal proceeding for cases of "substantial public interest." For example, *In Re Madoff Securities International Ltd* [2009] EWHC 422 (Ch) the court permitted transfer of certain data to the US because of the public interest in settling

[22] However, the scope of disclosure in England is wider than in other Member States, see Working Document 1/2009 on re-trial discovery for cross-border civil litigation (WP 158 of February 11, 2009) at page 6.

financial disputes created by the Bernard Madoff Ponzi scheme.

In Australia, the Commonwealth enacted the *Privacy Act 1998* (Cth) at the same time as the English DPA 1998 which also incorporates some of the objectives of the Protection Directive. The Commonwealth introduced a number of information privacy principles promulgated under the *Privacy Act 1998*. Principle 9 provides "[a] record keeper who has possession or control of a record that contains personal information shall not use the information except for a purpose to which the information is relevant." Principle 10 requires a record keeper to use the personal information only for the purpose it was obtained. Principal 1(a) requires consent of the individual concerned if personal information is to be used for another purpose. Principle 11 also discusses the "limits on the disclosure of personal information."

Data privacy considerations are given more weight in England and Australia than in the US, but that is not to say they do not exist in the US. A litigant may request a court to issue a "protective order" regarding the "confidential" nature of the documents so that they will be treated appropriately, including forbidding disclosure to non-parties. A party must make a motion to the court in order to obtain a protective order, whereas in England and Australia data privacy is governed by statutes.

Discovery Sanctions

In the US Rule 37 entitled "[f]ailure to make disclosures or cooperate in discovery; sanctions" provides that when a party has failed to make discovery opposing counsel may make a motion for sanctions. As a practical matter judges tend to reserve sanctions for egregious conduct but have discretion regarding sanctions they may impose. Typical sanctions might include: striking a pleading; dismissing an action or cause of action; issuing an adverse inference regarding the evidence in question or the lack of any such evidence; award of attorney fees and legal costs; and/or award of punitive and/or compensatory damages. Proactive litigants who co-operate with opposing counsel and meet their discovery obligations are much less likely to be sanctioned. In one matter the absence of "…reasonable policies and procedures for managing its information and records" was a pertinent factor courts consider when imposing sanctions.[23]

Courts have authority to impose sanctions for spoliation. Spoliation is "the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation."[24] For example, in *Reino de Espana v. American Bureau of Shipping, Inc.*, Spain sued the American Bureau of Shipping in the Southern District of New York regarding the loss of an oil tanker off the coast of Spain. Defendant requested production of specific e-mails from Spanish government agencies which were refused. Spain argued the e-mails were subject to

[23] *Adams v. Dell*, Inc. 621 F.Supp 2d 1173, 1193-94 (D.Utah 2009).

[24] *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999).

Spain's privacy laws and did not produce them. The court ordered disclosure of the e-mails and in part granted defendant's motion for sanctions.[25]

The verdict returned by the jury in *Zubulake v. UBS Warburg, LLC* was about $9 million in compensatory damages and about $20 million in punitive damages for an employment gender discrimination claim.[26] The punitive damages were rendered because UBS acted with reckless disregard as to Laura Zubulake's rights. The high award may have been allowed in part because of UBS's lack of document preservation and spoliation of electronic evidence (e-mails).

In England sanctions were discussed by Justice Morgan in *Rybak v Langbar International Limited* where a party deliberately used a software cleaning program on a computer which over-wrote files that would have been used in evidence. Morgan J held that Rybak was in breach of an order to disclose documents. Moreover, Rybak's claims and defenses to counter-claims were struck-out.[27]

Also in England in *Douglas v. Hello! Ltd* the court distinguished the circumstances where documents were destroyed before and after the commencement of legal proceedings. The English court approved and followed the Australian *Cowell* decision[28] which held, sanctions do not apply unless the destruction of documents before proceedings have commenced is done in "…an attempt to pervert the course of justice."[29]

In England Section 31.23 CPR enables proceedings for contempt of court to be brought against a person making a false disclosure statement. In other words if the documents identified on a parties "list of documents" have been falsified (or destroyed documents are omitted from the list), this provision may come into play. Subparagraph (2) provides such proceeding may only be commenced by the Attorney General or with permission of the court. As a matter of practice this provision may not be used that often. Contempt proceedings may be brought in Australian Federal Court under Order 35A of the Federal Court Rules for similar reasons.

After the *Cowell* decision the Victorian state legislature enacted the *Crimes (Document Destruction) Act 2006* (Vic) which inserts a new section into the *Crimes Act 1958* (Vic) to make it a crime to destroy documents or evidence that is to be used in legal proceedings. See also the *Crimes Act 1900* (NSW) entitled "[t]ampering with evidence,

---

[25] 2008 WL 3851957 at *4 (S.D.N.Y.) August 18, 2008.

[26] Eduardo Porter, *UBS Ordered to Pay $29 Million in Sex Bias Lawsuit*, New York Times, April 7, 2005, see http://www.nytimes.com.

[27] [2010] EWHC 2015 (Ch), Para 6.

[28] [2003] EWHC 55 (Ch) [86].

[29] *Op. Cit.* Para 173 and 175.

etc." Note, the prosecution must prove each element of the crime beyond a reasonable doubt which is a different standard than that required for civil proceedings.

In Australian Federal Court the decision by Kenny J in *Research in Motion Ltd v Samsung Electronic Australia Pty Ltd Limited* discussed the concept of "spoliation" where a party had deliberately destroyed back-up tapes. It was stated that spoliation essentially requires the deliberate destruction of evidence.[30]

Privilege Issues

Each of the subject countries applies the law of privilege to litigation and generally, the concept is somewhat similar among them.

However in the US one difference, in terms of process, is that pursuant to Rule 26(b)(5) a party asserting a claim for privilege must identify each document withheld on a privilege log. Generally, this means logging the type of document, date of creation, document author, recipients (including those copied) and a brief description why the document/communication is privileged. An example of a privilege description for a document may be "email chain from in-house counsel to outside counsel and company employees provides information for the purpose of rendering legal advice regarding environmental compliance obligations." And managing large privilege logs in US practice can be time consuming and expensive.[31] Keep in mind that Federal courts usually defer to state law for privilege determinations which differs from jurisdiction to jurisdiction.

In England and Australia a privilege log is not required. As discussed, in these jurisdictions parties exchange their "List of documents." And the lists identify which documents by category are withheld from inspection on the basis of privilege.

Conclusion

Continued developments in technology enable countries to do business together on scales not previously seen. Technology has also made it easier for the subject countries to learn from each other's rules and laws, especially in relation to development of e-discovery obligations. The requirement to co-operate early during the e-discovery process in each of the subject countries suggests the "meet and confer" obligation is necessary to assist parties to agree and resolve e-discovery disputes as early as possible. As technology continues to evolve particularly in relation to the management of electronic data, and the refinement of key word searching for the identification of relevant evidence (or exclusion of irrelevant evidence) the subject countries will continue to learn from one another's

[30] [2009] FCA 320 (6 April 2009), Para 31.

[31] See generally, Peter Pfeiffer, *Managing Costs: E-mail Chains and Preparation of Privilege Logs* 20 No. 23 Westlaw Journal Insurance Coverage 10 (March 12, 2010) for a discussion on managing voluminous e-mail chains in the context of preparing privilege logs.

rules, processes and methodologies regarding efficient e-discovery management practices.