E-Discovery Around The World

Helen Bergman Moure, Brett Harrison, David A. Marquez-Lechuga, Gavin Foggo

Helen Bergman Moure is a Partner in K&L Gates' Seattle office. Since 1999, Helen's practice has focused within the firm's e-Discovery Analysis and Technology (e-DAT) Group. She oversees both large and small projects involving all aspects of the discovery process, from custodian identification and retention, to collection, processing, review and post-production litigation support. Helen is active in the Sedona Conference and is a frequent speaker on electronic discovery and document retention issues. Helen can be reached in Seattle at 206.370.8365 and helen.moure@klgates.com.

Brett Harrison is a Partner in the Toronto office of McMillan LLP. He has a general corporate commercial litigation practice with an emphasis on insolvency and cross-border disputes. As a member of the firm's Professional Standards & Excellence Committee, Brett is part of the group responsible for keeping the firm at the forefront of addressing e-discovery issues. Brett is also the editor of his firm's Cross-Border Litigation bulletin and has written extensively on cross-border issues. Brett can be reached in Toronto at 416.865.7932 and brett.harrison@mcmillan.ca.

David A. Marquez Lechuga is an Associate in the Guadalajara, Mexico office of Baker & McKenzie Abogados, S.C. His areas of practice and expertise include civil, commercial, and administrative litigation through the different levels of jurisdiction (including constitutional proceedings), as well as international judicial assistance. International judicial assistance includes service of process and documents, taking of evidence, recognition and enforcement of foreign judgments and awards, and proceedings in connection with international treaties and conventions to which Mexico is a party. David can be reached in Guadalajara at +52.33.3848.5300 and david.marquez-lechuga@bakernet.com.

Gavin Foggo is a U.K. solicitor and partner with London law firm Fox Williams LLP. He handles a broad range of U.K. and international business and commercial disputes, involving litigation, arbitration, mediation, and negotiations. Gavin is co-chair of the International Litigation sub-committee of the Commercial and Business Litigation committee of the ABA Litigation Section, and an active member of the ABA. He is also the Honorary Secretary of the London Solicitors Litigation Association. He is a regular commentator on litigation and business law issues, and is rated in the U.K. legal guides (***The Legal 500*** and ***Chambers Guide to the Legal Profession***). Gavin can be reached in London at +44.20.7614.2543 and gfoggo@foxwilliams.com.

This article is based on a paper the authors prepared for a seminar sponsored by the ABA's Section of Litigation.

The more intertwined international businesses become, the more you need to know about e-discovery all around the globe.

WITH THE RAPID GROWTH of technology has come the rapid shrinking of our global community; no longer are companies and other organizations contained by traditional geographic boundary lines. Consequently, corporations and organizations find themselves able, and more importantly willing, to expand their reach across international borders to participate in the global community. The inevitable result of such cross-border growth is the need to know and understand the relevant controlling law of each country in which an organization does business or maintains connections.

In litigation, the need to understand each relevant country's laws and rules is especially important. Discovery, in particular, requires special attention and understanding. The following discussion will address, generally, some of the necessary considerations when undertaking discovery in the United States, Canada, Mexico, and the United Kingdom. While the specific requirements of each jurisdiction may be varied and numerous, the message to practitioners remains the same: litigation

involving foreign jurisdictions requires research, careful planning, and deliberate decision-making. To that end, an important first step when crafting an international discovery strategy is consultation with local counsel in the relevant foreign jurisdiction to ensure a comprehensive understanding of the necessary steps to achieve your intended result.

THE UNITED STATES • In the United States, discovery, along with all other aspects of civil litigation in federal courts, is controlled by The Federal Rules of Civil Procedure. First promulgated in 1938, the rules did not specifically address the discovery of electronically stored information (ESI) until December 2006. Since that time, issues related to electronic discovery have been heavily litigated in American courts, resulting in a body of case law available to provide guidance to interested practitioners. Any discussion of electronic discovery in the United States, though, must begin with a discussion of the rules themselves.

The Federal Rules Of Civil Procedure

In December 2006, The Federal Rules of Civil Procedure were amended to address the discovery of ESI. Revised again in December 2007 to reflect style, captioning, and numbering changes, the amendments included revisions and additions to Rules 16, 26, 33, 34, 37, and 45, as well as Form 35. They cover six related areas, described in more detail below:

- Definition of discoverable material;
- Early attention to issues relating to electronic discovery;
- The format of production;
- Discovery of ESI from sources that are not reasonably accessible;
- The procedure for asserting claim of privilege or work product protection after production; and
- A "safe harbor" limit on sanctions under Rule 37 for the loss of ESI as a result of the routine operation of computer systems.

In addition, amendments to Rule 45 correspond to the proposed changes in Rules 26-37.

1. Definition Of Discoverable Material

The amendments introduce the phrase "electronically stored information" to Rules 16(b)(3)(B)(iii), 26(a)(1)(A)(ii), 33(d), and 34, to acknowledge that ESI is discoverable. The expansive phrase is meant to include any type of information that can be stored electronically. It is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and technological developments.

2. Early Attention To Electronic Discovery Issues

Several of the amendments require the parties to address ESI early in the discovery process, recognizing that such early attention is crucial in order to control the scope and expense of electronic discovery, and avoid discovery disputes. Rule 26(a)(1)(A)(ii) adds ESI to the list of items to be included in a party's initial disclosures. Rule 16(b)(3)(B)(iii) adds provisions for the disclosure or discovery of ESI as an item that may appropriately be included in the court's scheduling order. Rule 26(f)(3)(C) expands the list of issues that must be discussed as a part of the meet and confer process, and includes a requirement that parties develop a discovery plan that addresses issues relating to the discovery of ESI — including the form or forms in which it will be produced. It also requires parties to discuss any issues relating to the preservation of discoverable information, and address issues relating to claims of privilege or work product protection. *See, e.g., Lowery v. County of Riley*, 2008 WL 3562061 (D. Kan. Aug. 12, 2008) (denying motion to stay discovery, court set Rule 16(b) scheduling conference, directed parties

to conduct Rule 26(f) planning conference, and instructed parties to familiarize themselves with 2006 e-discovery amendments to the Rules, review ESI guidelines posted on court's Internet Web site, and become knowledgeable about their clients' information management systems and their operation, including how information is stored and retrieved); *Palgut v. City of Colo. Springs,* 2006 WL 3483442 (D. Colo. Nov. 29, 2006) (parties' stipulated Electronic Discovery Plan and Order to Preserve Evidence); *O'Bar v. Lowe's Home Centers, Inc.,* 2007 WL 1299180 (W.D.N.C. May 2, 2007) (court ordered parties to develop joint pre-certification discovery plan and articulated detailed guidelines for discovery of ESI adapted from the "Suggested Protocol for Discovery of Electronically Stored Information" set forth by the United States District Court for the District of Maryland).

3. Format Of Production

Rule 34(b)(1)(C) addresses the format of production of ESI, and permits the requesting party to designate the form or forms in which it wants ESI produced. The rule does not require the requesting party to choose a form of production, however, since a party may not have a preference or may not know what form the producing party uses to maintain its ESI. Rule 34(b)(2)(D) & (E) provide a framework for resolving disputes over the form of production, in the event that the responding party objects to the requested format(s). Finally, the amended rule provides that, if a request does not specify a form of production, or if the responding party objects to the requested form(s), the responding party must notify the requesting party of the form in which they intend to produce the electronically stored material — with the option of producing either in a form in which the information is ordinarily maintained, or in a reasonably usable form. *See Goodbys Creek, LLC v. Arch Ins. Co.,* 2008 WL 4279693 (M.D. Fla. Sept. 15, 2008) (where plaintiff did not specify format of production but complained that defendant's conversion and production in TIFF images made it "much more difficult" to search the documents, court granted motion to compel re-production of such documents and gave defendant three options for its re-production); *White v. Graceland Coll. Ctr. for Prof'l Dev. & Lifelong Learning, Inc.,* 586 F. Supp. 1250 (D. Kan. 2008) (conversion of ESI to .pdf files and production in paper format did not comply with Rule 34's option to produce in "reasonably usable form"); *L.H. v. Schwarzenegger,* 2008 WL 2073958 (E.D. Cal. May 14, 2008) (defendants' conversion of ESI from its original searchable and sortable format into .pdf files which did not have those capabilities violated Rule 34 notwithstanding fact plaintiffs had not requested native electronic format); *Perfect Barrier LLC v. Woodsmart Solutions Inc.,* 2008 WL 2230192 (N.D. Ind. May 27, 2008) (defendant's production of email in native format on computer disk satisfied Fed. R. Civ. P. 34(b) since Rule 34 "only requires [defendant] to submit the emails in the format in which it keeps them, Native format, and nothing more"; court further found that native format production was "reasonably usable" and denied plaintiff's motion to require reproduction in hard copy format).

4. ESI From Sources That Are Not Reasonably Accessible

Amended Rule 26(b)(2)(B) creates a two-tiered approach to the production of ESI, making a distinction between that which is reasonably accessible, and that which is not. Under the new rule, a responding party need not produce ESI from sources that it identifies as not reasonably accessible because of undue burden or cost. If the requesting party moves to compel discovery of such information, the responding party must show that the information is not reasonably accessible because of undue burden or cost. Once that showing is made, a court may order discovery only for good cause, subject to the provisions of amended Rule 26(b)(2)(C). *See, e.g., Disability Rights Council of*

Greater Wash. v. Wash. Metro. Area Transit Auth., 242 F.R.D. 139 (D.D.C. 2007) (motion to compel production of email from backup tapes granted); *Best Buy Stores, L.P. v. Developers Diversified Realty Corp.*, 247 F.R.D. 567 (D. Minn. 2007) (objection to magistrate judge's order compelling plaintiff to restore database to searchable format sustained, since database was not reasonably accessible in light of $124,000 cost to restore it and $27,000/month cost to maintain it, and defendants had not established requisite good cause); *Ameriwood Indus., Inc. v. Liberman,* 2007 WL 496716 (E.D. Mo. Feb. 13, 2007) (motion to compel production denied for failure to establish good cause).

This two-tier system seeks to provide a balanced, equitable approach to resolve the unique problem presented by ESI, which is often located in a variety of locations of varying accessibility — strongly favoring the production of relevant information from more easily accessible sources when possible. This provision received a great deal of attention during the public comment period, and the Advisory Committee made substantial changes to both the proposed rule and to the accompanying notes to address the concerns voiced, and to balance the interests of both requesting and responding parties. The responding party receives protection from being forced to tap hard-to-access sources, when retrieving information or determining the presence of responsive content cannot be achieved without incurring substantial burden or cost. The requesting party benefits from knowing the sources the responding party does not intend to search, and has a method of obtaining this information if it is truly warranted.

5. Asserting Claim Of Privilege Or Work Product Protection After Production

The addition to Rule 26(b)(5) sets forth a procedure through which a party who has inadvertently produced trial preparation material or privileged information may nonetheless assert a protective claim as to that material. The rule provides that once the party seeking to establish the privilege or work product claim notifies the receiving parties of the claim and the grounds for it, the receiving parties must return, sequester, or destroy the specified information. The Committee Note clearly states that the rule does not address whether the privilege or protection was waived by the production, but simply prohibits the receiving party from using or disclosing the information, and requires the producing party to preserve the information, until the claim is resolved.

6. "Safe Harbor"

The new Rule 37(e) safe harbor provision provides that, absent exceptional circumstances, a court may not impose sanctions on a party for failing to provide ESI lost as a result of the routine, good-faith operation of an electronic information system. It responds to the routine modification, overwriting, and deletion of information that attends the normal use of electronic information systems.

The Advisory Committee notes that the "routine operation of an electronic information system" refers to the ways in which such systems are generally designed and programmed to meet the party's technical and business needs, and includes the alteration and overwriting of information that often takes place without the operator's specific direction or awareness. The Committee further observes that such features are "essential to the operation of electronic information systems," and that there is "no direct counterpart in hard-copy documents."

The protection of Rule 37(e) applies only to information lost due to the routine operation of an information system, and only if such operation was in good faith. The Committee Note discusses the effect that the existence of a preservation obligation may play in determining whether or not the operation was in good faith, and expressly cautions: "A party cannot exploit the routine operation of an information system to evade discovery obligations

by failing to prevent destruction of stored information that it is required to preserve."

Local Federal District Court And State Court Rules

At least 41 United States District Courts now require compliance with special local rules, forms, or guidelines addressing the discovery of ESI. In some districts where there are no local rules or court-mandated forms, individual judges have created their own forms or set out their own preferred protocols for e-discovery.

Generally, these local rules expand, in varying degree, the obligations of litigants relating to conferences and reports required under Rule 26(f). Parties involved in litigation in these districts must observe these additional requirements. Although similar to the Federal Rules amendments that encourage early attention to electronic discovery issues, these local rules tend to go much farther and impose affirmative obligations on counsel to investigate and become knowledgeable about their clients' computer systems.

Additionally, more and more states are adopting statutes and court rules addressing the discovery of ESI, and others are actively considering whether to follow suit. The state e-discovery rules that are in place vary considerably in scope and purpose. Many of the recently enacted state rules mirror or closely track the 2006 e-discovery amendments to the Federal Rules of Civil Procedure, e.g., Arizona, Minnesota, Montana, and Utah. Others, like those in Texas and Mississippi, attempt to define the reasonable scope of electronic discovery and prescribe cost-shifting in certain cases.

Accordingly, practitioners are well advised to consult the civil rules in each relevant jurisdiction to determine the nature and scope of their electronic discovery obligations.

Case Law: Lessons Learned

Unlike some other countries, American courts have developed a relatively large body of case law resulting from a myriad of conflicts surrounding the recently enacted amendments to the federal Rules. One of the most commonly litigated issues is a party's failure to preserve or spoliation of electronic data. In the United States, a party has an obligation to preserve relevant data "when the party has notice that the evidence is relevant to the litigation or when a party should have known that the evidence may be relevant to future litigation." *Forest Labs., Inc. v. Caraco Pharm. Labs., Ltd.,* 2009 WL 998402, at *2 (E.D. Mich. Apr. 14, 2009) (*citing Fujitsu Ltd. v. Fed. Express Corp.,* 247 F.3d 423, 436 (2d Cir. 2001)); *Silvestri v. Gen. Motors Corp.,* 271 F.3d 583, 591 (4th Cir.2001) ("[t]he duty to preserve material evidence arises not only during litigation but also extends to that period before the litigation when a party reasonably should know that the evidence may be relevant to anticipated litigation").

Accordingly, upon a party's failure to uphold its duty, whether negligent or purposeful, courts have indicated their willingness to impose sanctions, including (among others):

- Default judgment. *Krumwiede v. Brighton Assocs., L.L.C.,* 2006 WL 1308629 (N.D. Ill. May 8, 2006) (plaintiff's willful and bad faith spoliation of evidence and "hide the ball" tactics warranted default judgment on counterclaims); *Metropolitan Opera Ass'n, Inc. v. Local 100,* 212 F.R.D. 178 (S.D.N.Y. 2003) (judgment in plaintiff's favor entered on issue of liability when defendants failed to produce email and electronic documents and failed to preserve computer hard drives, among other discovery abuses); *QZO, Inc. v. Moyer,* 594 S.E.2d 541 (S.C. Ct. App. 2004) (no abuse of discretion for trial court to strike defendant's answer and enter judgment for plaintiff on issue of liability, when defendant reformatted computer's hard drive, effectively erasing any information the computer

may have contained, a day before surrendering it for court-ordered inspection); *Nartron Corp. v. Gen. Motors Corp.*, 2003 WL 1985261 (Mich. Ct. App. Apr. 29, 2003) (court dismissed plaintiff's claims as discovery sanction after four-day evidentiary hearing on alleged discovery abuses by plaintiff, e.g., delays in responding to discovery requests and attenuated and piecemeal production of altered/partially deleted database); *Century ML-Cable Corp. v. Carrillo*, 43 F. Supp. 2d 176 (D.P.R. 1998) (default judgment entered against party who willfully destroyed customer records and laptop computer following TRO prohibiting destruction of those items); *Long Island Diagnostic Imaging, P.C. v. Stony Brook Diagnostic Assocs.*, 728 N.Y.S.2d 781 (N.Y. App. Div. 2001) (trial court erred in not dismissing defendants' counterclaim and third-party complaint as sanction for spoliation of evidence — contrary to court's orders, defendants purged databases and produced backup tapes that were compromised and unusable); *Crown Life Ins. Co. v. Craig*, 995 F.2d 1376 (7th Cir. 1993) (court entered default judgment against insurer on agent's counterclaim as sanction for insurer's willful failure to comply with discovery orders requiring the production of relevant database); *Am. Bankers Ins. Co. of Fla. v. Caruth*, 786 S.W.2d 427 (Tex. App. 1990) (entry of default judgment on issue of liability against insurer for failure to produce computer data was not an abuse of discretion); *Computer Assocs. Int'l v. Am. Fundware, Inc.*, 133 F.R.D. 166 (D. Colo. 1990) (defendant's destruction of source code warranted default judgment on issue of liability);

- The issuance of an adverse inference instruction. *Zubulake v. UBS Warburg, LLC*, 229 F.R.D. 422 (S.D.N.Y. 2004) (*Zubulake V*) (when defendant acted willfully in destroying potentially relevant information, which resulted in the absence of such information or its tardy production, court granted plaintiff's motion for sanctions including adverse inference instruction and monetary sanctions); *see also, 3M Innovative Properties Co. v. Tomar Electronics*, 2006 WL 2670038 (D. Minn. Sept. 18, 2006) (sanctions including adverse inference instruction imposed, based upon defendant's failure to implement legal hold or conduct a reasonable search for responsive documents); *E*Trade Secs. LLC v. Deutsche Bank AG*, 230 F.R.D. 582 (D. Minn. 2005) (sanctions in the form of an adverse inference instruction and attorneys' fees imposed when party committed spoliation by permanently erasing hard drives, failing to retain DVDs of relevant audio recordings, and failing to place adequate litigation hold on email boxes while making no changes to its three-year retention policy for email backup tapes); *Housing Rights Ctr. v. Sterling*, 2005 WL 3320739 (C.D. Cal. Mar. 2, 2005) (adverse inference instruction and monetary sanctions imposed when defendants committed "egregious" discovery abuses, including: failure to institute or communicate a proper legal hold; failure to verify with appropriate personnel whether there was an email backup system; failure to search for documents; and "purposeful sluggishness" in taking steps to prevent destruction of evidence and in responding to discovery requests); *Broccoli v. Echostar Communications Corp.*, 229 F.R.D. 506 (D. Md. 2005) (adverse inference instruction and monetary sanctions imposed when defendant failed to suspend its "extraordinary email/document retention policy" which provided for automatic purging of emails after 21 days and complete deletion of all electronic files of former employees 30 days after their departure); *Advantacare Health Partners, LP v. Access IV*, 2004 WL 1837997 (N.D. Cal. Aug. 17, 2004) (adverse inference instruction and monetary sanctions warranted when, in advance of court-ordered inspection, defendants deleted from their computers numerous electronic files

that had been copied from former employer's computer systems); *Anderson v. Crossroads Capital Partners, LLC,* 2004 WL 256512 (D. Minn. Feb. 10, 2004) (plaintiff's use of "Cyberscrub" data wiping software before court-ordered inspection warranted adverse inference instruction); *3M v. Pribyl,* 259 F.3d 587, 606 n.5 (7th Cir. 2001) (negative inference instruction warranted when six gigabytes of music were downloaded onto hard drive the night before the computer was to be turned over for inspection); and

- Monetary sanctions.

Another issue frequently addressed by the courts is the obligation of a party and counsel to investigate the existence and location of potentially relevant data. In 2008, a federal magistrate judge imposed unique sanctions upon a party's outside counsel after finding that the attorneys had assisted their client, Qualcomm, in committing a "monumental and intentional discovery violation" by "intentionally hiding or recklessly ignoring relevant documents, ignoring or rejecting numerous warning signs that Qualcomm's document search was inadequate, and blindly accepting Qualcomm's unsupported assurances that its document search was adequate." *Qualcomm Inc. v. Broadcom Corp.,* 2008 WL 66932 (S.D. Cal. Jan. 7, 2008).The court observed that the attorneys "then used the lack of evidence to repeatedly and forcefully make false statements and arguments to the court and jury." As such, the court found that the attorneys had violated their discovery obligations and also may have violated their ethical duties. Declining to impose monetary sanctions against the attorneys, the court ordered six of Qualcomm's outside counsel to forward a copy of the order to the State Bar of California for appropriate investigation. The court also ordered certain of Qualcomm's in-house lawyers and the sanctioned outside counsel to participate in a comprehensive Case Review and Enforcement of Discovery Obligations program, described as "a collaborative process to identify the failures in the case management and discovery protocol utilized by Qualcomm and its in-house and retained attorneys in this case, to craft alternatives that will prevent such failures in the future, to evaluate and test the alternatives, and ultimately, to create a case management protocol which will serve as a model for the future." *Id.* at *18. Recognizing Qualcomm's responsibility for the violations as well, the court ordered Qualcomm to pay Broadcom's attorneys fees and costs in the amount of $8,568,633.00. *Id.* at *20.

In a similar case, the court rendered judgment in favor of plaintiffs on the issue of liability and ordered defendants to pay attorneys' fees when the court found that defendants and counsel had engaged in egregious discovery violations, including: representing to the court that all responsive documents were produced despite failing to ensure an adequate search had been undertaken; failing to implement a document retention policy to prevent the destruction of responsive documents; failing to ensure an adequate understanding of responsiveness on the part of those responding to discovery; and failing to adequately identify and follow up with persons who might have relevant documents, among other things. *Metropolitan Opera Ass'n., Inc. v. Local 100,* 212 F.R.D. 178 (S.D.N.Y. 2003).

Discovery In Foreign Jurisdictions: How Have American Courts Responded?

A discussion of the rules and case law surrounding electronic discovery within the United States provides only a portion of the picture, though. In today's ever-shrinking global community, relevant electronic information could be, and often is, stored in locations all over the globe. Accordingly, any practitioner should be acutely aware of the likelihood that foreign jurisdictions have their own rules governing the discovery of electronically stored information (or any information for that matter) and that those rules are often in conflict with the Fed-

eral Rules of Civil Procedure and America's broad discovery policies.

Acknowledging a jurisdiction's rules or laws is different, however, from following them. United States courts have consistently found that foreign requirements for discovery, as established by the Convention on the Taking of Evidence Abroad in Civil Matters (the Hague Evidence Convention) or by the European Union's Data Protection Directive (Directive 96/46/EU), for example, do not trump the Federal Rules of Civil Procedure as to actions in American courts.

The purpose of the Hague Evidence Convention, signed by the United States in 1970 and ratified by the Senate in 1972, was to "establish a system for obtaining evidence located abroad that would be 'tolerable' to the state executing the request and would produce evidence 'utilizable' in the requesting state." *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct.*, 482 U.S. 522, 530 (1987) (citing Phillip W. Amram, *Explanatory Report on the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters* (ca. 1970)). The Hague Evidence Convention "instituted a uniform procedure for the issuance of 'letters of request' (a/k/a/ 'letters rogatory'). Letters of Request are petitions from a court in one nation to a designated central authority in another, requesting assistance from that authority in obtaining relevant information located within its borders." The Sedona Conference Working Group 6: International Electronic Information Management, Discovery and Disclosure, *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery*, at 17 (2008), available at http://www.thesedonaconference.org/dltForm?did=WG6_Cross_Border (hereinafter Sedona Framework).

Despite the United States appearing as signatory, however, United States courts have rejected the proposition that The Hague Evidence Convention constitutes a binding agreement to abide by the procedures set forth therein for the purpose of obtaining discovery from a foreign jurisdiction. In the case of *Societe Nationale*, supra, the United States Supreme Court concluded that "the optional Convention procedures are available wherever they will facilitate the gathering of evidence by the means authorized in the Convention. Although these procedures are not mandatory, the Hague Convention does 'apply' to the production of evidence in a litigant's possession in the sense that it is one method of seeking evidence that a court may elect to employ." *Id.* at 541.

In 1995, The European Parliament and the Council of the European Union adopted its Data Protection Directive (the Directive). The Directive had two stated objectives:

- "In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data";
- "Member States shall neither restrict the free flow of personal data between Member States for reasons connected with the protection under paragraph 1."

Directive 95/46/EC of the European Parliament and of the Council of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of data, Official Journal L 281, 23/11/1995 P.0031-0050, available in English at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (visited May 12, 2009).

Essentially, the basic tenets of the Directive establish that an individual has the right to notice of the collection of her data, the right to choose not to have that data collected, the right to know how the information will be used and to restrict its use, the right to know the extent to which the data will be protected, the right to challenge the accuracy

of the data and to provide corrected information, and the right to seek legal redress to protect her privacy rights. Rebecca Herold, *European Union Data Protection Directive of 1995 Frequently Asked Questions,* Computer Security Institute Alert Newsletter, May 2002, http://www.informationsheild.com/papers/EU%20Data%20Protection%20Directive%20FAQ.pdf. The Directive accomplished the goal of harmonizing the protection of personal data among member states thus easing the transfer of data between them. In contrast, "transfers of personal data from [European Economic Area] to third countries that do not provide adequate protection for privacy are prohibited, subject to some limited derogations." Sedona Framework, supra, at 12. Many European countries (and other countries around the world) also attempt to restrict the discovery of information intended for disclosure in a foreign jurisdiction by passing "blocking statutes." *Id.* at 18. Some statutes prohibit the "disclosure copying, inspection or removal of documents from a specific country" while others "are designed to protect commercial interests of the citizens from cross-border interference by other States, such as in the case of U.S. Antitrust, SEC, and similar foreign regulations." *Id.* These blocking statutes are often cited in support of foreign entities' motions for protective orders. *Id.* Foreign entities are often particularly keen to win such motions when the penalties for violating such statutes may result in civil or criminal penalties. *Id.*

United States courts are thus far generally unpersuaded by the arguments of foreign entities attempting to prevent the disclosure of personal data subject to the Directive or local blocking statutes. In *Societe Nationale Industrielle Aerospatiale,* as discussed above, the United States Supreme Court rejected the proposition that the Hague Evidence Convention provided the exclusive means for obtaining discovery in a foreign jurisdiction. In that opinion, the court opined that "the concept of international comity requires in this context a more a particularized analysis of the respective interest of the foreign nation and the requesting nation…" to determine whether to compel production. *Societe Nationale,* supra, 482 U.S. at 543-44. Accordingly, the court indicated its support for the consideration of the five factors set forth in the *Restatement (Third) of Foreign Relations Law of the United States* §442(1)(c):

- The importance to the ... litigation of the documents or other information requested;
- The degree of specificity of the request;
- Whether the information originated in the United States;
- The availability of alternative means of securing the information; and
- The extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine the important interests of the state where the information is located.

Societe Nationale, supra, 482 U.S. at 544 n. 28.Subsequent consideration of the issue in American courts resulted in the recognition of two additional factors: "the hardship of compliance on the party from whom discovery is sought, and the resisting party's good faith." *Strauss v. Credit Lyonnais, S.A.,* 249 F.R.D. 429, 439 (E.D.N.Y. 2008) (citing *Minpeco, S.A. v. Conticommodity Servs., Inc.,* 116 F.R.D. 517, 523 (S.D.N.Y. 1987)).

Later opinions have maintained the earlier courts' refusal to relinquish control of discovery to directives of foreign treaties or laws. *Strauss,* 249 F.R.D. 429; *In re Vivendi Universal, S.A. Secs. Litig.,* 2006 WL 3378115 (S.D.N.Y. Nov. 16, 2006); *Reino de Espana v. Am. Bureau of Shipping,* 2006 WL 3208579 (S.D.N.Y. Nov. 3, 2006); *Societe Nationale,* supra. In *Strauss*, supra, United States citizens brought suit against a French bank alleging that the bank was liable for damages for aiding and abetting and for providing material support to terrorists. The bank, Credit Lyonnaise, S.A., sought a protective order preventing the production of material

subject to French bank secrecy laws. The court refused to grant defendant's motion for a protective order despite significant evidence presented that to produce the information requested would violate French law and evidence that at least one French attorney was fined for seeking information in violation of French blocking statutes. Analyzing each of the factors established in *Societe Nationale* and subsequent opinions, the court determined that a protective order was not appropriate. Specifically addressing the blocking statutes at issue, for example, the court noted that "it is well settled that such statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of the production may violate the [foreign] statute." *Strauss,* supra, at 449-50 (citing *Societe Nationale,* supra, 482 U.S. at 544 n. 29). The court's analysis also rejected defendant's assertions that it could face criminal and civil penalties upon its finding that the bank had failed to show that prosecution or civil consequences related to the disclosure were likely. *Id.* at 455. Concluding its opinion, the court noted that most, if not all, factors weighed in favor of the plaintiffs, and highlighted the importance of the court's determination that the interests of the United States and France were mutual with regard to thwarting terrorist financing and outweighed the "French interest in preserving bank customer secrecy, and its generally-stated sovereign interest." *Id.* at 456. The court's conclusion also outlined the court's reasoning that the information was crucial to the litigation, that the requests were narrowly tailored, and that there was no alternative means of securing the information.

Despite the strongly defended position that American courts can compel production of data from European and other foreign jurisdictions, a minority of courts have nonetheless indicated a willingness to grant protection to foreign entities seeking to prevent the production of information subject to European privacy laws. In *Salerno v. Lecia, Inc,* 1999 WL 299306 at *3 (W.D.N.Y. Mar. 23, 1999), for example, the district court found that even if collateral estoppel did not bar reconsideration of a state court's denial of plaintiff's request for production of documents subject to European National Data Protection Laws, "the document production sought by plaintiff is precluded by Directive 95/46/EC and by the German Act on Data Protection." Similarly, the Supreme Court of Texas overruled a trial court's denial of protection against production of documents protected by foreign blocking statutes when the trial court failed to appropriately balance the competing interests of the parties and relevant law. *Volkswagen, A.G. v. Valdez,* 909 S.W. 2d. 900 (Tex. 1995); *see also Husa v. Laboratoires Servier SA,* 740 A.2d 1092 (N.J. Super. Ct. App. Div. 1999) (ordering compliance with the Hague Convention on Evidence upon defendant's motion for an order requiring its use). These cases are the exception, however, not the rule, but perhaps offer a small foothold to foreign entities concerned about the consequences of being compelled to violate local law.

Alternatives For Data Transfers And Their Availability In Litigation

Outside of a legal battle, there are several options available to ease the transfer of personal data between countries. The following is a brief overview of several of the available alternatives for cross-border data transfers as presented by the Sedona Conference's *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery.* (The alternatives discussed contemplate data transfers in multiple contexts, including (or sometimes excluding) litigation. Accordingly, careful attention should be paid to the parameters of each alternative and its applicability or inapplicability to relevant scenarios.)

First, and perhaps most obvious, is the option to transfer personal data with the unambiguous consent of the person to whom the data pertains. Although less practical in more complicated scenarios, in which the data to be transferred belongs to only a few people, sufficient consent may be obtained to facilitate the data transfer. "In order for the consent to be considered valid, it must be: (1) given before the transfer; (2) unambiguous; (3) specific to the transfer or category of transfers; (4) freely given; and (5) informed." Sedona Framework, supra, Appendix E (2008).This option may be unavailable, though, if the data is commingled with other data, such as customer information, for example, because of the necessity of obtaining consent from each data subject.

A second way to facilitate a transfer of data is participation in the "Safe Harbor" framework developed between the U.S. Department of Commerce and the European Commission. Participation in the Safe Harbor eliminates the need for consent and provides "predictability and continuity" for companies that commonly transfer personal data into the United States. *Id.* Under the framework, participating companies are required to join a self-regulatory privacy program or develop their own self-regulatory privacy policy that complies with the requirements of the Safe Harbor and to annually self-certify their compliance to the Department of Commerce. Such companies must also: "provide a contact person or persons to handle questions, complaints and access requests; establish an independent recourse mechanism to investigate unresolved complaints, and have procedures in place for verifying compliance." *Id.*

An entity's participation in the Safe Harbor means it will be deemed to provide adequate protection by all countries in the European Union, resulting in "unabated" data flow to those entities. Participation is limited, though, to organizations within the jurisdiction of the U.S. Federal Trade Commission or the Department of Transportation. Accordingly, entities outside of that jurisdiction (such as telecommunications and financial services companies) are not eligible. Also outside the framework of the Safe Harbor are "onward transfers" of data to third parties, such as in litigation. In those cases, organizations must notify the data subjects of the transfer and provide an option to opt out. If such notice is not possible, an organization has the option to enter a written agreement with the third party to provide the same level of privacy as is provided by companies within Safe Harbor.

Written agreements, as described above, constitute a third option to more easily accomplish the cross-border transfer of data. After "years of negotiation," the European Commission has adopted a "set of standard contractual clauses that will ensure adequate safeguards for international transfers of personal data." *Id.* These "Model Contractual Clauses" allow for the transfer of data upon both parties' agreement to be bound by the established terms. There are two clauses available: controller-to-controller and controller-to-processor. This option is a good one for organizations that do not need day-to-day transfers, but are occasionally required to do so for litigation, for example. Difficulties with Model Contractual Clauses, however, include the need to anticipate every possible data transfer and use lest the agreement become outdated and expose the organization to enforcement actions, among others. Thorough research is necessary to determine the proper parameters of such agreements in each relevant jurisdiction.

A final option for consideration is the use of Binding Corporate Rules (BCRs). This option may be best utilized by those corporations with "complex corporate structures and a web of cross-border data transfers." *Id.* "Personal data can be transferred outside of the European Union but within a group of companies in a manner that ensures adequacy by the adoption of binding codes of corporate conduct by the organization or binding corporate rules

("BCRs")." *Id.* Such rules detail "what information is collected, how it is processed, used and stored, and who may access this data" as well as providing employees the right to enforce the code against the organization(s) and providing for the creation of an "independent ombudsman team" whose job is to address data privacy concerns. *Id.* Once approved by the relevant Data Protection Authority, this option allows for "seamless transfer of data between the offices of multi-national organizations." *Id.*

As with the other alternatives, the use of BCRs is not without difficulty. For instance, such rules do not provide "safety" for the transfer of data outside the corporate group. Accordingly, data subject to "onward transfer" for litigation purposes will not be protected and will require additional and alternative safeguards. Also, the creation and implementation of BCRs is a time-consuming and potentially expensive undertaking requiring thorough research and an understanding of what is necessary to accomplish compliance with each country's data protection laws. For additional information, *see* Sedona Framework, supra; *see also* Article 29 Data Protection Working Party, *Working Document 1/2009 on pretrial discovery for cross-border civil litigation* (2009), available at http://ec.europa.eu/justice_home/fsj/privacy/_docs/wpdocs/2009/wp158_en.pdf.

CANADA • As in many other areas of jurisprudence, the case law related to e-discovery is not nearly as developed in Canada as it is in the United States due to the lack of reported cases on the issue. In addition, there have been few statutory developments in Canada to provide guidance. That being said, there are both provincial and federal groups, including a Working Group of the Sedona Conference (Sedona Canada) that are working toward this goal. Sedona Canada published *The Sedona Canada Principles Addressing Electronic Discovery* in January 2008 (the Sedona Canada Principles) and the Ontario E-Discovery Implementation Committee has released guidelines for the discovery of electronic documents (the Guidelines) and a model e-discovery order (the Model Order). The Sedona Canada Principles, Guidelines, and Model Order, combined with the existing case law, provide some guidance on the application of e-discovery in Canada.

The Canadian System For Discovery

Given that e-discovery in Canada is based on the same basic Sedona principles that U.S. e-discovery is, the systems are very similar. The differences relate mainly to the fundamental differences between discovery in the two countries. The most significant differences between the U.S. and Canadian discovery processes are:

- Only one representative of a corporate party can be examined;
- An individual being examined must undertake to make inquires in order to provide answers to relevant questions asked at the examination;
- Although written interrogatories are not typically utilized, undertakings are provided at the examination that are fulfilled in writing (in a manner similar to written interrogatories). Once answers to undertakings have been provided, a party has a right to re-examine on those answers;
- There is an implied undertaking that none of the evidence or information disclosed during the discovery process can be used "for any purposes other than those of the proceeding in which the evidence was obtained." Ontario, Rules of Civil Procedure, r. 30.1.01(3);
- Questions asked at examinations must be relevant to a matter in issue and can not simply relate to a "train of inquiry" which may lead to relevant information.

E-Discovery

As mentioned earlier, the case law related to e-discovery is not nearly as developed in Canada as it is in the United States. In addition, there have

been no statutory revisions in Canada to provide guidance.

Guidance is beginning to be made available, however, from a number of other sources. In January 2008, Sedona Canada published the aforementioned Sedona Canada Principles, available at http://www.thesedonaconference.org/dltForm?did=canada_pincpls_FINAL_108.pdf. In addition, the Ontario E-Discovery Sub-Committee of the Discovery Task Force has released guidelines for the discovery of electronic documents in Ontario and model e-discovery precedents, including a model preservation order. Task Force on the Discovery Process in Ontario, *Guidelines for the Discovery of Electronic Documents in Ontario* (2005) (Ontario Guidelines). The Sedona Canada Principles and the Ontario Guidelines and models, combined with the existing case law, provide substantial guidance on the application of e-discovery in Canada.

What Is E-Discoverable?

The types of documents covered by e-discovery in Canadian cases are almost identical to those provided for under the U.S. e-discovery rules. In Ontario, the definition of "document" in the Rules of Civil Procedure includes "data and information in electronic form." Supra, r. 30.01(1)(a). The Ontario Guidelines explain that "data and information in electronic form" can include "active data," "archival data," and "backup data," all of which might be discoverable. Further, the Guidelines explain that "any data or information that can be readily compiled into viewable form, whether presented on the screen or printed on paper, is potentially within the definition of 'document' under Rule 30.01 of the Rules of Civil Procedure." This data might include "meta-data," "residual data," and "replicant data." Ontario Guidelines, supra, at 10-11 (Principles 4-5).

Consistent with recent U.S. developments, metadata is now generally producible. Metadata has been found to be "data and information in electronic form." *Hummingbird v. Mustafa,* 2007 CanLII 39610 (Ont. S.C.J.). Although metadata is not specifically referred to in the Sedona Canada Principles, it is dealt with by encouraging parties to produce documents in a format that preserves metadata, unless it is agreed that metadata will not be relevant. The commentary to Principle 8 indicates that electronic documents and data should be produced in electronic format (or some other format that preserves metadata and allows it to be produced when relevant), unless the metadata is known to be irrelevant. Sedona Principles, supra, comments 8.b, 8.c. The principles in the Ontario Guidelines go further, requiring that: "Parties should discuss the need to preserve or produce meta-data as early as possible. If a party considers meta-data relevant, it should notify the other party immediately." Ontario Guidelines, supra, at 12 (Principle 7).

However, this broad requirement does not always apply to all data. Principles 3 and 4 in the Ontario Guidelines indicate that in most cases, the primary source of electronic documents will be the parties' active data (rather than archival or backup data). Parties will not normally be required to search for, review, or produce documents that are deleted, hidden, or residual absent agreement or court order. Ontario Guidelines, supra, at 10 (Principles 3-4). Similarly, the Sedona Canada Principles similarly provide that parties, absent agreement or an order to do so, are not required to search for deleted or residual ESI. Sedona Principles, supra, Principle 6.

Preservation

As in the United States, parties in Canada have a duty to take reasonable and good-faith steps to preserve relevant electronic documents. However, both the Ontario Guidelines and the Sedona Canada Principles acknowledge that preservation will not always be reasonable. The Ontario Guidelines allow that "it is unreasonable to expect parties to

take every conceivable step to preserve all documents that may be potentially relevant." Sedona Principles, supra, Principle 5; comment 3.a.

The Model Preservation Order defines the duty to preserve as taking "reasonable steps to prevent the partial or full destruction, alteration, testing, deletion, overwriting, shredding, incineration, wiping, relocation, migration, theft, or mutation of documents, as well as to prevent any action that would make the documents incomplete or inaccessible." Task Force on the Discovery Process in Ontario, Model Document 7: Preservation Order, s. 3.2.

The Principles and Guidelines also contemplate notice to parties who might be affected by a duty to preserve electronic data. The Ontario Guidelines include as a principle that: "Parties should place each other on notice with respect to preserving electronic documents as early in the process as possible, as electronic documents may be lost in the ordinary course of business." Sedona Principles, supra, Principle 6. A similar statement is made in the commentary to the Sedona Canada Principles. Sedona Principles, supra, comment 3.d. Parties should consider at this stage what electronic data might be in the hands of third parties, and what must be done to preserve that data.

Third Parties

There is not yet significant jurisprudence in Canada considering e-discovery issues involving non-parties, but it is most likely that the general law of third-party discovery will apply. In Canada, non-parties are generally only required to produce documents if:

- The documents are not obtainable from a party to the litigation;
- The documents have been requested from the non-party and it has refused to produce the documents; and
- The requesting party can establish that the documents are necessary in order for it to prosecute or defend the action.

E-Production

The manner in which documents are produced, which is not specified in any statute, is covered extensively in the Ontario Guidelines and the Sedona Canada Principles. Courts in Canada have held that the governing principle is achieving "broad disclosure," which requires the production of information in its native electronic format when available. *Cholakis v. Cholakis* (2000), 44 C.P.C. (4th) 162 (Man. Q.B). The commentary to the Ontario Guidelines reinforces this, requiring parties to "produce a document in electronic form if, for any reason related to the litigation, it is not sufficient to produce a printout or scanned version of the document." Ontario Guidelines, supra, at 15. This is to achieve the goal set out in Principle 11 of the Guidelines, to "facilitate access to the information in the document, by means of electronic techniques to review, search, or otherwise use the documents in the litigation process." *See* Sedona Principles, supra, Principle 8. Note that production of an electronic record does not eliminate the obligation to produce paper documents that are the source of the information contained in the electronic record. *Cooper & Stein v. Konstan* [1997] O.J. No. 3399 (Ont. Gen. Div.).

In some cases, additional hardware or software might be required in order for a party to make use of electronic data that has been produced. The case law is divided on where the obligation lies to provide these devices. Courts may order that the producing party take steps to enable access to electronic material when the requesting party is not reasonably able to access them. *Procter & Gamble Co. v. Kimberly-Clark of Can. Ltd.* (1989), 25 C.P.R. (3d) 244 (Fed. T.D.). This does not include the provision of a licensed copy of software if a license can be obtained elsewhere by the requesting party. *Logan v. Harper,* 2003 CanLII 15592 (Ont. S.C.J.).

Privacy

Privacy can become an issue during the disclosure of electronic data in discovery. In Canada, the Personal Information Protection and Electronic Documents Act (PIPEDA) governs the use of personal information by the private sector (except in British Columbia, Alberta and Quebec, which have substantially similar provincial statutes). While PIPEDA would generally prohibit the disclosure of any personal information, including personal information stored electronically, the Act excepts personal information disclosed when the disclosure is "required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records." PIPEDA, S.C. 2000, c. 5, s. 7(3)(c).

Costs

Although costs are dealt with in a similar manner to the United States, with each party bearing the expense of collecting, reviewing, and producing its own electronic documents while the requesting party bears the cost of copying those productions, the Canadian cost regime differs in that it is a "loser pays" system. As a result, while it is possible to obtain cost-shifting orders, it is less common because a significant portion of the "proper and reasonably necessary" costs of production will be recovered by the successful party. This system is reinforced by the Ontario Guidelines, which recommend that the costs of preservation, retrieval, review, and production of documents be borne by the producing party, with the requesting party incurring the cost of copying those productions. Any other cost shifting would occur at the end of the litigation through a cost award. Ontario Guidelines, supra, at 16-17. The Sedona Canada Principles recommend a similar allocation.

With respect to documents discovered from third parties, although the requesting party is normally required to pay for some of the costs of the non-parties in making production, it is normally much less than the actual cost of production.

Obtaining Discovery In Canada

The taking of evidence for use in a foreign proceeding is slightly different in Canada than in most other jurisdictions. The reason for this is that, unlike many other nations (including the United States), Canada is not a party to the Hague Convention on Taking of Evidence Abroad in Civil or Commercial Matters (the Hague Convention). Accordingly, parties seeking to compel Canadian evidence for use in a foreign proceeding must utilize a Letters of Request (also known as Letters Rogatory) process governed by Canadian statute and common law, rather than the Hague Convention.

Canada's provincial and federal Evidence Acts contain specific provisions allowing for the enforcement of Letters of Request. Canadian courts promote the comity of nations and are generally deferential to the decisions of foreign courts. Canadian courts will order the enforcement of Letters of Request in most cases. However, the decision to enforce Letters of Request is completely discretionary in Canada, and some Canadian courts have refused to enforce Letters of Request in certain cases.

Contents And Scope

To satisfy the test under Canadian law for enforcing a Letter of Request, the applicant must establish through an affidavit that:

- The evidence sought is relevant;
- The evidence sought is necessary for trial and will be adduced at trial, if admissible;
- The evidence is not otherwise obtainable;
- The order sought is not contrary to public policy;
- The documents sought are identified with reasonable specificity; and
- The order sought is not unduly burdensome, bearing in mind what the relevant witnesses

would be required to do were the action to be tried in Canada.

Friction Division Products Inc. v. E.I. DuPont de Nemours & Co. (No. 2) (1986), 56 O.R. (2d) 722, 732 (H.C.J.).

The applicant must also show that:

- The foreign proceeding is already pending or underway before a court or tribunal of competent jurisdiction; and
- The Letter of Request was granted at a hearing of the foreign court; and
- Enforcement of the Letter of Request is absolutely necessary to do justice in the foreign litigation; and
- The evidence sought is relevant to a substantial issue in the foreign litigation (i.e., is not required just to corroborate existing evidence or to attack witness credibility).

With respect to the relevancy requirement, care should be taken to ensure that the requested evidence is squarely related to the allegations set out in the foreign complaint. In *Pecarsky v. Lipton Wiseman Altbaum & Partners,* (1999) 38 C.P.C. (4th) 170 (Ont. S.C.J.), the Ontario Superior Court of Justice refused to enforce a Letter of Request when there was considerable uncertainty as to whether the documents requested were properly related to the issues in the U.S. litigation. The Court found that the addition of the words "among other things" to the U.S. complaint was insufficient to justify the enforcement in Canada of such a broad document request.

Canadian courts have discretion to enforce a Letter of Request only in part, such as by limiting the scope of questions to be asked during examination or documents ordered to be produced in accordance with Canadian laws of evidence and civil procedure. If a Canadian court finds the request too broad, it is likely to — but will not always — order more restricted discovery than that requested, rather than reject the request in its entirety.

MEXICO • On May 29, 2000, Mexico enacted provisions in several bodies of law based on the Model Law on Electronic Commerce drafted by the United Nations Commission on International Trade Law (UNCITRAL). Paragraph 43 of the Guide to Enactment of the Model Law establishes that the general principles on which the Model Law is based, are to:

- Facilitate electronic commerce among and within nations;
- Validate transactions entered into by means of new information technologies;
- Promote and encourage the implementation of new information technologies;
- Promote the uniformity of law; and
- Support commercial practice.

Likewise, on August 29, 2003, Mexico enacted provisions based on the UNCITRAL Model Law on Electronic Signatures. These provisions, intended to bring legal certainty to the use of electronic signatures, also establish criteria of technical reliability for the equivalence between electronic and hand-written signatures, and establish basic rules for assessing possible responsibilities and liabilities for the signatory, the relying party, and trusted third parties intervening in the signature process. The aforementioned provisions are the main regulations dealing with electronic data that may be used as evidence in a litigation proceeding (either in Mexico or abroad).

The Mexican System For Discovery

As is the case in most civil law countries, Mexico does not have a formal discovery process. Under Mexican law governing civil and commercial proceedings, a party in a dispute does not have the obligation of delivering or disclosing to the counterpart any information related to the subject matter of the dispute before the proceeding commences. Nevertheless, the law establishes means to obtain

the evidence in question once a litigation has commenced.

The obligation to produce documents arises if such documents are related to a litigation proceeding and are requested by a court. In order for a court to issue an order to request documents from a party to a litigation proceeding (or to a third party), the following conditions must be met:

- The documents are not obtainable from a party to the litigation;
- The documents are necessary in order to prosecute or defend the action; and
- The documents in question are identified by the requesting party (as opposed to a generic description).

See Articles 50 and 1061 of the Commercial Code and Article 561 of the Federal Code of Civil Procedures.

Scope Of E-Discovery

As explained in the previous section, Mexico does not have a formal discovery process. However, it is possible to request a party to produce electronic data to be used as evidence in a litigation proceeding before a foreign court by means of the following alternatives:

- Using uniform international regulations, such as the Hague Convention or the Inter-American Convention on the Taking of Evidence Abroad; or
- Using domestic provisions that regulate the process to obtain evidence in Mexico to be used abroad.

Under both alternatives, the process of taking evidence is commonly completed through a court. Article 15 of the Hague Convention provides that a diplomatic officer or consular agent of a Contracting State may, in the territory of another Contracting State and within the area where he exercises his functions, take the evidence without compulsion of nationals of a State which he represents in aid of proceedings commenced in the courts of a State which he represents.

The Federal Code of Civil Procedures, Article 210-A, explicitly acknowledges electronic data as evidence as follows:

"Any information generated or communicated contained in electronic means, optical or in any other technology are acknowledged as evidence. … To appraise the evidentiary strength of the information referred to in the previous paragraph, it is necessary to consider the reliability of the method in which it was generated, communicated, received or stored, and if appropriate, if it is possible to attribute the content of the information to the originator of such information and if the information contained therein is accessible so as to be usable for subsequent reference."

Based on the aforementioned provision, any information generated or communicated and contained in electronic means may be used as evidence (subject to the procedures and limitations set forth in other provisions). Mexican law provides a general framework to determine the reliability of the information generated or communicated in electronic means. Accordingly, the reliability may be ultimately supported with an expert witness opinion.

E-Preservation

Article 49 of the Commercial Code, establishes the following:

"Merchants are obligated to preserve at least for ten years the originals of those letters, telegrams, data messages or any other document containing a contract or agreement that create rights and obligations. … For purposes of preserving or presenting the originals, in the case of data messages, it is required to have the information maintained flaw-

less and unaltered as of the moment in which its was generated in its final form and accessible so as to be usable for subsequent reference."

Based on the foregoing, it is mandatory to preserve electronic data that contains a contract or agreement that creates rights and obligations. The specific requirements to preserve electronic data are set forth in a Mexican Official Standard called NOM-151-SCFI-2001 (NOM-151). Compliance with NOM-151 is compulsory.

E-Production

Although the Commercial Code establishes the obligation of preserving electronic data in flawless and unaltered form, the manner in which an electronic document has to be produced is not specified in any statute. However, considering that Mexican law establishes the criteria to appraise the evidentiary strength of electronic data:

- Confirm the method by which it was generated, communicated, received, or stored;
- Determine if it is possible to attribute the content of the information to the originator of such information; and
- If the information contained therein is accessible so as to be usable for subsequent reference, it may be advisable to obtain the electronic data with the assistance of an expert witness in IT and with the participation of a court clerk who would certify the process by which the electronic data in question was obtained.

It should be noted that the Article 561 of the Federal Code of Civil Procedures establishes that the obligation to produce documents at proceedings followed abroad does not include the obligation of producing documents identified by general characteristics. Accordingly, it is necessary to identify the specific document.

Costs

The Mexican Federal Constitution establishes that court fees and expenses are forbidden. Likewise, the Hague Convention establishes that the execution of the Letter of Request shall not give rise to any reimbursement of taxes or costs of any nature.

Nevertheless, if expert witnesses are required for the taking of evidence, although questionable, the requesting party may have to cover the fees of such expert witness. To avoid any argument aimed to contest the legitimacy of the payment of the expert witnesses' fees, it may be advisable to follow the process set forth under Article 14 of the Hague Convention (if applicable).

Obtaining Discovery In Mexico

Mexico is a party to the Hague Convention. Accordingly, if the proceeding in which the electronic data would be used as evidence is in a court of a country that is also a party to the Hague Convention, the provisions of such convention will primarily govern the evidence-taking process. Mexico has a blocking statue with respect to "pretrial discovery of documents." Article 23 of the Hague Convention. In accordance with such blocking statute, in order for a document to be produced, the following requirements must be met:

- A litigation proceeding has commenced;
- The documents are reasonably identified as to their dates, content, and any other pertinent information;
- The facts or circumstances that may lead the requesting party to believe that the documents requested are in possession, control, or custody of a party located in Mexico are reasonably specified; and

- A direct connection between the evidence or information requested and the pending litigation proceeding, is identified.

When the Hague Convention was enacted in Mexico (published on February 12, 1990 at the Federal Official Gazette), those requirements were established within the clarifications and reservations of the Mexican Government to the Convention

If the proceeding in which the electronic data would be used as evidence is in a court of a country that is not a party to the Hague Convention, the obtaining of evidence may be conducted following provisions of the Federal Code of Civil Procedures or the Code of Civil Procedures of the State in which the evidence is located, as appropriate. Most of the Codes of Civil Procedures of the States establish that foreign Letters of Request must be completed in accordance with the provisions set forth under the Federal Code of Civil Procedures. However, there are a few States that have their own regulations in this regard. In order to obtain electronic data in Mexico, it is necessary to comply with the following conditions set forth in the Federal Code of Civil Procedures (Articles 559 to 563) and the Commercial Code (Article 49 and 50) (if applicable):

- The evidence sought is related to an ongoing litigation proceeding;
- The order sought is not contrary to public policy. (The Supreme Court of Justice has established that the scope of concept of "public policy" has to be analyzed on a case-by-case basis);
- The documents sought are identified with reasonable specificity; and
- The Letter of Request was granted by a foreign court.

THE UNITED KINGDOM (ENGLAND AND WALES) • The discovery of electronic documents in the United Kingdom is governed by two different sets of rules, depending upon whether the discovery is in respect of proceedings in England or in respect of assisting proceedings in another country, for example, the United States. In this article, each is considered in turn.

E-Discovery For Proceedings In England

The United Kingdom Court rules were changed in October 2005 to incorporate new requirements for the disclosure of electronic documents. Like Canada, however, there are relatively few reported cases in the United Kingdom relating to e-discovery, and the English jurisprudence in this area is much less developed than in the United States. The approach to electronic discovery in the United Kingdom is underpinned by the country's attitude to discovery in general for hard copy and electronic documents. As a result, probably the biggest conceptual difference between the United Kingdom and the United States is in the scope of what is discoverable.

Scope Of Discovery

With the introduction in 1999 of new Civil Procedure Rules (CPR) largely devised by leading English judges, "discovery" was renamed "disclosure" and its scope was substantially reduced. They abolished the need to produce volumes of neutral background documents, and the need to produce documents that did not themselves affect the issues in the case (but which could lead to a "train of enquiry" to potentially relevant documents). Instead, the disclosing party is now usually required only to undertake "standard disclosure" and produce the non-privileged documents:

- On which it intends to rely;
- Which adversely affect its case or another party's case, or support another party's case; and
- That are required by a relevant practice direction.

CPR 31.4. A "document" is defined as "anything in which information of any description is recorded." This extends to electronic documents, including email and other electronic communications, word processed documents, and databases. The guidance explicitly states that "[i]n 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 back-up systems and electronic documents that have been 'deleted.' It also extends to additional information stored and associated with electronic documents known as metadata." CPR 31 Practice Direction, paragraph 2A.1.

In addition, all procedural steps, including disclosure, are subject to the court's overriding objective to do justice. One of the key factors in assessing what is just is the concept of proportionality. While the receiving party can apply for specific disclosure orders, the court normally requires such orders to be proportionate in terms of the likely importance of the documents, the amount in dispute, the ease and cost of production, and the financial positions of the parties. The following factors are relevant in assessing what is reasonable:

- The number of documents involved;
- The nature and complexity of the proceedings;
- The ease and expense of retrieval of any particular document; and
- The significance of any document that is likely to be located during the search.

CPR 31.7(2). The following factors are relevant to assessing the "ease and expense of retrieval":

- The accessibility of the electronic documents;
- The location of the electronic documents;
- The likelihood of locating relevant data;
- The cost of recovery;
- The cost of providing disclosure and inspection; and
- The likelihood that electronic documents will be materially altered in the course of recovery, disclosure, or inspection.

CPR 31 Practice Direction, paragraph 2A.4. This means in practice that English judges (and the parties' lawyers) tend to limit the scope of electronic disclosure very much more than they do in the United States and (to a lesser extent) than in Canada. Most standard disclosure in the United Kingdom is limited to online or active electronic documents created during a specified time period by specified personnel, and often to those documents identified by keyword searches. Each party is, however, required to specify the scope of its searches for electronic documents and to state what media was searched, the extent of the search, and whether searches were done by reference to keywords or concepts. It must also explain what electronic documents were not searched for, including documents before or after a specific date, documents on specified computer systems or media, and types of files. CPR 31.3 and CPR 31 Practice Direction, paragraph 2A.5. Searches for metadata, embedded data, or deleted files are relatively rarely undertaken when providing standard disclosure; when sought pursuant to a specific disclosure order, the applicant normally needs to limit its request to a limited type of electronic data and show that its production is strictly necessary for the fair disposition of the case.

As in the United States and Canada, litigants in the United Kingdom are under a duty to preserve documents at least from the time when litigation commences, and probably from when litigation is in contemplation. If a party fails to preserve electronic documents, this can lead to an adverse inference by the court that the party in default destroyed them because they were prejudicial to its case. *Douglas v. Hello! Limited* (No 3) [2003] 1 All ER 1087. Litigants are also under a duty to cooperate with regard to the disclosure of electronic material. *Digicel (St. Lucia) Limited v. Cable & Wireless plc* [2008] EWHC 2522(Ch). If there are disagreements, they

are expected to be raised at the first case management conference. CPR 31 Practice Direction, paragraphs 2A.2 and 2A.3.

Costs

Like Canada, and unlike the United States, the United Kingdom has a "loser pays" costs regime. Each party pays its own costs initially in producing its own disclosure and in inspecting that of the other parties. But the winning party normally recovers a good proportion (on average, about two-thirds in commercial cases) of its costs overall, including its costs of disclosure and inspection. This has made e-discovery costs-shifting orders less frequent in the United Kingdom than in the United States, although the English court retains a wide discretion as to the award of costs. It can order that specified electronic materials (including inaccessible data) be disclosed, and that the receiving party pay some or all of the disclosing party's costs of production.

Third-Party Discovery

Any application for disclosure against a person not a party to the proceedings must be supported by evidence and the court will only make such an order when the documents sought under this rule are "likely to support the case of the applicant or adversely affect the case of one of the other parties to the proceedings; and disclosure is necessary in order to dispose fairly of the claim or to save costs." CPR 31.17(3). The requesting party is normally required to pay the reasonable costs of production of the non-party. *Totalise plc v. The Motley Fool Limited and another* [2002] 1 WLR 1233. In addition, any party may serve a witness summons (subpoena) shortly before trial on a third party, requiring the third party to attend trial with specified documents.

E-Discovery In England For Non-U.K. Proceedings

The United Kingdom is a party to the Hague Convention. In order to give effect to the principles of the Convention, the Evidence (Proceedings in Other Jurisdictions) Act 1975 (the Evidence Act) was passed. The English High Court may order the taking of evidence in England and Wales at the request of a U.S. (or other non-U.K.) court pursuant to the powers under this Act. There is no inherent jurisdiction to act in aid of the U.S. court and the powers available to the English court are limited to the scope of this statute. The general principle that is followed in England in relation to a request from a U.S. court for assistance in obtaining evidence in foreign proceedings is to give effect to that request so far as is proper and practicable and to the extent that is permissible under English law.

The Evidence Act enables the English court to order the production of documents and the taking of depositions in England to support proceedings in the U.S. (or other countries). Although there are no reported cases under the Evidence Act regarding electronic documents, there is no doubt that the court's powers under the Act extend to electronic documents. The English court can make an order against anyone within its jurisdiction, whether or not they are parties to the U.S. proceedings.

The Evidence Act does not reproduce the provisions of the Convention but contains additional material and is drafted with the intention of being able to apply to all types of requests. An application to the English court for assistance in obtaining evidence for civil proceedings in a court outside the United Kingdom should be made pursuant to a request issued by or on behalf of the court outside the U.K. Section 1(a), Evidence Act. The English court must also be satisfied that the evidence is to be obtained for the purposes of civil proceedings that either have been instituted before the requesting court or whose institution before that court is contemplated. Section 1(b), Evidence Act. When the foreign proceedings have been settled or discontinued, the request will be refused. *Re International Power Industries Inc,* The Times, July 25, 1984 (1985) B.C. L.C. 128.

An application for an order under the Evidence Act must be made to the English High Court. CPR 34.16 to 34.24 and Practice Direction 34. It must be supported by written evidence and accompanied by a Letter of Request from the U.S. court as a result of which the application is made. The application is usually made without notice (ex parte) and an order granted and served on the disclosing party. If the disclosing party or other parties to the U.S. proceedings object to the scope of the order, the court will require a hearing at which it may confirm or vary or overturn any order made ex parte.

Scope Of Discovery

The application must be in relation to "proceedings in any civil or commercial matter" under both English law and the law of the U.S. court. Section 9(1), Evidence Act. While there is no internationally accepted definition of civil or commercial proceedings, for the purposes of English law this includes all proceedings other than criminal proceedings. In the absence of evidence to the contrary, the English court will accept the statement of the foreign court in its request that the evidence is required for the purposes of civil or commercial proceedings in that court.

The English court is not permitted under the Evidence Act to make an order for documentary (or oral) discovery that is wider than the steps that can be required to be taken for the purposes of evidence in English proceedings. Section 2(3), Evidence Act, giving effect to the United Kingdom's limitation to Article 23 to the Hague Convention. The scope of disclosure in English proceedings is set out above. The request must therefore not be of a wide-ranging "investigatory" nature, or seeking neutral background documents, or "train of inquiry" documents.

However, the scope of discovery under the Evidence Act is even more restricted. The English court cannot make a general discovery order to produce all relevant documents, as would typically be made in U.S. proceedings. Nor can the English court order that classes of documents be produced. The request must not be a wide-ranging "investigatory examination" or a "wish list" but must seek to obtain evidence for direct use in proceedings. *Re Westinghouse Electric Corp. Uranium Contract Litigation* [1978] AC 547 and *Honda Motor Company Limited and another v. Neesam and others* [2007] EWHC 581(Ch). The Evidence Act requires the documents sought to be "particular documents specified in the order." Section 2(4)(b), Evidence Act. The House of Lords (the U.K. equivalent of the U.S. Supreme Court) has ruled that these words are to be interpreted strictly:

- "Particular documents specified in the order" requires there to be "individual documents separately described." *Re Asbestos Insurance Coverage Cases* [1985] 1 All ER 716; and
- The applicant must produce evidence to satisfy the English court that the documents specified are actual documents that exist or have existed.

In that particular case, the House of Lords refused to order disclosure of the documents, which included:

- Written instructions from the respondents to obtain specimen insurance policies;
- Written instructions to obtain certain other specimen insurance policies; and
- Exemplars of certain excess comprehensive policies in use in the London insurance market during the period 1950-66.

With respect to the first two categories, it was held that these were conjectural documents that might or might not exist and there was no evidence that there was usually a single document or set of documents by which written instruction for policies were transmitted. The third category was refused as it was "clearly a description of a class of documents and not of particular documents." The class was

also not clearly defined and the policies could not be distinguished from policies of other firms, leaving the request far too wide to be given effect to by the English court. In this case, it was suggested that the Letters Rogatory should be sent back to the California court to be reconsidered by the judge with a view to them being amended and restricted.

This reasoning will no doubt be applied to electronic documents. Accordingly, requests for the disclosure of an individual's "inbox" of electronic documents, or "all emails passing between X and Y in respect of the contract" will be rejected by the English court. This is a key point in practice. It is vital for the Letter of Request from the U.S. court and the application to the English court to specify individual "particular documents," otherwise the English court will reject the request as being too wide. While the English court can make minor amendments to the request if drafted in a way it considers unacceptable, it has no powers to modify the original foreign request so as to substitute a category of documents different to those requested by the foreign court.

Data Protection And Blocking Statutes

The European Parliament and Council adopted the Data Protection Directive, which required European Union member states to introduce legislation to bring about the objectives of the Directive. Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of data.

These objectives were to protect the rights of privacy of individuals with regard to the processing of data (especially electronically held data), and to restrict the use and dissemination of that data. One of the key restrictions is the prohibition on sending the data outside the European Union to other countries with more liberal data protection laws (such as the United States). This Directive was enacted into U.K. law by means of the Data Protection Act 1998 (the Data Protection Act).

However, unlike in a number of other European Union member states, the United Kingdom has stipulated certain exceptions with regard to the processing of data that would otherwise come under the Data Protection Act. These exceptions include when "disclosure is necessary (a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or (b) for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights." Section 35(2), Data Protection Act. Accordingly, the U.K. Data Protection Act does not prevent electronic disclosure under the Evidence Act when such disclosure is necessary for the resolution of court proceedings. In addition, several European countries have blocking statutes that restrict the discovery of documents in foreign jurisdictions. The United Kingdom, however, has no blocking statute and instead relies on its limitation to Article 23 of the Hague Convention, and the resulting restrictions in the Evidence Act (discussed above).

CONCLUSION • Cross-border discovery presents unique challenges and considerations. The above presents an overview of the types of issues you must consider in matters reaching across international boundaries. As stated in the introduction, careful planning, research, and deliberate decision-making, along with consultation with local counsel in the relevant foreign jurisdiction, are the keys to approaching these challenging issues.