

CROSS-BORDER DISCOVERY

Evolving Issues and Challenges

THE HURON LEGAL
INSTITUTE

Global expansion of companies and technology developments such as cloud computing have significantly increased the likelihood that U.S. litigants will have data housed outside the country and will therefore be involved in cross-border discovery. The Huron Legal Institute recently hosted a Briefing in Houston to address some of the legal and practical issues related to cross-border discovery. The briefing was conducted by a panel of experts from corporate law departments, outside counsel, and state and federal judiciary,¹ anchored by Nigel Murray, Managing Director in Huron Legal's London office and moderated by Carolyn Southerland, Managing Director in Huron Legal's Houston office. The panel discussion focused on issues related to U.S. businesses seeking data kept in the European Union, since many other countries have followed the E.U. model to establish their own regulations. Some of the challenges are summarized here, along with a few practical take-away tips offered by the panelists.

OVERVIEW OF THE ISSUES

Stemming from fundamental philosophical dichotomies regarding the nature of “privacy” and the legal system and conduct of litigation, there are broad differences between how the U.S. and the E.U. address the processing of personal information. Because of these differences, efforts in U.S. litigation or investigations to discover data housed in the E.U. can be fraught with complications and can lead to possible sanctions or criminal liability in one or the other jurisdiction.

Historic Dichotomies

Fundamental to the issue of cross-border discovery (and a prevalent theme throughout the panel discussion) is the fact that there are numerous dichotomies between U.S. and E.U. culture, legal structure, and laws and regulation when it comes to data protection and privacy. These dichotomies and the laws that stem from them drive the tensions and problems that arise when attempting to obtain information from outside the U.S. The primary dichotomy is between some of the fundamental rights in the U.S. and Europe. In the U.S., free speech is one of the most fundamental rights. Elsewhere, by contrast, the right to privacy predominates. In Europe, the importance of privacy has cultural roots in World War II, where there was often a fear of being “turned in” by one’s neighbors, and where secret files were kept regarding individuals. This dichotomy carries forward to the treatment of corporate data. U.S. law assumes that corporations own the data they control, whereas in Europe there is no assumption that possession gives the holder any rights to data if it is “personal” in nature.

There is a dichotomy, as well, between the prevailing legal systems. The federal legal system in the U.S. and that of most of its states is based on the common law model, whereas in the E.U. and elsewhere, many countries have code-based legal systems. In the U.S., the judiciary is a separate branch of government, whereas in the E.U., courts are frequently part of the justice department rather than a separate branch of government. The U.S. promotes open

discovery in litigation, whereas in many other jurisdictions there is none. The standard for discoverable information in the U.S. is usually “reasonably likely to lead to the discovery of relevant or admissible evidence,” whereas in the U.K., the standard is for the disclosing party to disclose “those documents on which they rely and on which the other party or parties may reasonably rely.” This creates an atmosphere of different underlying views on obtaining information: in U.S. litigation, courts encourage open discovery between parties while in the E.U., not only is privacy protected, but if any of the E.U. Data Commissioners perceive privacy violations they are prone to share information about these violations with enforcement agencies.

Directive 95/46/EC

Discovery of personal data in the E.U. is governed by Directive 95/46/EC of the European Parliament and the Council of 24 October 1995. That Directive is designed to protect fundamental rights of natural persons – their privacy and personal data.² It directs the member states to implement provisions protecting these rights; consequently, while the underlying principles are the same among E.U. countries, each country has its own version of the protective law resulting in 27 variations.³ The data subject to privacy protection includes any information regarding identified and identifiable natural persons, ranging from identification numbers, address, and union membership to physical and psychiatric attributes. The protection may extend to the “processing” of such data, and in some countries processing can be so broadly defined as to include the preliminary review of data or even issuing a legal hold.

To further complicate matters, the playing field is changing. The E.U. Commission is expected to issue soon a new directive that is intended to improve and strengthen the protections as well as streamline the process by giving individuals clarity about their rights and how to protect them. However, because the Commission recognizes the conflict between the U.S. and E.U. approaches, an

umbrella agreement is planned to address the conflicting discovery rules. The two organizations working to develop protocols for that agreement include the Article 29 Working Party, comprised of E.U. Data Commissioners, and the Sedona Conference®, a non-profit organization that brings together leading jurists, lawyers, academics, experts and others to address challenging issues faced by the legal system and has been on the leading edge of examining discovery issues.

The E.U. Directive has served as a model for a number of other countries, including Russia, Canada, and Japan. China is expected to produce a similar act, and some Arab countries have rules to protect personal data as well.

Blocking Statutes

In addition to the privacy laws required by Directive 95/46/EC, several European countries have blocking statutes that prohibit the transfer of certain categories of data out of the country under any circumstances. These blocking statutes often pre-exist the newer privacy laws, and may or may not overlap in terms of the protected data.⁴ Some blocking statutes can trigger very serious sanctions when violated.

Jurisdiction

The conflict in discovery laws leads to the parallel problem of disputes regarding who has jurisdiction over cross-border discovery issues – the U.S. court where the underlying case is filed or the E.U. state where the data lies. The Hague Convention provides procedures for transmission and execution of Letters of Request for one contracting state to obtain evidence from another contracting state for use in judicial proceedings.⁵ Hague requests must be very specific in nature, unlike common U.S. requests for “all” and “every” bit of data.

In *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa*, 482 U.S. 522 (1987), a case involving the French blocking statute, the U.S. Supreme Court held that the Hague Convention was not intended to establish exclusive or mandatory provisions, but that parties seeking discovery located in a foreign nation have two options: the Federal Rules of Civil Procedure or the Hague Convention procedures. The court further set forth a “comity analysis” to determine which method should be used if the responding party requests the Hague procedures. Subsequent courts have refined the comity analysis⁶ and used it for a variety of discovery issues. See, e.g., *In re Global Power Equipment Group, Inc.*, 418 B.R. 833 (Bankr. D. Del. 2009), finding that the responding party had possession, custody, or control of the discovery because the party with possession of the data was a related corporate entity with agency status and was involved in the transaction at issue, and that the *Société Nationale* comity analysis weighed in favor of using the Federal Rules of Civil Procedure for obtaining discovery from the responding party.

Thus, U.S. courts where a lawsuit is filed and where the parties have appeared are likely to enforce U.S. rules of procedure regarding requests for discovery of information housed overseas, yet the countries where the information is housed may sanction parties who produce information protected by the privacy rules or without complying with the Hague Convention.

Safe Harbor

“Safe Harbor” has sometimes been raised as a potential aid to reconcile cross-border discovery issues. While safe harbor facilitates doing business cross-border and may be helpful in preliminary discovery considerations, Safe Harbor was designed to address day-to-day business operations, not litigation or discovery.

Directive 95/46 prohibits the transfer of personal data to non-E.U. nations that do not meet the European “adequacy” standard for privacy protection. Within E.U. countries, data protection is presumed “adequate” when business is conducted across E.U. borders, but there is no such assumption for business conducted between the U.S. and the E.U. In order to bridge the different privacy approaches and provide a streamlined means for U.S. organizations to comply with the E.U. privacy Directive, the U.S. Department of Commerce in consultation with the European Commission developed a “Safe Harbor” framework⁷ for eligible parties subject to the jurisdiction of the Federal Trade Commission or Department of Transportation. Among other things, compliance with Safe Harbor requires parties to have a privacy policy conforming to U.S.-E.U. Safe Harbor Privacy Principles that is posted and publicly available, as well as an independent recourse mechanism to investigate unresolved complaints and a mechanism for verifying compliance. Parties must reaffirm their self-certification annually to the Department of Commerce.

PRACTICAL TIPS

The panelists offered the following practical thoughts regarding how to deal with cross-border discovery challenges.

Laying the Foundation

- **Establish a good relationship with your organization’s IT team.** In-house counsel should be involved in issues involving data storage such as negotiations regarding outside storage. Additionally, make sure IT has the functionality -- policies and tools -- in place to address cross-border discovery issues when they arise.
- **Know what data your organization has and specifically where it is located before there’s any question of litigation.** Evaluate not only data maintained on company servers, but also data maintained by third-party vendors or in “the cloud.”

- **Carefully negotiate vendor contracts for external housing of data.** In some cloud computing arrangements data could be housed in multiple locations. IT tends to look at using unallocated storage in the most efficient way, without necessarily considering legal issues. It is important to know where the data will be housed and to carefully address issues such as getting the data back, access in the event of litigation, how the organization's data might be co-mingled with others', retention and data privacy policies, prior notification before giving data to third parties such as the government, and more.
- **Gain an understanding of the relevant laws and regulations for any countries where your organization has data.** If there are countries where the organization has a lot of data, find out now what the laws are, including what may fall within the definitions of "personal" or "processing," and carefully look at your retention policies and legal hold procedures in this context.
- **Make sure your organization is internally prepared and in compliance.** Make sure the organization is in compliance with the Safe Harbor provisions and certified accordingly. Safe Harbor does not ensure proper registration on a country-by-country basis, but does at least address a threshold. Remember, however, that Safe Harbor allows data to go back and forth within the organization in the ordinary course of business, but it does not address production to third parties.
- **Have a good records retention policy and execute it efficiently.** A good records and information management program goes a long way toward narrowing the amount of potentially relevant and responsive data, whether it is housed in the U.S. or out of country.

Handling the Matter

- **Develop a plan for how to deal with the issue of cross-border discovery in the event of litigation.** One panelist suggests that when there is a request for discovery of overseas data, develop a roadmap: first consider all U.S. rules that may come into play (for example, Fed. R. Civ. P. 26, 34, and 45, and 28 U.S.C. §1782). Then juxtapose those with the foreign jurisdiction's data privacy rules, doing research on the individual country's twists on the E.U. directive.
- **Engage local counsel.** Engage local counsel who is knowledgeable about the country's rules and procedures.
- **Once there's litigation, act early: bring to the court's attention any potential cross-border discovery issues as early as possible before the discovery deadlines.** Not only should you let the judge know of the potential issues, be sure you have briefing available to educate the judge regarding the issues and the relevant laws, including those that may affect

the ability to issue a legal hold, process information, etc. For some courts, it may even be possible to raise the issue before litigation actually arises.

- **Evaluate the nature of the potentially responsive information.** Is it important? Can it be found elsewhere? Where is it housed? An early evaluation of this nature can help minimize issues further down the line.
- **Consider less intrusive measures of responding.** Consider in-country processing or review of data, or review within the E.U. if appropriate. Cull and limit the data as much as possible, so that the only data being exported is the most relevant, least personal information. But remember that the privacy rules also apply to "processing" personally identifiable information, so review in place may even be considered a violation. Carefully consider who will review the information and how.
- **Consider obtaining consents from those individuals whose data is affected.** It is always a good idea to remember the human factor. Many blocking statutes are invoked by individuals. Note that a blanket consent as a condition of employment may not be sufficient, since many laws require consents to be very specific.
- **Use protective orders and confidentiality agreements to the extent possible.** Every effort should be taken to protect personal data. Consider using protective orders and confidentiality agreements regarding the information that is ultimately transferred, as well as differently "branding" the private data before it is sent.

Keeping Order

- **Document what is transferred and the details.** It is a good idea to be very clear regarding what information is collected and transferred, how that process is done, what security measures are in place, and other relevant information.
- **Address what will happen to the data once the litigation is over.** Once the litigation has ended consider the process for handling the data – how will it be secured? Will it be returned or destroyed? Factor these issues into external vendor contracts as well.
- **Capture lessons learned.** Incorporate any insights gained from the matter into the organization's best practices for managing international matters.

NOTES

¹ Other panelists included Gail Foster, Baker Botts LLP; Browning E. Marean III, DLA Piper US LLP; Margaret C. Mousoudakis, LyondellBasell Industries; Hon. James M. Rosenbaum, JAMS; Carter J. White, Ph.D., M-I SWACO, a Schlumberger Company; Jennifer B. Williams, Vinson & Elkins LLP; and Hon. John T. Woodridge, Baker Hughes Incorporated.

² To read the directive, see <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

³ See <http://www.huronconsultinggroup.com/eudata.aspx> for information regarding individual countries' laws.

⁴ For example, the French blocking statute prescribes sanctions for certain parties -- natural persons with French citizenship or residency, or directors, representative, agents or employees of legal entities with registered offices or branches in France -- who disclose information while participating in foreign discovery without going through the Hague procedures. See French Penal Code Law No. 80-538.

⁵ For the text of the *Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters*, please see http://www.hcch.net/index_en.php?act=conventions.text&cid=82.

⁶ See *Strauss v. Credit Lyonnais, S.A.*, 249 F.R.D. 429, 454-56 (E.D.N.Y. 2008).

⁷ For more information on the Safe Harbor framework, please see <http://export.gov/safeharbor/index.asp>.

To learn how Huron Legal's solutions can deliver value for your organization, contact us at **1-866-229-8700** or huronconsultinggroup.com.