

Corporate Counsel

Litigation Management

Global Discovery—What U.S. Companies Need to Know



*Contributed by Kenneth Prine and Kathryn Johnson,
Redgrave LLP*

- **Cross-border litigation may present discovery issues for the parties involved, such as conflicts between U.S. discovery rules and foreign data and privacy protection laws.**
- **The Hague Convention of 1970 establishes an international framework for cross-border discovery without the need for utilizing diplomatic channels.**
- **Legal departments of U.S. companies should prepare for cross-border discovery and develop good lines of ongoing communication with their legal and IT colleagues abroad.**

The increasing globalization of business continues to thrust U.S. companies into discovery relating to documents and information that are located in other countries. Global discovery presents unique challenges for companies as they seek to comply with both U.S. and foreign legal requirements. Common law states, such as the United States, tend to have more expansive discovery practices, while civil law States, including most EU member states, have more restrictive discovery practices. This article

briefly discusses some of the issues that companies should be aware of with respect to global discovery, provides an overview of the Hague Convention procedures, and concludes with practical suggestions to streamline global discovery efforts by building bridges between U.S. and foreign company personnel.

Discovery in U.S. litigation arguably has the broadest scope of any country. Parties are allowed to seek discovery on documents, information, and things that are relevant to any party's claim or defense and the information to be discovered need not be admissible, but only must appear to be reasonably calculated to lead to the discovery of admissible evidence.¹ In practical terms, U.S. discovery can seem like a wide-ranging inquiry that sweeps in a large volume of information that is not, itself, admissible evidence. This approach to discovery may very well be novel and difficult to understand for a company's foreign-based personnel. Further, there are few court rules or other regulations that meaningfully reduce the volume of information that is subject to discovery. In a real sense, there is a general presumption in the United States that information is properly discoverable. In much of the rest of the world, that presumption is reversed—and is expressed in various data transfer and data protection regulations.

The practical effect of foreign regulations that prohibit the transfer of data or that impose strict privacy standards is that companies that are engaged in U.S. litigation often find their discovery obligations to be at odds with the local regulations where certain personnel or information resides. Companies cannot merely ignore the data transfer and data protection regulations of foreign countries in which they operate. At the same time, U.S. courts are generally not persuaded to limit a party's discovery obligations simply because some of the discoverable information is protected by foreign regulations. The prevailing notion is that if a company is doing business in a U.S. jurisdiction, then it must abide by U.S. court rules, regardless of whether those rules create difficult situations for the company with respect to its foreign-based data.

Originally published by Bloomberg Finance L.P. Reprinted with permission. Bloomberg Law Reports® is a registered trademark and service mark of Bloomberg Finance L.P.

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.

The primary types of foreign regulations that limit a U.S. company's use of foreign-based information are local blocking statutes and EU Member State regulations that implement Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (EU Privacy Directive). The blocking statutes and data protection regulations vary country by country. While the specific scope of each country's statutes is beyond the scope of this article, there are common elements that companies should be aware of.

Privacy Regulations

The EU Privacy Directive provides that Member States shall implement regulations that are designed to give certain levels of protection to the processing of personal data, among other things. Both "processing"² and "personal data"³ have definitions that are broader than what U.S. companies may be accustomed to. In general, the data protection regulations permit the unrestricted transfer of data within the EU, but prohibit the processing and transfer of personal data to jurisdictions that do not provide the same level of data protection as the jurisdiction where the data resides.

The United States generally is not considered by the EU to provide adequate levels of data protection. Therefore, if companies are seeking to move information from EU countries to the United States for discovery purposes, they will need to satisfy the data protection requirements of the jurisdiction where the information is located.

Blocking Statutes

Blocking statutes are designed to prevent the transfer of certain types of information across territorial borders. The specific types of information may vary, but generally blocking statutes apply to more than just personal information. Many blocking statutes carry the threat of both monetary and criminal penalties.

For example, France's blocking statute, Law no. 80-538 of July 16, 1980, is designed to prevent evidence being taken from France for extraterritorial judicial proceedings upon threat of imprisonment and fine.

Article 1 of the Blocking Statute provides:

Subject to international treaties or arrangements, it shall be prohibited for any individual who is a French citizen or has his usual residence in France and for any senior officer, representative, agent or employee of a legal entity having its registered office or a branch in France to disclose to foreign public authorities, whether in writing, orally or otherwise, in any place whatsoever, any economic, commercial, business, industrial, financial or technical documents or information, if such disclosure might impair French sovereignty, security, essential economic interests or public order.

Further, Article 1A adds:

Subject to international treaties or arrangements, it shall be prohibited for any individual to request, seek or disclose, whether in writing, orally or otherwise, any economic, commercial, business, industrial, financial or technical documents or information, if such actions aim at establishing evidence in view of foreign judicial or administrative proceedings, or in the framework of such proceedings.

As to penalties for violation, Article 3 provides:

Without prejudice to any greater penalties provided by law, any violation of the provisions of articles 1 and 1 bis of this law will be punished by imprisonment of [six months] and by a fine of [18,000 euros] or by only one of these two penalties.

Companies must bear in mind that it is not sufficient to satisfy just the data protection authority or to comply with the local blocking statute. Companies must satisfy both. For example, in 2009, the French Data Protection Authority, the Commission Nationale de l'Informatique et des Libertés (CNIL), issued a deliberation⁴ wherein it reminded companies that compliance with the Hague Convention does not, at the same time, satisfy the CNIL's requirements regarding data transfer outside of the EU. The CNIL was clear that it does not cede its data protection mandate to following the provisions of the Hague Evidence Convention (discussed below).

Approaches to Global Discovery

Despite the general limitations on data transfer and the heightened privacy protections in many other countries, U.S. companies do have some options for complying with both their U.S. discovery obligations and the local regulations that govern their foreign-based information. The Hague Evidence Convention, discussed below, is the primary international agreement to which the United States is a signatory that addresses the transfer of information from one country to another for use in litigation.

Hague Evidence Convention

One attempt to facilitate cross-border discovery and improve cooperation between countries is the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (Hague Convention). Drafted in 1970, the Hague Convention establishes an international framework for cross-border discovery without the need for utilizing diplomatic channels. More than 47 States are signatories to the Convention, including the United States, Australia, and most EU Member States.

In order to pursue discovery using the Hague Convention, one must first determine whether or not the country in which the potential evidence resides is signatory to the Convention. A Letter of Request should be submitted (in English or French, unless the

country specifically requires translation into another language) to the Central Authority in that country. The letter should detail, at a minimum, the requesting authority, the parties to the matter, the specifics of the matter, and the evidence requested. Especially if the evidence resides in a civil law State, the evidence requested should be limited in scope and specifically applicable to the matter at issue. If the Central Authority determines that the letter complies with the Convention, they will forward the letter to the authority within the country that is able to execute the request. Article 9 of the Convention requires that the “Letter of Request shall be executed expeditiously.”

The Hague Convention allows signatories to refuse to execute Letters of Request under certain circumstances. Article 12 limits this refusal to situations where: 1) the execution of the letter would fall outside of the functions of the judiciary in the executing State, or 2) execution of the letter would be contrary to national security or sovereignty in the executing State. However, the target of the letter could also refuse to provide the evidence if it determines that it has a duty to refuse based on: 1) the laws of their State, or 2) the laws of the requesting State. Also, States are specifically allowed to refuse to execute pre-trial discovery Letters of Request (and many States have declared this refusal). Conflicts between States regarding Hague Convention procedures are to be resolved through diplomatic channels.

In practice, once a court mandates use of the Hague Convention (or the parties agree to such a course of action), the parties should cooperate in drafting documents that support the U.S. court’s request to the Central Authority in the country where the information resides. Supporting documents should include a clear statement of the relevant facts, such that the Central Authority has sufficient understanding of the case to make an informed decision as to whether to permit discovery of the requested information. Another helpful supporting document is a list of requests that are tailored to the facts and claims in the case.

Practical Guidelines

Legal departments in U.S. companies can take practical steps now to be prepared for cross-border discovery. U.S. legal department personnel (attorneys, paralegals, and other litigation support personnel) should develop good lines of ongoing communication with their foreign Legal and IT colleagues. The intra-company relationships that U.S. Legal personnel have with their foreign-based colleagues will ease the process of global discovery for U.S. litigation.

IT Colleagues

One place to begin the dialogue with foreign-based IT colleagues is to understand the company’s global information systems. After the 2006 Amendments to the Federal Rules of Civil Procedure, many company’s developed “data maps” to help the legal

personnel to understand where the company’s information was located. In order to be proactive in preparing for global discovery, a company may wish to develop similar data maps that describe the locations of foreign-based data. It would be imprudent for legal personnel to assume that the company’s global IT environment mirrors that of the United States—especially in the case of companies that are based outside of the United States. Developing a global data map can assist the company to track where foreign-based documents and information are located, and can identify the foreign-based IT personnel who will be crucial to the success of future discovery efforts.

Good working relationships with foreign-based IT colleagues will also be critical for successfully preserving data that may need to be preserved for discovery purposes (assuming resolution of the data protection and data transfer issues described above). A company’s foreign-based IT personnel need to understand what the U.S. legal team needs for data preservation, as well as how quickly the preservation measures may need to be put in place. In some cases, foreign-based IT personnel may be needed to provide answers to interrogatories or to provide other information for the defense of the case.

Further, if company information is to be collected, processed, and reviewed in locations abroad, the local IT personnel could be valuable in working with the company’s vendors for those services.

Legal Colleagues

With respect to pending or reasonably anticipated litigation, companies will be held to the same standards for preservation, collection, processing, review, and production for their foreign-based information as they will be for information located within the United States. The practical effect of these standards is that a company should make sure that its litigation hold and data preservation processes reach to foreign-based personnel and information. Cooperation from the company’s foreign-based legal personnel will often be crucial to the success of litigation hold and preservation efforts.

Depending on the personnel involved with the U.S. litigation, the foreign-based legal personnel may be needed to assist with such things as custodian data identification interviews and securing proper consent for the processing and use of their personal data.

Conclusion

U.S. companies with foreign-based personnel and operations are well-served to be proactive in learning about their foreign-based information environment and with building discovery processes and working relationships between U.S. and foreign-based legal and IT personnel. Building the global discovery processes and relationships before the onset of litigation will help the company

to reduce its risk of failing to take the necessary steps for data preservation, while avoiding the extra expense that also seems to accompany projects that are done under the pressure of an active case.

Kenneth Prine is a partner in Redgrave LLP's Minneapolis office. Kathryn Johnson is an analyst in Redgrave LLP's Minneapolis office.

¹ Fed. R. Civ. P. 26(b)(1).

² Article 2 (a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

³ Article 2 (b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

⁴ Deliberation No. 2009-474 of 23 July 2009 concerning recommendations for the transfer of personal data in the context of American court proceedings known as "discovery."