Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Tips For Managing Int'l Privacy Issues In E-Discovery

Law360, New York (November 04, 2013, 12:52 PM ET) -- An international banking organization with offices in both the United States and France is sued in the United States for fraud. Much of the data relevant to the United States litigation is located on centralized servers in France, although the data can be accessed by individuals in the United States. The organization is unsure if it can produce that data in the United States litigation without running afoul of France's data privacy laws and blocking statute.

Data Consolidation and Globalization

It is not uncommon for information — including electronically stored information — sought in discovery in U.S. legal proceedings to be located outside of the United States. Access to such information is complicated by the differing perspectives of various foreign jurisdictions toward the discovery or disclosure of such information. In addition, the movement toward cloud computing models has the potential to further complicate the legal questions that arise in connection with U.S. discovery.

International Data Privacy and E-Discovery

While the United States has a discovery system that encourages extensive production of information, many other countries have far more protective schemes. In particular, the European Union member states have detailed data protection laws based on the EU's Data Privacy Directive. Those laws tightly regulate when and how personally identifiable information (which encompasses a broad range of information including name, age, gender, marital status, nationality, citizenship, veteran status, personal or business contact information and identification numbers) may be collected, processed, stored and transferred by an organization.

In January, 2012, the European Commission outlined plans to update the EU's existing data protection law regime by establishing a single framework of data protection throughout the European Union. The plans call for bringing within the scope of the EU data protection rules those businesses based outside of the European Union but that target EU citizens. Recent reports state that the new EU data protection rules and a new cybersecurity framework are to be adopted by early 2015.

In addition, several European countries have enacted blocking statues designed to protect sovereignty and shield foreign nationals from intrusive U.S.-style litigation. Violations of these foreign laws may result in serious consequences for the organization, including criminal charges. Taken together, these laws create a tension between the mandate of the U.S. Federal Rules of Civil Procedure to produce all relevant electronic records and the laws of other countries regulating discovery and transmission of ESI.

There are several questions an organization will face in determining whether data located abroad must be produced in a U.S. litigation. First, what are the conditions under which ESI "stored" outside of the United States is deemed to be in a domestic party's "possession, custody or control" under the Federal Rules of Civil Procedure? Consistent with the emphasis on full disclosure in the American legal system, U.S. courts construe the term "control" broadly. Thus, a party has control if it has the legal right, authority or practical ability to obtain the materials sought upon demand.

Second, does the applicable foreign law permit the processing, transfer and production of overseas ESI? The answer to this question will depend on location of the data and the laws of the country at issue.

Third, will the U.S. courts require the production of relevant data regardless of any foreign restrictions? The answer to this question is generally yes, although U.S. courts have been more willing to give deference to restrictions arising from data privacy laws than those arising from foreign blocking statues.

Best Practices for Managing International Data Privacy Issues in E-Discovery

Because the U.S. courts tend to require the production of relevant data in an organization's possession, custody and control regardless of any foreign restrictions, it is helpful for an organization to consider the best ways to ensure that it can meet both its U.S. and foreign legal obligations. As with any effort to manage and minimize risks, the best practice is to evaluate those risks before litigation arises and implement standard controls.

Know Your Data and Your Legal Obligations

Every organization should be familiar with the laws governing its data and how that data may be collected, processed, retained or transferred before litigation commences. Involving local counsel and data privacy professionals in the litigation process will help to minimize the risks associated with the collection, processing and transfer of data in connection with U.S. litigation and ensure that the organization does not violate its local rules and regulations. This is particularly important given the proposed changes to the EU data protection rules.

Limit Collection

The best way to minimize the risks associated with collecting, processing and transferring data located abroad in connection with a U.S. litigation is to limit the scope of the data at issue. Litigation counsel should negotiate the scope of data to be produced with opposing counsel in an effort to reduce the amount of unnecessary and nonresponsive data collected. And an organization should consider implementing collection procedures that are specifically targeted at identifying relevant data from the outset, rather than employing a broad collection philosophy and relying on the review process to narrow the data for production.

Consider On-Site, In-Country Review

In some instances, an organization may facilitate its ability to collect and process data relevant to a U.S. litigation by conducting the review in the country in which the data resides. This review will help to identify only the information that is actually relevant to the U.S. litigation before it is transferred, and may minimize the quantity of personally identifiable information at issue.

Consider Redaction or Anonymization

Even where data located abroad is relevant and must be produced in a U.S. litigation, it may not be necessary to produce the portion of that data that constitutes personally identifiable information. Use of anonymization techniques or redaction of personally identifiable information may address an organization's data privacy obligations.

Evaluate Transfer Options

An organization must remember that it retains responsibility for ensuring that personally identifiable information is protected in accordance with the laws of its place of origin, even after the data is transferred to the United States. There are various options for such transfer, including use of "safe harbor" vendors, employing the Hague Evidence Convention procedures, negotiating vendor contracts that include model contractual language or other provisions designed to ensure the data protection, or implementing strict protective orders.

--By Edmund Sautter, Mark C. Hilgard and Kim Leffert, Mayer Brown LLP

Edmund Sautter is a partner in Mayer Brown's London office. Mark Hilgard, Ph.D., is a partner in the firm's Frankfurt office. Kim Leffert is counsel in the firm's Chicago office. They are members of the firm's litigation and dispute resolution practice and the electronic discovery and records management group.