MAYER·BROWN

Electronic Discovery & Records Management

TIP OF THE MONTH

May 29, 2009

Managing International E-Discovery Conflicts: Liberal US Discovery Rules Meet Foreign Data Protection Laws

Scenario:

A multinational corporation is a defendant in a products liability action in a US federal court. During discovery, the plaintiffs request production of relevant emails from employees of an overseas affiliate of the defendant who are stationed in the Netherlands, France and Germany.

Discovery Issues Associated with Foreign Data Protection Laws

Foreign data protection laws present unique and potentially serious issues for multinational companies involved in government investigations or civil discovery. Whereas the principal e-discovery challenges within the United States involve how a party can best meet its obligations to preserve, collect, review and produce relevant data, an increasing number of foreign jurisdictions prohibit or restrict these very activities. This presents significant practical hazards as e-discovery instincts that might seem standard within the United States — such as collecting and reviewing a broader collection of data than might be strictly required — could lead to violations of foreign law. US courts have, to date, been reluctant to relax parties' obligations to respond to discovery, even where compliance with US discovery obligations might result in a violation of foreign law.

Differing Conceptions of Discovery and Privacy

At the root of these conflicts between US and foreign law are differing fundamental approaches to two key questions.

Pretrial Discovery: Whereas US rules of civil procedure permit broad pretrial discovery with minimal participation by the court, most other countries have much more restrictive views of the proper scope (and cost) of civil discovery, and often require direct court involvement in discovery.

Employee Privacy: Whereas US employees are generally deemed not to have an "expectation of privacy" with respect to email and other data created and stored on an employer's computer system, this view is not widely shared overseas.

Foreign Statutes and Regulations

In recognition of these differences, and in some cases for the express purpose of protecting citizens from the burdens of litigation discovery, many foreign countries have enacted strict privacy regulations and

discovery "blocking" statutes.

The most prominent such regulation is the European Union's data protection directive. Adopted in 1995, the directive, together with the implementing laws of the various EU member states, restricts the "processing" and overseas transfer of "personal data." The definitions of "processing" and "personal data" are broadly worded, and might be read to restrict even the preservation of data (as well as any subsequent filtering and review) and to apply to any document that contains so much as an individual's email address. While a number of exceptions may permit the processing and transfer of data under some circumstances (e.g., unambiguous consent of the individual in question, or where it is necessary for the purposes of "legitimate interests" of the employer), the scope of these exceptions is the subject of significant uncertainty.

It is important to note that the EU's data protection directive applies to all overseas transfers of personal data, including a multinational corporation's voluntary transfer of its *own* protected information to the United States for disclosure in discovery. Also, while US privacy concerns often can be assuaged by the entry of a stipulated protective order limiting the recipient's use of confidential employee information, this solution alone generally will not satisfy the requirements of foreign data privacy laws.

Foreign blocking statutes can be more straightforward — simply prohibiting any activities in furtherance of foreign discovery proceedings. For example, a French statute prohibits "requesting, seeking, or disclosing in writing, orally, or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature for the purposes of constituting evidence in view of foreign judicial or administrative proceedings." In a rare reported case of enforcement of this statute, a French lawyer was recently fined €15,000 for seeking discovery in France in response to a US court order.

US Courts Enforcing Discovery Obligations

Despite the restrictions imposed by foreign law, US discovery obligations, which extend to all materials within the "possession, custody or control" of a party to a US litigation, may still require production of overseas data. US courts have been reluctant to recognize foreign data protection laws as insurmountable obstacles to the gathering of responsive information stored overseas. As one court recently observed regarding electronic discovery of data residing in the Netherlands:

It is well settled that foreign blocking statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce (let alone preserve) evidence even though the act of production may violate that statute.

US courts will apply a balancing test if called upon to determine whether to enforce discovery obligations in the face of a foreign blocking statute. Factors considered include: How important is the information? How narrow is the request? What is the impact of noncompliance with the foreign statute on the foreign state's interests? Further, although the authority exists to order production, US courts are unlikely to enforce those orders through sanctions if the failure to comply is due to a legal proscription and there is no evidence of "willfulness, bad faith, or any fault of" the party subject to the discovery.

In general, the possibility of fines and other remedies under foreign blocking statutes has not led US courts to relieve parties of their obligation to produce evidence located in foreign countries.

Managing the Catch-22

Where does that leave the multinational corporate defendant when faced with the possibility of being caught between conflicting laws in the United States and abroad? Upon receipt of a discovery request relating to data that resides in a foreign country, the defendant might consider the following steps before acting to preserve or collect the foreign data:

- Confirm that the data are within the party's possession, custody or control, and determine the physical location of the data in question, as well as the jurisdiction of employment of the individual data custodians.
- Consult with counsel in the relevant jurisdictions regarding the scope of privacy and data protection laws, and regarding potential alternate means of obtaining discovery in those jurisdictions, such as Hague convention procedures or local government consent.
- If a conflict is identified, consider conducting an initial internal "balancing" of the risks and benefits of compliance with US discovery obligations versus compliance with foreign law. Is voluntary production appropriate notwithstanding foreign law? Would production be appropriate only if compelled by the US court? Is there a reasonable basis to resist production?
- If the decision is made to preserve, collect, review and produce the data in question, consider strategies to minimize the risk of being found in violation of foreign law. Depending on the circumstances, effective measures might include some combination of the following: (i) obtaining consent of affected individuals, (ii) minimizing the volume of affected data through early use of narrowly tailored search terms, (iii) redacting personal identifying information from the data, (iv) minimizing the quantity of data transferred by conducting the review in the host country, (v) using protective orders and certified vendors in the United States to ensure the continued security of the data following transfer and production.

While courts in and outside of the US may always have different rules and norms regarding discovery, being aware of and planning for the differences will make facing international e-discovery issues easier.

For inquiries related to this Tip of the Month, please contact the authors, Joseph Baker at jbaker@mayerbrown.com, Kim A. Leffert at kleffert@mayerbrown.com,or Edmund Sautter at esautter@mayerbrown.com.

Learn more about Mayer Brown's Electronic Discovery & Records Management practice or contact Anthony J. Diana at adiana@mayerbrown.com, Michael E. Lackey at mlackey@mayerbrown.com, Thomas A. Lidbury at tlidbury@mayerbrown.com or Edmund Sautter at esautter@mayerbrown.com.

Please visit us at www.mayerbrown.com