Pitfalls of Global E-Discovery

For companies involved in legal proceedings, U.S. disclosure requirements can collide with global privacy and data protection laws, leaving businesses in a no-win situation. **BY TERA RICA MURDOCK**

Data protection and privacy laws have proliferated outside of the European Union, particularly in South America and Asia. These laws often regulate data transfer outside of a country’s borders as well as the processing of data, including failure to delete data after a certain time.

Conflict with these laws can occur when multinational companies or foreign companies become involved in litigation in the United States. U.S. courts have a system for preservation and disclosure of potentially relevant evidence by parties and non-parties. If a party fails to preserve relevant evidence, a court can issue sanctions. If a party refuses to disclose potentially relevant documents or data, a U.S. court can compel disclosure through court order.

This can place multinational companies or foreign companies in a situation where they are faced with either violating laws of one country or violating a court order in the United States. To mitigate the risk of being placed in such a situation, foreign and multinational litigants should be aware of data protection and privacy laws, and should sensitize employees to the ways in which data protection and privacy laws may be violated during litigation. These potential issues should be raised early in litigation.

**GLOBAL DATA LAWS**

The European Union enacted its Data Protection Directive in 1995. The directive requires each member state of the EU to enact its own body of law implementing the framework of the directive. The directive created a new set of terminology that other countries have adopted when creating privacy laws. Rather than being directed at a particular business sector — like medical records or credit reports — the directive regulates all personal data. Generally, “personal data” means information about any identifiable natural person, who is known as the “data subject.”

The directive applies to “processing” of personal data, which means any operation performed on personal data, including collection, storage, retrieval, use or dissemination. The directive sets out data quality principles that must be met when processing personal data, which includes destroying data when obsolete. The directive also states that the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited, unless the data subject has consented or in certain specific circumstances.

Countries in South America have followed the EU model in that they have enacted omnibus data protection laws, rather than sector-specific laws like those in the United States. They have also tended to use the terminology created by the EU directive. Argentina, Chile and Uruguay each have longstanding data protection laws that require disclosure from the data owner or consent from the data subject in certain situations when data is processed or transferred.

Colombia and Peru enacted data privacy laws in 2012 and 2011, respectively. Under these laws, before any information relating to a data subject can be collected, the data subject must give prior, informed consent. Further, the transfer of data to any countries that do not provide appropriate levels of privacy protection is prohibited. Colombia’s law sets forth a right for data subjects to know, update and correct their personal data. Peru’s law also provides data subjects with a right of access to data, and — similar to Colombia — a right to update, include, rectify or eliminate data.

While Brazil does not have a specific statutory regulation governing data transfer, a variety of laws, as well as the Brazilian Constitution, provide Brazilians with certain rights with respect to data collection. A Data Protection Bill similar to the EU directive has been proposed to the Brazilian legislature that would address data transfer and establish a Data Protection Authority with the power to issue sanctions.

In Asia, Hong Kong, India, Japan, South Korea and Taiwan have each enacted comprehensive data protection legislation. Countries in Asia that have enacted data protection laws have also focused on the impact that data processing or transfer can have on national interests. For instance, while China does not have comprehensive national legislation regarding data protection, the Law on Guarding State Secrets may have an impact on data processing, particularly where it involves transferring data outside of China. This law contains a catch-all category that includes anything identified as a state secret by national or local authorities. Whether a violation of the Law on Guarding State Secrets is intentional or negligent, the criminal code provides for a sentence of up to seven years.

**UNIQUE U.S. REQUIREMENTS**

Litigation in the United States operates on a broad system of disclosure through discovery. Under the rules of civil procedure of the various state and federal courts, the discovery process requires disclosure of all information that is relevant to a party’s claim or defense, including information that appears reasonably calculated to lead to the discovery of admissible evidence. Corresponding with this system of disclosure is a common law duty to avoid intentional or negligent withholding, hiding, altering or destroying of evidence and to preserve relevant documents.

If a party refuses or fails to disclose relevant data, the court may impose sanctions against the party or parties involved. These sanctions can range from monetary fines to the imposition of a contempt of court order. In some cases, the court may also award costs and attorneys’ fees to the party that prevails in the case.

**Summary**

- The EU's Data Protection Directive regulates the ‘‘processing’’ of all personal data.
- Many countries outside the EU have laws that are equally stringent.
- U.S. court disclosure requirements often conflict with global data protection laws.

GLOBAL COMPANIES involved in litigation in the United States may unintentionally violate data protection laws meant to protect the privacy of citizens in other countries.
documents, a court may compel disclosure through a court order. If a party then fails to comply with the court order, the court may order payment of attorney’s fees or costs, instruct the jury to make an adverse inference, dismiss the action, strike defenses, render a default judgment in favor of the plaintiff, or treat the failure to obey the order as contempt of court. Litigants that fail to preserve evidence may also face these same sanctions.

PRIVACY VS. DISCOVERY
A litigant that faces cross-border discovery decisions may see a conflict between data protection laws and discovery rules. As an example, suppose that a company is headquartered in the United States but has an office in a foreign country with data protection laws. A manager located in the foreign office supervises a U.S. employee, and makes a decision to fire that employee. The employee sues for discrimination in a U.S. court.

Once the company reasonably anticipated litigation, it would be required to preserve information potentially relevant to the litigation. This could potentially include the email of the manager in the foreign office. But what if the data protection laws of that foreign country required data to be deleted once it became obsolete? Preserving the e-mail could then be in conflict with the data protection laws.

Further, what if the manager had a right to update, rectify or eliminate data, as a data subject does in Peru? Any suggested change by the manager would violate the preservation duty required by U.S. courts. Finally, what if outside counsel downloaded the manager’s email to a hard drive and shipped it to their office in the United States for review and disclosure in discovery? This could be both processing of data and transfer of data to a third country, and could potentially conflict with data protection rules.

MITIGATING RISKS
Multinational companies, companies with foreign offices, and companies that store their data overseas in countries with stringent data protection laws should work proactively on the potential conflict. Before litigation ever begins, companies should educate employees about these possible issues. Employees outside of the United States should be informed of the obligations that apply in U.S. litigation. Employees, including general counsel, risk management and information services, should be trained regarding the privacy protections that may apply overseas.

In addition, companies should determine whether the data protection laws of a particular country allow it to obtain consent from data subjects to vary from deletion requirements (in order to allow for preservation) and from prohibitions on transfer. This should be done when employment begins or in advance of the event that requires data processing. If consents are obtained, they should be reviewed again if processing is ever required.

When litigation begins, counsel should evaluate these issues and consider contacting the foreign country’s data protection authorities or persons responsible for enforcement of data protection laws. In such an event, data protection authorities may be able to provide a protocol.

If a country’s laws prevent publication or dissemination and use, you may consider asking the U.S. court for a protective order that imports that foreign law. It can be difficult to maintain information confidentially in litigation because of laws requiring public access to courts and the First Amendment. A protective order negotiated by the parties and entered by the court can maintain personal privacy and provide an equivalent protection afforded by the foreign nation.

Finally, even with best efforts, a company may not be allowed to produce potentially relevant information in the United States because of a foreign country’s data protection laws. In such an event, counsel for the company should educate the court about the data protection laws, and detail the company’s good faith attempts to comply and support for its decision not to produce data.

Your New Wholesale Family
Brokerage. Underwriting. Programs. The new CRC family of companies delivers. Across our eight wholesale-dedicated brands, we have experts who can place risks of any size for nearly any industry.

Our 54 offices, 1,700 employees, and 300 brokers and underwriters wrote more than $4 billion in premium last year. We are ready to introduce you to our growing family and say, “Welcome home to the new CRC!”

www.crcwholesalegroup.com

©CRC Insurance Services, Inc. CA license 0778135