

## The Discovery Standard

### Discovery News

[nt](#)

#### FEATURE STORIES

## Framing the International E-Discovery Issues: Data Across the Globe

*Courtney Ingrassia Barton, Esq., Vice President, Industry Relations*

We live in a global business community fueled by advances in communication technology. An email can travel just as quickly from New York to London as it can from Madison Avenue to Park Avenue. But the ability to conduct business seamlessly across borders raises some very interesting issues about which legal system governs these transactions. Nowhere is this more complicated than in the world of e-discovery. In some countries, data, especially personal data, are sacrosanct. Conflict of laws issues related to data collection, processing and review all arise when those activities are conducted abroad and become even more complicated when data is removed from its home state.

Fueling the international conflicts are the attitudes abroad about the U.S. discovery process underscored by less liberal rules in other countries that see the American need for discovery as not only an invasion of privacy, but also an attack on foreign sovereignty. Of largest concern to those who litigate internationally is the EU Data Protection Directive (Directive 95/46) which restricts the transport of personal data to countries that do not have in place proper safeguards to protect that information. Although there are a variety of ways to comply with the Directive, other, more stringent laws, such as the French Blocking Statute, which imposes criminal liability for data transportation, are equally concerning. The solutions fashioned by the U.S. Courts to address these issues provide little comfort, as the U.S. Courts appear to have little sympathy when documents cannot be produced, no matter what the reason.

### EU Data Protection Directive

The U.S. has a sectionalized approach to data privacy. While we have a variety of laws such as Health Information Portability Accountability Act (HIPAA), which provides national standards to protect the privacy of personal health information and the Fair Credit Reporting Act (FCRA), which provides protection for consumer credit, our limited approach to data protection creates little conflict with our judicial system, which allows for wide latitude in collecting data under our liberal discovery rules.

By contrast, other countries such as the members of the European Union (EU), have a much more comprehensive approach to data privacy, as codified in the EU Data Privacy Directive. This, coupled with EU member states limited discovery procedures, and in some cases, their criminal laws protecting data, has created a conflict when multi-national corporations located in the U.S. are faced with collecting data abroad for U.S. litigation.

The EU Data Protection Directive<sup>[1]</sup> is a mandatory comprehensive regulatory scheme that protects the personal data of the citizens of its member states (along with Iceland, Liechtenstein and Norway). The Directive, a series of 34 articles, must be enacted into law by member states. At its core, the Directive requires parties to seek the consent in order to use personal data<sup>[2]</sup>, and imposes liability (including a private right of action for member citizens) when data is transmitted to non-member countries that do not provide an “adequate level of protection.” *See Article 25*. Although in general the United States falls into this category, a party can secure information from an EU member state through a variety of procedures, including consent, the Safe Harbor Approach<sup>[3]</sup>, Data Transfer Clauses, and Binding Corporate Rules. Moreover, under Article 26, a data transfer can take place to a third country that falls under Article 25 if “the transfer is necessary in legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims.” Article 26(d). The latter provision only applies, however, if the transfer is “necessary”, and although the Directive is mandatory, each member state interprets the Directive differently, so any exceptions should be thoroughly examined.

Those that violate the Directive can be subject to enforcement by EU authorities. EU citizens also have private right of action against those that violate the law. *See Article 22*.

### The French Blocking Statute

Similarly, but even more concerning are European states that have provisions for criminal liability for the removal of personal data, such as French Penal Code, Law No. 80 - 538 (July 16, 1980), also known as

The French Blocking Statute. Violation of this code carries with it punishment by fine and/or imprisonment for requesting, seeking or disclosing information directed toward establishing evidence in view of legal or administrative proceedings abroad. Unfortunately, while the Federal Rules of Civil Procedure (FRCP) give the courts the authority to order information from abroad, they do not protect parties from penalties for violating laws in foreign jurisdictions.

One solution is for parties to request courts invoke the Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, 847 U.N.T.S. 231, reprinted at 28 U.S.C. § 1781 (the "Hague Convention") when seeking information from such countries.

<sup>[4]</sup> Unfortunately, however, courts are often reluctant to grant such a request. For although in the leading case of *Societe Nationale Industrielle Aerospatiale v. United States District Court for the Southern District of Iowa*, 482 U.S. 522, 546 (1987), the Court recognized that "American courts should...take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or location of its operations, and for any sovereign interest expressed by a foreign state." *Id.* at 546, the trend has been to deny application of the Hague Convention and require parties to proceed under the FRCP. In *Enron v. J.P. Morgan Secur. Inc.*, No. 01-16034 (Bankr. S. D. N.Y. July 18, 2007), for example, the court held that threat of the French Blocking Statute did not excuse a party from its discovery obligation nor did it warrant the invocation of the Hague Convention. The party was promptly ordered to comply with its discovery obligations. See also, *In re Vinvendi Universal, S.A. Securities Litigation*, 2006 U.S. Dist. LEXIS 85211 (S.D.N.Y. Nov. 16, 2006) (requiring a third party to produce information from France under the Federal Rules of Civil Procedure); but see *Metso Minerals Inc. v. Powerscreen Int'l Distrib.*, 2007 U.S. Dist. LEXIS 51010 (E.D.N.Y. June 25, 2007) (granting use of Hague Convention procedures to obtain evidence from a third party in Northern Ireland who was not subject to the jurisdiction of the court). Although *Enron* and other courts have noted that the French blocking statute has rarely been invoked, this might be little comfort to a company that must produce information in direct conflict with that law.

It is also clear that parties that do not comply with the FRCP even in the face of violating another's country's law may face sanctions here in the United States. See, e.g., *United States v. Vetco*, 691 F.2d 1281 (9th Cir. 1981) (Vetco was sanctioned for not complying with IRS summons even though its attorneys argued that to fulfill its obligations under US law would violate Swiss law). But see, §442 Restatement of the Law, Third, Foreign Relations Law of the United States; Requests for Disclosure (requiring a good faith effort to secure permission from foreign country and court cannot impose sanctions for failure to comply with an order unless there has been deliberate concealment or failure to make a good faith effort, but a court may still grant an adverse inference instruction even if good faith has been shown). Comity also requires that U.S. courts undergo a balancing test when determining whether it is reasonable to compel foreign discovery. This balancing test varies from jurisdiction to jurisdiction, but in general, there are seven factors to be considered: (1) the importance to the litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interest of the state where the information is located; (6) the hardship of compliance on the party or witness from whom discovery is sought, (7) the good faith of the party resisting discovery. See *Reino de Espana v. Am. Bureau of Shipping*, 2005 U.S. Dist. LEXIS 15685 (S.D.N.Y. 2005).

## Conclusion

The issues surrounding international data collection are really the tip of the iceberg. The wide range of international issues are just starting to surface, such as the differing retention regulations here and abroad that affect the ability to collect and preserve relevant materials, and the concerns when litigating abroad under a foreign regulatory scheme. Further complicating the litigation process is the desire of many law firms and corporations alike to harness the efficiencies of our global community for more efficient document processing and review in places like India. These conflicts raise a whole host of ethical and security risks that need to be explored, as many countries that are popular outsourcing hubs may not have adequate privacy or data security infrastructure. As more and more companies go global and technology makes virtual communication a reality, both in-house and outside counsel will need to stay current on these issues and many more.

[1] [http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Dir\\_1995\\_46\\_EN.pdf](http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/DataProt/Legislation/Dir_1995_46_EN.pdf)

[2] The Directive does not cover business data. However, in today's business environment, it is often difficult to separate the two.

[3] See [www.export.gov](http://www.export.gov).

[4] Some countries, however, such as the United Kingdom, have opted out of the Hague Convention for purposes of pretrial discovery. Martindale-Hubbell Int'l Law Digest: Selected International Conventions, at 61 (2006); see also First Am. Corp. V. Price Waterhouse LLP, 154 F.3d 16, 22 (2d Cir. 1998). For countries that are not signatories to the Hague Convention, another approach is to use Letters Rogatory. See, e.g. Organization of American States Inter-American Convention on Letters Rogatory. [www.oas.org](http://www.oas.org).

[^ Return to top](#)



*Author Bio:*

**Courtney Barton** is Vice President of Industry Relations at Applied Discovery. She answers questions from readers in each issue of The Discovery Standard. You can submit a question to Courtney at [edstandard@applieddiscovery.com](mailto:edstandard@applieddiscovery.com).

[View Courtney Barton's biography.](#)