New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM

An ALM Publication
VOLUME 244—NO. 15
THURSDAY, JULY 22, 2010

INTERNATIONAL LITIGATION

Expert Analysis

The Conflict in Production Of Documents From Abroad

By **Lawrence W. Newman** And **David Zaslowsky**

The continuing trend of globalization and the steady expansion of multinational corporations increases the likelihood that businesses will have to respond to an adversarial proceeding in the United States that requires the collection, review and possible production of materials located abroad. For attorneys used to practicing under the Federal Rules of Civil Procedure (FRCP), this may seem like a clear enough task. However, multinational corporations dealing with information located in jurisdictions outside the United States must also be mindful of data privacy laws and other requirements in the foreign jurisdictions. In fact, there is a seemingly irresolvable conflict between broad U.S.-based discovery rules and EU member states' privacy and data protection directives. This article looks at some recent developments that show that the conflict is not close to being resolved.

U.S. Approach to Discovery

In the United States, the Federal Rules of Civil Procedure dictate that parties to pending or reasonably anticipated litigation must collect, preserve and produce all relevant records within their possession or control, including any records existing in electronic format. This obligation can extend to foreign subsidiaries or affiliates of the companies involved in the litigation, and courts can order persons subject to their jurisdiction to produce evidence even if the information is not located in the United States. Failure to comply with these disclosure requirements can result in sanctions in a civil suit (even dismissal or a judgment) and may even constitute a criminal offense in the case of a federal investigation.

The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters provides a standard procedure for making requests for information abroad through issuing "letters of request" or "letters rogatory." Under this procedure, a U.S. court seeks judicial assistance by way of "letter of request" sent to the central authority in the jurisdiction where the information is located, identifying the documents sought with specificity. The letters are then executed by a local court in that jurisdiction, should the data request be found reasonable.

Unfortunately for U.S. practitioners, because the foreign court is the one to determine whether the discovery request is reasonable, and because foreign courts generally believe that the practice of U.S.-style pretrial discovery is a wasteful fishing expedition, this process does not result in the mandatory production of all the information sought. Furthermore, the process can be bureaucratic and lengthy, and only applies to countries that are parties to the Hague Convention.

> EU jurisdictions have adopted data privacy laws in an attempt to restrict cross-border discovery of information intended for disclosure in foreign jurisdictions.

More than 20 years ago, the U.S. courts were called on to decide whether the Hague Convention was the exclusive means for a party to litigation in the federal courts to obtain evidence located outside the United States. In *Societe Nationale Industrielle Aerospatiale et al, v. District Court for the Southern District of Iowa*,[1] the U.S. Supreme Court held that the procedures afforded by the Hague Convention are but "one method of seeking evidence [abroad] that a court may elect to deploy." As a result, especially as it related to a party to a lawsuit, the practice was not to follow the Hague Convention.

Foreign Law Restrictions

Unlike in the United States, in the EU and in other foreign countries, protection of personal data is considered a fundamental human right. These jurisdictions have adopted data privacy laws in an attempt to restrict cross-border discovery of information intended for disclosure in foreign jurisdictions. Violations of the data privacy laws can lead to private rights of action by affected individuals, or criminal penalties for persons who authorized violative activities (including their corporate officers or outside counsel).

An overview of the policy on data privacy within Europe can be found in EU Directive 95/46/EC. The EU Directive is intended to protect the fundamental rights and freedoms and the right to privacy with respect to personal data. By its own terms, the EU Directive dictates that "[t]he Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if…the third country in question ensures an adequate level of protection." See EU Data Protection Directive 95/46/EC (1995) Art. 25(1).

Under the EU Directive, "personal data" encompasses a wide variety of information including such mundane information as names and positions of employees within a company, and their titles ("any information relating to an identified or identifiable natural person.") There is also a further sub-category of "sensitive" personal data receiving even greater protection—such as racial or ethnic origin, political opinions, religious beliefs, criminal matters and the like.

The EU Directive defines "processing" as "any operation or set of operations" performed on "personal data," including any retention, preservation, or archiving of data for a litigation hold; inconveniently for U.S. litigators, this covers virtually any and every action that would be done in the United States during discovery. Violations in EU member countries are punishable by fines ranging from less than 100,000 Euros to an unlimited amount,[2] and may result in jail terms in some countries including Sweden and Switzerland. Other sanctions include public reprimand, which is used as a method of generating negative publicity against violating companies in the UK, France, and Belgium.

Further complicating the issue of transnational discovery are the "Blocking Statutes" adopted

LAWRENCE W. NEWMAN *and* DAVID ZASLOWSKY *are members of the litigation department of the New York office of Baker & McKenzie. They are co-authors of "Litigating International Commercial Disputes" (West Group) and can be reached at lawrence.newman@bakermckenzie.com and david.zaslowsky@bakermckenzie.com.* JOI LAKES*, an associate in the New York office, assisted in the preparation of this article.*

by foreign jurisdictions, which restrict the collection, handling, and transfer of any personally identifiable information about individuals. Indeed, while U.S. civil procedure rules and government obligations might require that an organization retain certain data for litigation or investigation purposes, a foreign blocking statute might require that the same data be destroyed in order to protect individuals' privacy once the personal data has served the original purpose for which it was collected.

Article 7 of the EU Directive allows for "processing" of data to comply with legal obligations, and Article 26 of the directive allows transfer of data to non-EU countries to defend legal claims under six exceptions (consent, contract, legal obligation, vital interests of data subject, public interest or "legitimate interests"). One would think that these provisions would permit compliance with discovery demands made in U.S. litigation, but that is not the case.

Article 29 of the EU Directive creates independent data protection authorities to supervise compliance efforts pertaining to data protection, and the heads of each office meet as a group and provide advisory opinions. This group, the Data Protection Working Party, has issued multiple advisory opinions specifically stating that U.S. litigation requests do not qualify as "legal" or "legitimate" obligations.[3] Most recently, in February 2009, the Data Protection Working Party decided that "consent" was not deemed to be a reliable basis for transfer of personal data, and that the obligations created by the Federal Rules of Civil Procedure do not qualify as a "legal obligation." The Data Protection Working Party recommended restricting disclosure to anonymised or pseudonymised data after filtering by a "reliable third party based in the EU."

The Conflict Intensifies

Parties with data in an EU country that are asked to disclose private data in a U.S. litigation are placed on the horns of a dilemma—run the risk of violating their jurisdiction's privacy laws if they disclose, or being sanctioned in the U.S. if they refuse to do so. Yet there does not seem to be any movement on either side of the Atlantic to resolve this conflict.

Despite EU law, U.S. courts continue to follow *Societe Nationale* and refuse to use the Hague Convention's letter procedures in all instances involving the transfer of discovery materials from Europe. This has led to attorney sanctions in Europe. For example, in *Strauss v. Credit Lyonnais, S.A.*,[4] the Eastern District of New York ordered defendant Credit Lyonnais to produce documents without resorting to the Hague Convention's letters of request, acknowledging that pursuing information through the Hague Convention could be costly, uncertain and time-consuming. The court also noted that the defendant presented little evidence that France enforced the privacy laws that the company complained discovery would supposedly violate.

Credit Lyonnais' French outside counsel approached one of the company's former directors for a statement, but did not go through the Hague Convention's letters rogatory or letter of request procedures. Counsel was subsequently criminally prosecuted and fined. The French Supreme Court upheld the criminal conviction of the French attorney, as well as the 10,000 Euro fine.[5]

Despite France's calling the Eastern District of New York's bluff on the issue of lack of enforcement of the data privacy restrictions, each side has only become more entrenched over the last 12 months. In July 2009, the French data protection authority, Commission Nationale de l'Information et des Libertes (CNIL) confirmed that all U.S. discovery requests for the transfer to the United States of personal data located in France, or subject to the protections of France's data protection laws, must be made through the Hague Convention. Moreover, even for requests coming under the Hague Convention, French data protection laws still apply if "personal data" is included. French data protection laws require: limitations on scope, notice to data subject, right of data subject to object, security over personal data, and data protection either by corporate rules, safe harbor principles, or by protective order. Further, the party seeking to transfer the information may need authorization of CNIL prior to transferring the documents.

Parties with data in an EU country that are asked to disclose private data in a U.S. litigation are placed on the horns of a dilemma—run the risk of violating their jurisdiction's privacy laws if they disclose, or being sanctioned in the U.S. if they refuse to do so.

Notwithstanding these explicit instructions from CNIL, U.S. courts have not changed course. None of the district court decisions considering blocking statutes in France or other countries with similar regimes ordered them to use the Hague Convention after the July 2009 Recommendations. For example, in *In re: Global Power Equip. Group Inc.*,[6] the claimant, a Dutch entity, argued that the Hague Convention applied to discovery of information possessed by its French affiliate. The court held that, under *Societe Nationale*, the claimant could not shield documents from discovery by storing them with a French affiliate, as the Hague Convention procedures are optional and the claimant had not demonstrated hardship. The court cited to *Strauss* and distinguished *In re Christopher X*, stating that it was not clear that the sanctioned attorney in that case was "pursuing discovery in a manner that was ordered or approved by a U.S. court."

Similarly, in *Accessdata Corp. v. Alste Techs. GmbH*,[7] the U.S. District Court in Utah rejected a German defendant's argument that the Hague Convention applied, calling it unnecessary where the suit did not involve a foreign state as a party or a sovereign with a "coordinate interest in the litigation" or where the costs of transporting documents or witnesses is not high.

Obviously, the simplest way to avoid such conflicts would be to agree before discovery to conduct all discovery of documents with international sources through the procedures of the Hague Convention. But U.S. parties are not likely to agree to a time-consuming procedure that will not yield all the discovery they are seeking. Thus, decades after *Societe Nationale* and the first of the Blocking Statutes, the U.S. and foreign countries are actually moving further apart, rather than finding solutions to this intractable problem.

1. 482 U.S. 522, 541 (1987).
2. The largest fines have been levied against companies that were not engaged in litigation. For example, Spain imposed a one-million Euro fine against a company that inadequately protected personal data from Internet hackers and a 420,000-Euro fine against a company that disclosed clients' personal data for marketing purposes. However, lesser fines have been handed out in litigation-related cases.
3. February 2006: opined that SOX whistle blowing provisions in the United States are not a "legitimate interest" for "processing" of personal information.
November 2005: opined that US discovery obligations do not qualify under the exceptions to processing and transferring personal data.
February 2009: issued a decision relating to pretrial discovery further restricting transfer of data to the U.S.
4. 242 F.R.D. 199 (EDNY 2007).
5. *In re Advocat "Christopher X,"* No. 07-83228 (Cour de Cassation Dec. 12, 2007).
6. 418 B.R. 833 (D. Del. Br. 2009).
7. 2010 U.S. Dist. LEXIS 4566 (D. Utah Jan. 21, 2010).