What Every Corporate Litigator Must Know About E-Discovery Rules in the European Union.

To allay fears concerning the handling of users' personal information European regulators have established operating guidelines for social-networking web sites to ensure they comply with the region's privacy laws. The guidelines were established to shore up EU data privacy laws already in place.

Although the new EU guidelines are specific to social networking sites, they highlight the general rigidity of EU privacy laws. These laws have significant implications for litigation based in the United States. Adversaries collecting evidence for U.S. litigation among domestic states can be a challenging task, the task becomes backbreaking when dealing with EU nations. While not an impossible task, it does require that attorneys become familiar with the requirements of EU data privacy law to ensure that data will be available upon request and that an e-discovery demand won't expose their clients to prosecution for violation of EU data privacy laws.

Privacy laws in the European Union derive from EU Directive 95/46/EC and protect personal data from disclosure in virtually all cases. The protection afforded by this directive is in sharp contrast to Federal Rule of Civil Procedure 26, which mandates that parties disclose relevant information regarding "any matter not privileged."

In addition to the EU privacy laws, it is imperative that corporate counsel become familiar with the various "blocking" statutes enacted by EU member states. Switzerland, France and the United Kingdom, for example, have enacted blocking statutes that restrict discovery of information meant for disclosure in a foreign jurisdiction. A limited exception to these laws allows personal data to be transferred outside of the European Union for "the establishment, exercise or defense of legal claims." Because the EU has limited this exception to proceedings governed by the Hague Convention, it does not apply to U.S. proceedings conducted under the Federal Rules of Civil Procedure.

There are two important ways to legitimize the release of data in relation to e-discovery in the EU. First, data may be released if the data subject gives their unambiguous consent. Second, data may be released if necessary to comply with a "legal obligation." Although this provision is strictly interpreted, a US court order directing a company to produce data from a European subsidiary would most likely constitute a legal obligation. This may vary among EU member states. France, for example, has demonstrated an unwillingness to authorize the release of data pursuant to a foreign court order.

One often overlooked mechanism to streamline issues concerning the exchange of data in the EU is the US-European Union Safe Harbor Framework. The Framework offers a simpler and more efficient means of complying with the adequacy requirements of EU privacy laws, which should particularly benefit small and medium enterprises. The Framework applies only to US companies and allows for transfers of data without prior approval. A certification form can be found at the U.S. Department of Commerce's Safe Harbor Self-Certification website.

Another technique that can ease the pressure of compliance, a multinational enterprise can utilize is to commit itself to a binding set of corporate rules surrounding its data transfers. This option allows transfers of human resources data, since it applies to intra-group transfers. It also applies to companies across the globe, not just in the US, as is the case with the Safe Harbor Framework

Counsel should work with their clients to determine which of these options is best tailored to the client's needs. This should involve a thorough understanding of the corporate structure and IT department. Although any e-discovery would still need to constitute a legitimate exchange of information, proving legitimacy will usually prove to be an easier task than justifying a transfer of data to the US.

Any litigation reaching the European continent promises to frustrate and confound with a level of complexity not normally present in a purely American lawsuit. It is imperative that counsel confer with their clients as to the laws that will govern data created in the EU so that the clients can properly set up their IT structures and a select a mode of procedure to streamline the flow of data should litigation ever occur. It is equally essential to have access to lawyers versed in European law when litigation does arise. In this manner, the e-discovery can be conducted in the EU itself, which will limit the risk of any liability for violation of data privacy laws.

Trend to Watch: Look for the EU to further shore up their privacy laws as business between U.S. and EU increases.