



Bridging the Divide: Solutions for U.S. - European Cross-Border Electronic Discovery

By: Yoeli Barag, Esq. & Salim Elkhou

e-Stet e-Discovery

U.S. and European privacy laws have evolved in vastly different directions over the past several decades, leading to diverging views on satisfying legal discovery obligations in U.S. courts. Article 8 of the European Convention on Human Rights, a principal source of guidance on European privacy law, provides protections for one's "private and family life, his home and his correspondence," subject to certain restrictions. In fact, the European Court of Human Rights has given Article 8 very broad interpretation in its jurisprudence. Article 8 far exceeds any U.S. data privacy law and has been interpreted to protect the personal data of European custodians with respect to their U.S. discovery obligations. Article 8 has also created significant difficulty in accessing data residing in jurisdictions whose privacy protections exceed those of the United States.

The disconnect between U.S. and European privacy law, and the resulting impact on U.S. discovery law, will be the focus of this White Paper. This paper explores the impact of European privacy protections on the U.S. legal system, and proposes methodologies for bridging the conflict between European privacy principles and American discovery obligations.

Differing Views on Privacy Protections

The differences between the American and European approaches may be traced to the method of formulation of their respective laws. The Europeans crafted their laws legislatively, often with vast public support within member states and the European Union as a whole. The European street has also been active in forcing the creation of independent supervisory bodies-state, federal and pan-European-to enforce such rights. Rather than using the legislative process, the American approach is crafted by the court system under state and federal case law. This has led to a situation in which the courts require fluidity and transparency of litigants by creating laws that ensure the flow of information in the discovery context. It is, of course, quite convenient of the courts to have mandated policies that simplify the system and accelerate the legal process. The application of American law to European litigants is now firmly established.

European states generally view company work product-and personal information residing within such work product-as personal data afforded privacy protection under a wide body of law. Company work product is largely discoverable under all western European legal regimes, but the scope of discovery is often limited in order to safeguard personal information that may reside on company workstations or in company data repositories. The U.S. system, on the other hand, views company work product as discoverable company property, regardless of the ostensible presence of personal information in such work product.

Transferring Data in Compliance with European Directives

In order for European litigants to transfer discoverable data to "3rd countries"-including to the U.S.-certain principles must be followed. Such principles are espoused in the Data Protection Directive (European Union Directive 95/46) on the protection of individuals with regard to the processing of personal data and the free movement of such data. The

Directive regulates the processing of data within the European Union, often requiring that data processing be conducted on European soil. In order to later remove processed data (after text and metadata extraction, keyword searching, date and extension culling) to 3rd countries, the data must be subjected to rigorous principles:

1. Notice - Individuals must be informed that their data is being collected and about how it will be used.
2. Choice - Individuals must have the ability to opt out of the collection and forward transfer of the data to third parties.
3. Onward Transfer - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
4. Security - Reasonable efforts must be made to prevent loss of collected information.
5. Data Integrity - Data must be relevant and reliable for the purpose it was collected for.
6. Access - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
7. Enforcement - There must be effective means of enforcing the 6 principles above.

Bridging the Divide

In crafting procedures for data collection and evaluation, one must pay strong attention to the limits imposed by European law. Since onward transfers of data may only be conducted after all 7 principles have been followed, European litigants, and their legal counsel, may utilize certain creative steps to overcome the logistical hurdles imposed by European law:

1. Involve a European data protection officer to (i) certify compliance with European directives and (ii) determine what precisely is relevant.
2. Limit discovery to the minimum extent required.
3. Consider de-personalizing personal data for the limited needs of U.S. courts.
4. Formulate restrictive data retention policies to circumvent discovery obligations.
5. Perform the culling of data in consultation with a data protection officer while maintaining the data within European territorial boundaries.

Step 5 above is the crux of how electronic discovery may be conducted. Mobile data collection teams may be dispatched to Europe with forensic acquisition capabilities. Once data is collected locally, it may be processed, searched and culled by mobile processing computer equipment dispatched to the host country. While processing such information in-country may prove costly, it serves to restrict data transfers to the absolute minimum data set required for adequate disclosure under U.S. discovery law.

While the recommendations above do not constitute legal advice, they may be followed to protect the data of



European custodians, while complying with U.S. law. And while they are rather straightforward, and certainly not fool proof, they set the stage for advancing negotiations between legal teams. In short, it is possible to achieve the ends of both the U.S. and European legal systems without a terrible degree of complication.

About e-Stet

e-Stet is a global provider of electronic litigation support services. We offer comprehensive solutions to streamline the discovery process from the smallest to the largest projects. We employ a highly qualified staff of computer scientists and technicians, managers and partners with a wide range of experience in the legal technology market and access to multiple resources globally. Our focus is not only to deliver excellent quality to each individual project; we are continually working to develop the most cutting edge ways for helping our clients serve their clients competently and efficiently.