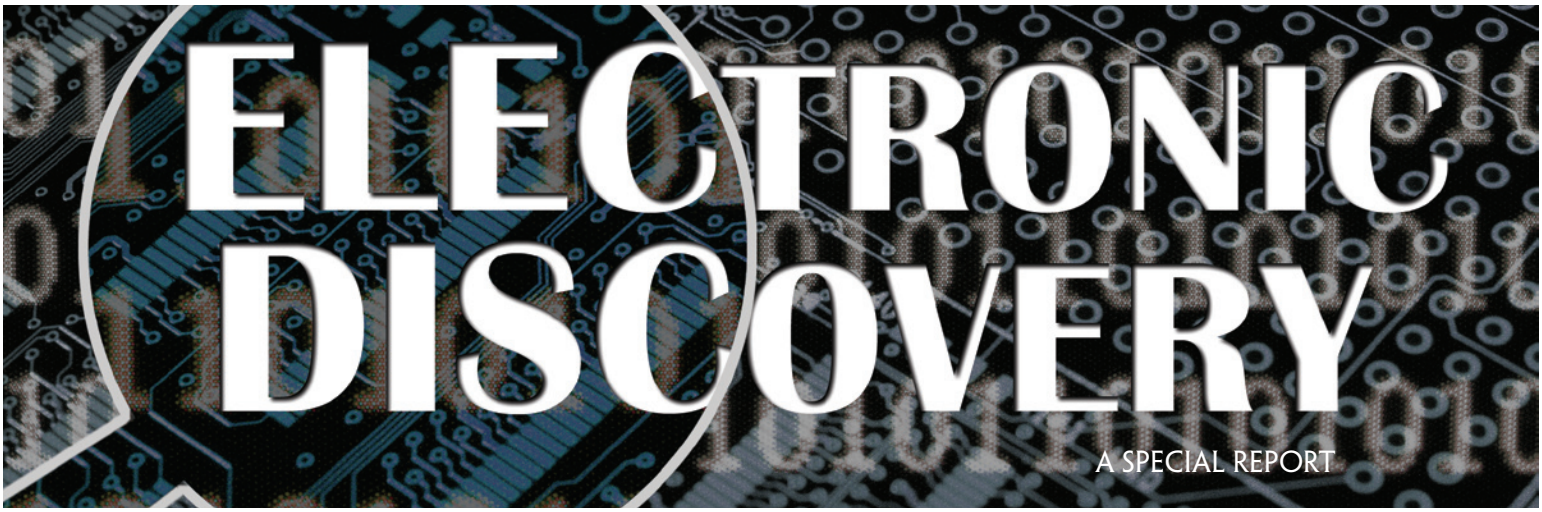
THE NATIONAL LAW JOURNAL
DECEMBER 20, 2010
An ALM Publication



Discovering Europe: How to navigate Europe's privacy protections

BY JOE LOOBY

As more businesses operate globally than ever before, they increasingly must meet external demands for data from foreign business units and offices as part of investigations or legal actions. Many of these organizations have discovered that complying with such requests can be quite challenging. The cause: a growing array of stringent data-privacy regulations in other countries, especially in the European Union.

For instance, to comply with a U.S. Department of Justice request for e-mail correspondence or documents originating in certain E.U. countries, a company cannot simply gather those documents and bring them to the United States for review and production. Because individual employees' privacy rights in the European Union are very strong (and quite different from those in the United States), the E.U.-to-U.S. transfer of an employee's personal data requires a permissible basis.

The three most common permissible bases are conditions in which the data controller (e.g., company) provides safeguards with respect to the protection of privacy and fundamental rights through standard contractual clauses, binding corporate rules or safe harbor. However, each basis can be time-consuming and costly to implement, and can present significant challenges — especially if they are not put into effect well before a litigation or regulatory request is received.

Matters are complicated further in the European Union by the fact that each member country — and sometimes, local jurisdictions within those countries — can implement privacy and protection rules differently. Germany, for example, has more than 10 local jurisdictions that can issue their own rules and regulations for data privacy. Certain countries also have what are known as "blocking statutes" designed to restrict the sharing of information with foreign public authorities. E.U. privacy rights protect E.U. customer data, as well. Thus, a company's counsel must weigh carefully each case of data transfer in consideration of the specific facts and circumstances. In other words, there is no silver bullet.

Another challenge involves differing views of consent from country to country. In the United States, consent generally trumps all: A person need only give approval for the use of data. Routinely upon hiring, many U.S. employees are asked to consent and prospectively waive any and all rights to the e-mails and documents they create pursuant to employment and/or on employer-owned property. That's not the case in the European Union, where a person's consent cannot be given prospectively and where consent must be fully informed. E.U. citizens also have the right to revoke consent. As a result, the E.U. data privacy regulator (i.e., the E.U. Working Party) has indicated that consent is generally unworkable as a permissible basis to transfer such protected data to the United States.

In short, although there are ways for companies to take data out of foreign countries, doing so can be extremely complex, challenging and costly. Fortunately, there is another approach.

TAKING THE PROCESSING TO THE DATA

Instead of transferring data out of a country for review and processing, a growing number of companies are doing the reverse: taking the review and processing to the data. Doing so enables them to meet their discovery demands while complying with E.U., sovereign and local laws and protecting the privacy of individuals — and conforming to the Sedona Conference, E.U. Working Party and RAND Europe report guidance.

In such instances, a company brings a team of experts and mobile technology to a foreign facility to process, filter and review the data as appropriate. Based on the experiences of several companies that have taken this route, the following hypothetical scenario demonstrates the challenges of this approach as well as effective responses to those challenges.

Suppose an E.U. multinational corporation was involved in litigation and an investigation originating in the United States. To help prepare for the case and respond to discovery requests, the company's law firm identified approximately a half-dozen employees who may have possessed relevant documents. Although the employee list started small, it grew large — ultimately including dozens of custodians and potentially hundreds of gigabytes of e-mail and documents. The data resided in a European country, so they could not simply be removed from that country for processing and review at a U.S. data center. Furthermore, because the majority of documents were in German, foreign-language reviewers and technology that could process and present multiple language documents was needed. All of these challenges were exacerbated by a short time frame: The company had just one month to collect, review and produce the relevant data.

The company's law firm determined the best approach would be to deploy a small, mobile investigations team to the European client's offices to assist in the collection, processing, filtering and review of relevant data. This mobile forensic and litigation team began by interviewing custodians to, among other things, identify the location of relevant documents, as well as to inform custodians of the nature of the request and the process to be employed. The team then collected documents, assigning each collection an anonymous identifier.

Using a mobile processing and review tool, the team quickly processed the anonymized data collections on-site. A series of keyword searches helped cull irrelevant, duplicative and personal data while maintaining compliance with E.U. data laws. The tool's foreign-language capabilities enabled the team to overcome the language challenges and correctly assign review assignments based on the documents' language and reviewer fluency. The company also either secured the appropriate permissions from custodians to export specific identified relevant documents or removed and redacted all personally identifiable information from them.

Following this approach, the company ultimately met the court's deadlines while complying with E.U. data privacy regulations.

SEVEN CRITICAL SUCCESS FACTORS

For companies facing such a challenge, seven important considerations can help make the discovery process more efficient and effective:

1. ***Proportionality.*** A company should assess the proportionality, quality and relevance of the data collected. In the European Union, the mantra is "selectively collect." It is not "overcollect and selectively process."

2. ***Processing***. A company should use a qualified and trusted E.U. third party to process the data. This party should employ data-privacy and -protection practices in line with the European legal framework.

3. ***Anonymizing.*** An organization should anonymize or pseudo-anonymize (remove any personally identifiable information such as e-mail addresses, e-mail signatures, etc.) each custodian's data as soon as practical, and preferably immediately after collection and before processing.

4. ***Filtering***. Tested keywords should be applied to filter the documents on-site to further identify and remove those that are potentially irrelevant and duplicative.

5. ***Privacy Log***. A privacy log should be considered when an employee withholds consent for a large volume of documents, and in any instance in which redaction or production otherwise may be infeasible.

6. ***Redaction***. Redaction of e-mail and documents to remove all personal data (names, addresses, phone numbers, etc.) means the documents no longer contain information that would make them subject to privacy-protection laws. But a company still must be wary of potential "blocking statutes."

7. ***Protocols***. Before data are legally removed from the country, a company should have relevant protocols in place — for example, protocols to log and assure the secure encrypted transfer and storage of data.

Multinational companies with a presence in the U.S. market need the ability to produce employee e-mail and documents in the United States. This need is not just to defend against regulator or litigant request. It can extend to a company's need for a means to balance its employees' privacy rights while prosecuting its own interests, such as when another company violates its patents or commercial rights, thus requiring U.S. court intervention.

The need for global organizations to provide potentially sensitive data and documents to third parties around the world is not going to abate anytime soon. In fact, as global commerce and information exchange continue to grow each year, the demand will become even stronger. Yet because of global variations in privacy laws and notions of consent, as well as language barriers, the difficulties of fulfilling these demands are significant.

For a growing group of organizations, the solution lies in a different approach to cross-border data requests. These businesses have determined that the benefits of global business outweigh the burdens of international data transfers, and have adopted procedures that protect their employees' rights to privacy. By using mobile, multilingual data processing and review tools, these companies have surmounted the hurdles of cross-border data sharing, enabling them to comply with information requests, protect their interests and respect individual privacy.

Joe Looby is a New York-based senior managing director of FTI Consulting Inc., which delivers consulting expertise and advanced technology for investigations and complex litigation matters. Looby has provided expert testimony and consulting on economic and technology issues and appeared before regulatory agencies on diverse matters. He has spoken and written extensively on litigation technology, electronic evidence and computer forensics. Looby is a former U.S. Navy JAG lieutenant, regulator and software developer.