

# TRILANTIC

Publication: Law Practice Today

Circulation: Web

Date: October 2008

Page <http://www.abanet.org/lpm/lpt/articles/mgt10081.shtml>

---

## Discovery from the European Perspective

By [Nigel Murray](#)

October 2008

*Practicing law in Europe has its challenges and how you will deal with discovery in different legal systems is one of them. This update will assist you in thinking through similarities and differences in systems - and preparing your case.*

On a recent discovery project in France, we wanted to use the weekend to expedite our task. No go. French law mandates adherence to the 35-hour work week. We were not allowed into the client's offices because no employee had enough hours available to supervise us.

Just as work customs and laws are different, regulations governing electronic discovery are not the same in Europe as in the U.S.—and they vary from nation to nation and state to state within the European Union.

I have been in the eDiscovery industry since the early 1990s. Over the last couple of years, I have seen in Europe a dramatic increase in primarily U.S.-based international disputes. Regulatory matters can have international considerations, such as SEC and DOJ inquiries involving subsidiaries or even parent companies based in Europe. Cases include money laundering inquiries and, more recently, investigations regarding the Foreign Corrupt Practices Act. U.S. law firms and corporations faced with international matters should understand what is going on in the U.K. and the European Union, in terms of eDiscovery.

## Differences Between the U.K. and U.S. Legal Systems

In the U.K., *discovery* is called *disclosure*. It is a “push” rather than a “pull” system. The lawyer for a party is legally an officer of the court. As such, the lawyer must hand over to the other party all documents that directly support both their client's position and the other party's position. Each party *discloses* to the other the relevant documents in the case. In the U.S., the giving party must *respond* to a request—often with no real idea as to the scope and size of the request.

# TRILANTIC

In the U.K. disclosure process, parties are required to carry out a reasonable search for all the documents they are obliged to disclose. What factors define “reasonable”?

- The number of documents involved;
- The nature and complexity of the proceedings;
- The ease and expense of retrieving any particular document;
- The significance of any document that is likely to be found.

Generally, searches are either agreed by the parties or directed by the judge prior to the event. The guiding principle is *proportionality*. Are the efforts and costs involved proportionate to the amount in dispute? Often, the parties deem that *no* electronic document collection is proportionate. (This is slowly changing as the realization sinks in that a document collection without the electronic documents is less than complete.)

This attitude is surprising, because the form that must be signed by the disclosing party is fairly emphatic and all-encompassing. Even mobile phones and PDAs are mentioned. Those vendors who provide concept search tools get a mention, too! In the past, this form was signed by the law firm on the case. However, I am detecting certain reluctance by lawyers to sign, and the obligation is shifting to their clients.

Overall, a major difference between the English and U.S. legal systems regarding litigation is that the *loser* pays both party’s costs—all of them, unless it has been agreed beforehand that some elements will be shared (for example, setting up an electronic courtroom).

I would note two other differences. First, in the U.K. we have no juries in civil litigation, only in criminal cases. Accordingly, the use of technology has been slow to evolve in civil courts; this is changing for the better. Second, insurance-funded class action disputes are rare (though they are starting to pick up). I was involved in one in the mid-1990s—the first and only tobacco litigation held in the U.K. The claimants lost, which caused quite a bit of suffering because they personally had to pay the tobacco companies’ legal costs. This successfully put people off class actions.

## **Differences Between the EU and U.S. Legal Systems**

While U.S. and English systems are based on common law, European systems are based on Roman law. The differences are huge, and I will highlight only a few that affect eDiscovery.

# TRILANTIC

Cases are tightly run by the presiding judge and there is *NO* discovery or disclosure. Nothing. There is no obligation to hand over documents to the other side. As you can imagine, the eDiscovery market in the EU is small—somewhere between zero and negligible, with the main demand coming from those cases for English or U.S. jurisdictions.

## EU Data Protection – An overview

The European attitude toward individual rights is different from that in the United States. For example, if a company gives an employee a laptop PC with which to work, the data on the laptop are deemed to be personal to the individual. The company needs the individual's permission before anyone can access the information. Furthermore, an individual's personal data must be strictly safeguarded. In some countries, the levels of safeguard are clearly spelled out—with dire consequences for any failure. In Finland last July, the data manager (CIO) of a company was jailed for six months for not putting adequate controls in place to protect employee data.

In October 1998 the EU adopted the 1995 directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Article 1 treats privacy as a basic human right. Articles 2-4 state that the directive covers *all* processing of *all* personal data except in matters related to public security and criminal law. It prohibits the processing of personal information unless the individual has been informed and “unambiguously” consents.

Article 4 also obliges all EU member states to enshrine the directive into their national laws—and this is where the fun starts. Each country has applied different rules. Some are very stringent, others less so. And there are not just *national* rules; in Germany, for example, where the government is a federal system, 14 of the 16 states have their own data privacy laws.

In a U.S.-based matter (litigation or regulatory) involving data based in Europe, four key questions need to be addressed:

- How do I identify what needs to be collected? Once I do, what must I do before starting a collection?
- Can I collect, and if so, how and where?
- Can I process, and if so, where?
- What can be shipped for review—or must the review occur onsite, within the country, within another EU country or within an outside country that is deemed to provide adequate protection (Canada, for example)?

# TRILANTIC

Each matter must be addressed on an individual basis, taking into account the type of case, the country, the client, the type of data to be collected and the local laws. Collecting data in the EU should be approached with great caution, because the person doing it could end up in jail.

Some of you are thinking, “Ah, this does not apply to me because we have safe harbor, or we use a vendor who has safe harbor.” Okay—but what, exactly, is safe harbor?

To bridge the different approaches to privacy between the U.S. and the EU and to provide a streamlined way for American organizations to operate in Europe, the U.S. Department of Commerce and the EU Commission developed a “safe harbor” framework, which was approved by the EU in 2000. The primary aim was to enable companies with European subsidiaries to operate as if there were no borders. Since then, a plethora of organizations have sought safe harbor accreditation, including eDiscovery vendors. To comply with the principles, a company must be certified and have its name registered in a database of safe harbor companies.

The system is essentially self-regulated—the fact that a company says it is complying is regarded as good enough. The framework ostensibly is backed by federal law. If a company is found not in compliance, it can be charged with deception. To my knowledge, this has not been tested. More importantly, there has been no legal test of safe harbor from any EU country. Most U.S. legal professionals I know do not want any of their clients to become the test case.

The export.gov Web site provides a good summary of safe harbor.

## **Other Things to Consider**

Working methods can affect your eDiscovery project abroad. The average European does not work like Americans. We like our holidays, and the idea of working on a 24-hour basis is alien to some. In France, as you read above, the 35-hour work week is strictly enforced.

Language frequently is a factor. In half the cases heard by the London Commercial Court, both parties are based overseas; in 80 percent, one of the parties is based overseas. Obviously, we regularly deal with foreign languages. One specific issue is processing. (Can the software process an e-mail box or loose files in, for example, Russian? Can it recognize non-Latin character filenames without inserting lots of question marks?) Another is searching. (Can your software search across multiple languages and character sets?) A third is review. (How will you review documents in French, Japanese, etc.?)

# TRILANTIC

Working in this industry in Europe has its challenges. They can be overcome if you are aware of some of the pitfalls and plan ahead, employing local knowledge.