The Sedona Conference Journal

Volume 5 2004

U.S. Discovery of Electronic Documents in Europe

Ashish S. Prasad & Tara Thompson

Recommended Citation: Ashish S. Prasad & Tara Thompson, *U.S. Discovery of Electronic Documents in Europe*, 5 SEDONA CONF. J. 119 (2004).

For this and additional publications see:
https://thesedonaconference.org/publications

U.S. DISCOVERY OF ELECTRONIC DOCUMENTS IN EUROPE

Ashish S. Prasad and Tara Thompson
Mayer Brown Rowe & Maw
Chicago, IL

This paper explores some of the special issues that may arise when U.S. litigation requires the discovery of electronic documents in Europe. The first section discusses European law with respect to discovery procedures, attorney-client privilege, privacy requirements and the Hague Convention. The second section discusses the challenges that arise for U.S. litigators as a result of European law on these topics, and strategies for overcoming these challenges.

I. DIFFERENCES BETWEEN U.S. AND EUROPEAN LAW

A. Discovery Procedures

Discovery procedures in Europe differ widely across countries. In England, for example, discovery (called disclosure) is relatively straightforward compared to the U.S. Cases primarily involve standard disclosure, pursuant to which a party is required to disclose only those documents on which he relies and those which adversely affect his own case, adversely affect another party's case or support another party's case. Each party provides the other party with a formal List of Documents that cover these categories, and the other party is then entitled to inspect the documents and make copies of them (at their own expense). Moreover, while parties are required to make a reasonable search for documents falling within these categories, they may limit their initial search on the grounds that an extensive search would be disproportionately costly. It is only if a party does not comply with discovery that the opposing party is allowed to apply for more specific, or more extensive, discovery; a court may order a party to produce specific documents if a requesting party can convince the court that the party is hiding evidence. The court will then order the party to disclose specific documents or classes of documents, carry out a search based on specific criteria, and disclose any documents located as a result of that search. English courts have adopted these rules as a method of managing cases by reducing costs and delay in litigation.

Like U.S. law, English law is gradually becoming cognizant of electronic documents. Electronic documents, including backup tapes, are discloseable under English law, although subject, again, to such disclosure being proportionate.

B. Attorney-Client Privilege – Determining What is Discoverable

Another primary way in which European law differs from U.S. law in the context of discovery is in defining what documents are protected by attorney-client privilege. Under U.S. law, of course, confidential communications conducted with a lawyer, even an in-house lawyer, are protected by attorney-client privilege. This means that, if an email containing advice from an attorney is stored on a company's computer system, that email is generally

protected by attorney-client privilege and not discloseable. These same rules are generally in force in common law states like England. For other European states, however, the production of documents memorializing attorney-client communication are only protected where those documents are in the possession of a lawyer.[1] In addition, attorney-client communications in European countries (other than England) are generally only recognized where the lawyer is an independent attorney and not in-house counsel; in-house counsel in these countries are not considered members of the bar because they are not regarded as independent.[2] In Germany, attorney-client privilege does extend to in-house counsel if the in-house attorney maintains a separate private office and is acting in his or her capacity as an attorney.[3]

C. Privacy Requirements

A major difference between U.S. and European discovery rules, and a difference that can create problems in U.S. litigation, are strict European privacy laws. European Directive 95/46/EC relating to the processing of personal data ("the Directive") and national implementing legislation in EU Member States such as the Data Protection Act of 1998 ("DPA") in the UK have implications for the transfer of "personal data" in the course of data collection and review for U.S. litigation. The DPA and Aticle 25 of the Directive set out eight principles that must be observed in processing personal data. The eighth principle states that personal data must not be transferred to a country or territory outside the European economic area ("EEA") unless that country or territory ensures an "adequate level of protection" for individuals in relation to processing of personal data. The United States is not currently accepted by the European Commission as providing an adequate level of protection. As a result, under these rules, data cannot be transmitted to the United States if it constitutes personal data, unless a recognized exception to this rule applies, or another means is used to achieve adequacy of protection of the data.

Personal data is defined as data that relates to a living individual who can be identified from that data alone or in conjunction with other information in the possession of the data controller. In the United Kingdom, the Court of Appeal has recently given a restrictive interpretation to that definition, so that information will only constitute personal data if it "relates" to the individual in a strict sense, i.e., it has the individual as its focus or is biographical in nature. As a result, some documents that name or refer to individuals and that might be relevant in the context of litigation will no longer be considered to constitute personal data in the United Kingdom, but Courts in other Member States might take a wider view of the meaning of personal data.

It is important to note as well that the DPA only applies to information that is either processed electronically or recorded as part of a structured filing system such that particular information relating to an individual is readily accessible. Information collected for disclosure electronically will meet these criteria, but paper documents may not.

There are a few major exceptions to the DPA and the Directive, which should also reduce concerns about these privacy rules for corporations trying to comply with United States discovery obligations. The most relevant, set out in Article 26(d) of the Directive

1 See, e.g., Case No. 155/79, *A.M. & S. Europe Ltd. V. Commission*, 1982 E.C.R. 1575. This case may also be authority for the proposition that in-house lawyers do not enjoy privilege with respect to communications with their client where the client is a party to an investigation into possible breaches of what were Articles 85 and 86 of the Treaty of Rome, an exception to the privilege enjoyed by in-house lawyers under English law.

2 Laurel S. Terry, *An Introduction to the European Community's Legal Ethics Code Part I: An Analysis of the CCBE Code of Conduct*, 7 Geo. J. Legal Ethics 1, 4 (Summer 1993).

3 *See id.*

4 *FSA v. Durant*. [2003], EWCA Civ 1746, Court of Appeal.

(implemented by paragraph 5 of Schedule 4 of the DPA), provides that the eighth data protection principle does not apply where the transfer is "necessary or legally required for . . . the establishment, exercise or defence of legal claims." The drafting of the equivalent provision in the DPA is more detailed than in the Directive, and also expressly allows the transfer of data where necessary for the purpose of obtaining legal advice or in connection with any legal proceedings, or is otherwise necessary for the purpose of establishing, exercising or defending legal rights. This exception is embodied in the Directive, but is subject to implementation by national law in each country individually. It is possible that the implementation in other EU Member States such as Germany may be more restrictive than in the United Kingdom, but ultimately the scope would be subject to determination by the European Court of Justice.

There has been some discussion in academic literature about the meaning of the word "necessary" in this context, and the precise scope of this exception, but to date we are aware of no courts that have reached decisions on this point. The exception is not limited to proceedings or claims to which the data subject is a party. It is likely, then, although courts have not yet directly ruled on this issue, that where transfer of information is legally required for the purpose of U.S. proceedings, the transfer will be recognized as an exception to the DPA and the Directive. However, a wholesale transfer of information in order to enable assessment of information to take place in the United States could contravene the eighth principle. In other words, a corporation who sends vast amounts of data to the United Sates in order to review the data to determine if it is subject to U.S. discovery rules might be violating the DPA and the Directive. For that reason, it might be appropriate to arrange for prior relevance review of documents likely to contain personal data to take place within the European Union prior to any transfer.

Additionally, the DPA and the Directive include an exception for information that the data subject has given his consent to be transferred, but in most cases this is unlikely to be practicable in the context of litigation, unless the data concerns an employee of the company, in which case it may be possible to obtain consent prior to transfer, provided the consent is genuine and freely given.

Where the legal proceedings exception does not apply, or the transfer is made on too large a scale to benefit entirely from the exception, there are other methods by which compliance with the eighth data principle might be achieved. One possible approach might be to use one of the sets of model clauses approved by the European Commission for use by organizations that wish to transfer personal data out of the EU.[5] There are two sets of model clauses that may be used, depending on whether the recipient organization will act as a "data controller" or "data processor" as defined in the Directive. Consideration would need to given to the appropriate parties to the agreement and form of clause to be used, depending on the nature and purpose of the transfer. The use of the clauses would place the parties under various obligations with respect to the use of the data. For example, individual data subjects must be notified if certain sensitive or special categories of data are to be transferred, data may only be used for the purpose for which it is transferred, and there are restrictions on further onward transmission of information. No prior approval would be required for transfer from the United Kingdom based on these clauses, but the transferring organization would need to be able to demonstrate that the clauses had been used properly in the event of any challenge. In some EU countries the transfer would need to be approved

5 Commission Decisions 2001/497/EC and 2002/16/EC, available online at http://europa.eu.int./comm/internal_market/privacy/modelcontracts/en.htm.

by a national authority, which (other than in exceptional circumstances) would be required to accept the standard clause as offering adequate protection.

Alternatively, transfer may be permitted if the recipient in the U.S. has committed to observe the "safe harbor" principles agreed between the U.S. Department of Trade and Commerce and the EU Commission,[6] but U.S. companies may be reluctant to do this, and it may well be inappropriate to do so in the context of information transferred for the purpose of litigation

D. The Hague Convention

The Hague Convention of March 18, 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters (the "Hague Convention") provides rules that member states (which include the United States, Germany, the United Kingdom, and France) must follow in obtaining evidence for use in proceedings. Chapter I of the Convention provides for letters of request addressed by the U.S. court requesting discovery to a central authority in the state from which it is requesting discovery. The party requesting discovery must then comply with the discovery rules applicable in the state in which it is requesting documents or other discovery. Chapter II of the Convention provides for evidence gathering by diplomatic officers appointed by the requesting state. These diplomatic officers, in gathering documents, must also follow the rules of civil procedure in the state in which they are gathering documents, and lack the power to compel the production of documents. The United States Supreme Court, however, has held, in *Societe Nationale Industrielle Aerospatiale v. United States District Court*, 484 U.S. 522 (1987) that U.S. courts did not necessarily have to comply with the Hague Convention when subjecting foreign companies to discovery procedures. For this reason, where a European company is a party to U.S. litigation, it may not be able to rely on the Hague Convention as a method of avoiding U.S. discovery obligations, especially if there is a possibility of a finding of personal jurisdiction in the U.S. over the European company.[7]

II. CHALLENGES AND STRATEGIES

Despite the increasing uniformity of international business and, to a lesser extent, the increasing uniformity of international litigation, attorneys working with European corporate clients in complying with U.S. discovery rules may still experience a disconnect between what their clients expect the U.S. discovery process to entail and what it will actually involve. In addition, continuing language and technological barriers may present difficulties in carrying out document review processes that U.S. discovery compliance has come to require. This section discusses some of the problems attorneys face in helping European clients respond to U.S. discovery requests and explores some strategies for minimizing them.

A. Privacy Laws and Logistical Problems in Analyzing Data

The strict nature of European privacy laws creates difficulties for European corporations seeking to comply with both U.S. discovery obligations and European rules governing the privacy of personal data. Although personal data concerns will not arise in every case, they are increasingly common, and out of an abundance of caution corporations

6 Commission Decision 520/2000/EC of 26 July 2000, available online at http://europa.eu.int/comm/internal_market/privacy/adequacy_en.htm.
7 For a discussion of the Hague Convention and its effect on discovery in U.S. courts, see James Chalmers, *The Hague Evidence Convention and Discovery Inter Partes: Trial Court Decisions Post-Aerospatiale*, 8 Tulane Journal of International and Comparative Law, 189 (Spring 2000).

may want to broadly interpret their privacy obligations. Because of the broad exception for information produced pursuant to legal obligations, European companies should have little problem in producing relevant documents to the United States, but problems may arise during the review process itself. Because documents sent outside Europe to be reviewed for potential relevance and production in U.S. litigation may be interpreted as violating privacy laws, a feasible strategy may be to process and review documents on-site or within the relevant country, and to produce to the United States only those documents that will be disclosed to the other side. For large-scale litigation, this may entail bringing U.S. counsel and document production consultants to Europe to manage the discovery process.

B. Foreign Language Data

Although technology is continuously becoming more advanced, and English is increasingly becoming a common language for even internal business communications in Europe, language barriers continue to be a problem for U.S. discovery compliance. The legal team reviewing documents for relevance must include reviewers who are fluent in languages other than English, and search tools must be able to handle searches in other languages, including languages that use different character sets than English.

C. Different Conceptions of Backup Tapes

While European discovery processes can require the production of backup tapes, the production of backup tapes for U.S. litigation purposes may be a problem for European companies. Most European companies that use backup tapes think of these tapes as primarily for disaster recovery and not for litigation purposes. Some European companies never planned on freezing the contents of backup tapes, or retaining them for longer than their policies on retention of materials, so orders requiring preservation, or orders to produce, may come as a shock and may pose substantial technical problems.

D. Unfamiliarity with Large-Scale Discovery

Despite the increasing frequency of European corporate involvement in U.S. litigation, many European companies are unprepared for the large-scale nature of U.S. litigation. This is in large part because of the limited nature of most European discovery. Large-scale litigation of the type increasingly common in the United States is still a rarity in Europe, so the kind of large-scale document production that litigation has come to require in the United States may be a challenge to even the most international of European companies. Corporate culture in many European companies may also be different – many executives, for instance, may find it extremely invasive for an attorney to review their personal correspondence or files and to produce those documents to the other party in U.S. litigation. For this reason, U.S. attorneys advising European companies on U.S. discovery requirements should be prepared to explain in a clear way what U.S. courts require and work with their clients to meet these requirements in an efficient way.