Proskauer

International HR Best Practices Tip of the Month

October 2008

This Month's Challenge

Employers face conflicting legal obligations when discovery demands in U.S. litigation seek information about employees in the EU.

Best Practice Tip of the Month

Proceed with caution, and with full awareness of the risks on both sides of the Atlantic. Evidence of vigorous enforcement of the blocking statute in the EU member country where the data are located might persuade the U.S. court to curtail the discovery request.

Production of EU Employee Data in Discovery in U.S. Litigation May Spell Trouble

In this age of ceaseless employee litigation, employers in the United States are all too familiar with their obligations under U.S. discovery rules to search their paper and electronic files for documents and to turn them over to employee-plaintiffs. It is a (perhaps unfortunate) fact of life that the Federal Rules of Civil Procedure broadly allow for the discovery of all nonprivileged relevant information in a defendant's possession, custody or control—information that may be found in any number of locations, including abroad. With the growth of globalized workforces, U.S.-based multinationals are increasingly coming up against statutes in the European Union that, under threat of criminal sanction, forbid compliance with the company's U.S. discovery obligations. So far, neither the U.S. nor the European courts have demonstrated a willingness to defer to the other, and the resulting pinch is being felt by the multinational corporation stuck in the middle.

As the law currently stands, it is often impossible simultaneously to comply with both EU and US law, such that a company is faced with an intractable dilemma: Should the company turn over relevant documents and refuse to comply with EU data protection laws, risking a possible EU enforcement action by a member states' data protection authorities? Or should it refuse to comply with U.S. discovery obligations and thus risk sanctions from a U.S. court? The good news is that the courts and governments are aware of the problem; the bad news is that none of them has taken any steps to find a solution.

The Problem

The Catch-22 is best explained using the following example: A U.S. citizen employed abroad by a multinational corporation is terminated, ostensibly for performance or redundancy. The employee returns to the United States and brings suit against his employer, alleging that it has discriminated against him on the basis of his age (or any other protected status). In discovery, he asks for detailed information about his former co-workers who were or may have been similarly situated to him: name, age (or sex, race, etc.), performance records, reasons for termination, and so forth. To a U.S. court, this sort of information is routine grist for the discovery mill. Accordingly, on motion of the plaintiff, the court will order the company to collect the information in the EU, transfer it to the US, and turn it over to the plaintiff.

However, the processing, transfer, and disclosure of such data violates EU data protection law. The EU Data Protection Directive (and the various Member States' data protection laws transposing the Directive) restrict the processing, transfer and disclosure of personal data to countries whose data protection laws do not match the EU"s level of protection, such as the United States. The Directive broadly defines personal data as "any information relating to an identified or identifiable natural person." Such personal data undoubtedly would include information contained in employee personnel files and e-mails, for instance. "Processing" is also broadly defined and includes the "collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or otherwise making available . . ." of personal data. The EU Directive not only restricts the transfer of data to the U.S., but Article 7 of the Directive prohibits the collection and useof such data unless it is justified because one of the following grounds has been met:

- the data subject has*unambiguously given his consent*; or
- processing is necessary *for the performance of a contract* to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
- processing is *necessary for compliance with a legal obligation* to which the controller is subject; or
- processing is necessary in order to *protect the vital interests of the data subject*; or
- processing is necessary for the *performance of a task carried out in the public interest or in the exercise of official authority* vested in the controller or in a third party to whom the data are disclosed; or
- processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject.

Several of these authorized exceptions look promising, but none has emerged as a clearly legal basis for production of personal information pursuant to U.S. discovery rules. The Article 29 Working Party (the EU Committee charged with clarifying the EU Data Protection Directive) has stated that obligations imposed by U.S. statutes do not qualify as a "legal obligation" under the Directive's Article 7, reasoning that if foreign laws could impose legal obligations that conflict with the Directive itself, the protections afforded to data subject's personal information would be eviscerated. *See* Art. 29 Data Prot. Working Party, WP 117, Op. 1/2006, 00185/06EN (1 Feb 2006).

Further, the "necessary to protect the vital interest of the data subject" exception does not apply, because in fact disclosure of personal data in discovery would likely not be in the interest of the data subject (here, an EU employee who is not a party to the litigation). Compliance with discovery obligations would not fall within the "public interest" or exercise of "official authority" exceptions, either, because the U.S. is not considered an "official authority" within the EU; only EU authorities are relevant.

Unambiguous consent is not an option either: EU authorities have opined that in order for consent to be meaningful, the data subjects (*i.e.,* the employees about whom data are being sought) must be able to freely withdraw their consent. Article 29 Data Prot. Working Party, Opinion 8/2001 (5062/01/ENFinal WP 48). A U.S. court is unlikely to accept the proposition that compliance with a discovery order depends on whether a third party is willing to consent to compliance. Certainly, in the U.S., employees are not free to prevent relevant data about them from being turned over in a litigation.

Nor can a company rely on the EU data protection transfer mechanisms that it utilizes in the ordinary course of its business, *i.e.*, the Safe Harbor Program and model contractual clauses (previously discussed in our December 2007 newsletter). These are the two most popular mechanisms to transfer employee personal data from the EU to the US, and one of the two is usually necessary, since the U.S. is not on the approved list of countries that have robust data protections laws and that consequently do not require such data transfer mechanisms to be in place. Safe Harbor and model contracts only concern the *transfer* of employee data from the EU to the US; they do not legitimize the collection and *processing* of data for a non-approved purpose in the first place, such as the disclosure of EU employee personal data in a U.S. litigation. Thus, Safe Harbor or model contracts will be of little use in this instance.

Yet Another Problem: EU Blocking Statutes

Some countries provide an additional obstacle to compliance with U.S. discovery obligations: they explicitly restrict cross-border discovery of information that could be used in connection with a foreign legal proceeding. Historically, U.S. courts have not backed down in the face of such statutes, pointing to the absence of enforcement to conclude that the fear of prosecution for compliance with U.S. discovery requirements was merely hypothetical and insufficient to justify withholding of information. That situation may be changing. In France, such a law was recently invoked when a French attorney provided documents to a U.S. litigation team in connection with a U.S. proceeding. Earlier this year, the French Supreme Court upheld the conviction of the attorney for providing information pursuant to discovery demands in a U.S. litigation, in violation of a provision of French Penal Law that makes it unlawful to provide "economic, commercial, industrial, financial or technical" information to be used as evidence in a foreign judicial or administrative proceeding. This case tightens the squeeze on multinational employers, which may no longer be able to ignore these laws blocking the discoverability of information in connection with a foreign (*i.e.*, U.S.) legal proceeding. Perhaps, armed with this precedent, the company may be able to persuade a U.S. court that compliance with a discovery demand seeking personal data from an EU country is truly impossible.

The Solution: Forthcoming?

The Article 29 Working Party has recognized that this intractable problem needs to be addressed and a solution found. Accordingly, it has announced in its 2008-2009 agenda that it will take up the issue of data protection issues in the context of international discovery, and has marked the issue as "high priority." Similarly, the CNIL, the French Data Protection Agency, expressed concern in a January 2008 statement that international discovery raises problems that urgently need to be addressed.

This is not the first time that EU data protection law and U.S. law have butted heads. Just a few years ago, EU data protection laws prohibited U.S. public companies from operating anonymous whistleblowing hotlines in Europe, despite the mandate in the U.S. Sarbanes-Oxley Act that they do so. After U.S. companies were found by EU data protection authorities to have violated EU law, the issue was ultimately resolved through direct negotiations between the U.S. and EU governments. A similar solution may be needed to untangle yet another EU-US deadlock. In the meanwhile, companies have little choice but to carefully weigh their risks and plead for relief from the courts.

- **Howard Z. Robbins**
  Partner
- **Anthony J. Oncidi**
  Partner