

Cross-border Challenges for e-Discovery

Seth Berman*

Cross-border electronic discovery (or disclosure as it's called in the UK context) is becoming increasingly common and increasingly fraught with peril. As the scope of international business and US discovery expands, litigants in US courts need to collect, cull, review, analyse and ultimately produce ever-growing amounts of electronic data. Often this data does not reside in the US, but nevertheless is relevant to US litigation. This effectively expands the reach of US discovery rules to other countries, including countries that take a remarkably different (and often dim) view of US discovery practice. This article explores the potential pitfalls facing a corporation dealing with cross-border electronic discovery matters, and suggests different strategies to address these difficulties.

Electronic discovery and US litigation

Courts in the United States (US) take a very broad view of the need to preserve, review and produce material relevant to US litigation. Under US civil procedure rules, a litigant needs to begin preserving data relevant to a lawsuit as soon as they know a lawsuit is likely to occur. More worrisome for cross-border litigation is the scope of this preservation requirement. In the words of Rule 26 of the Federal Rules of Civil Procedure:

‘Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defence – including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter.’

In practice, this means that at the request of the opposing party, litigants must be prepared to scour their own electronic and other records (and

* Seth Berman, Managing Director, Stroz Friedberg Ltd.

their employees' memories) for any information that may be relevant to the matter involved in the lawsuit.

If this prospect were not daunting enough, the scope of data subject to preservation, as opposed to production to the other party, is even broader. In most instances, US litigants are required to preserve *any* data that may contain potentially relevant information, even if searching that data would be prohibitively expensive and/or unlikely to find any non-duplicative, relevant information.

Failure properly to preserve potentially relevant information can lead to significant sanctions including the loss of the case. In 2004, the United States District Court for the Southern District of New York decided on sanctions related to the case of *Laura Zubulake v UBS Warburg LLC*. In that case, Laura Zubulake had sued UBS Warburg in what would otherwise have been a fairly routine employment discrimination case. Defendant UBS Warburg failed properly to preserve electronic data, including potentially relevant e-mail communications. As a result of this failure, the Court instructed the jury to assume that the missing e-mails were supportive of Zubulake's case, and prevented the authors of the missing e-mails to testify and contradict that assumption. In large part as a result of this instruction, the jury awarded Zubulake US\$29 million in compensatory and punitive damages.

Similarly, in *Coleman (Parent) Holdings, Inc v Morgan Stanley & Co* (Fla Cir Ct, 2005), Morgan Stanley failed properly to preserve relevant backup tapes and other material. As a result of that omission, the judge instructed the jury to assume that Morgan Stanley was guilty of fraud as claimed by Coleman – thereby effectively awarding the case to Coleman. The jury ultimately awarded Coleman almost US\$1.5 billion in damages. Luckily for Morgan Stanley, the judgment was ultimately overturned for other reasons, but the lesson is still very clear: a party that fails in its preservation and disclosure obligation does so at its peril.

Within the context of data owned by a litigant involved in US litigation, the lesson of these cases is very clear: preserve early; preserve broadly; employ defensible culling techniques; avoid discovery mistakes.

This advice, though sometimes hard to implement in practice, is a useful guide to US litigants when the data they need to preserve, review and ultimately produce is in the US. If, as often happens to multinational corporations, the data resides outside the borders of the US, following the dictates of US litigation rules becomes much trickier.

Electronic discovery and European data protection rules

In general, US law assumes that a corporation owns the data it possesses or controls. Thus, US corporations rarely have to worry that their preservation, processing, review or disclosure of data relevant to a lawsuit would violate any other entities' or individuals' rights to the data. In those circumstances, where relevant data is otherwise protected from disclosure (such as if the data contains a third party's trade secrets, or is classified), litigants work with courts and opposing parties to negotiate an appropriate non-disclosure agreement, allowing the opposing litigator's access to the relevant data, without violating the necessary confidentiality.

The law in most European countries, by contrast, does not assume that a corporation's possession of data gives them a right to use it as they see fit. European law generally assumes that individuals, whose personal information is contained within a corporation's records, retain a right to protect that data from being exported or disclosed to third parties. For example, the European Union (EU) Data Protection Directive states:

'Article 1 – Object of the Directive

In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons and, in particular, their right to privacy with respect to the processing of personal data.'

The EU Data Protection Directive provides protection to 'any information relating to an identified or identifiable natural person', in particular, to an 'identification number or... one or more factors specific to [an individual's] physical, physiological, mental, economic, cultural or social identity'. This includes not only financial information (such as bank account or credit card numbers), but also an individual's address information, membership in a trade union, racial or ethnic identity, health status and even e-mail addresses. Given the detailed information that corporations routinely keep about their employees, customers and suppliers, virtually any corporate dataset will contain some of this protected information.

The EU Data Protection Directive regulates the disclosure of this private data and its export to countries that do not provide adequate (from the European point of view) protection for this data. Because EU law does not consider the United States a country with adequate protection of personal data, the EU Data Protection Directive can create a significant potential conflict with US discovery obligations.

The problem is made more complicated by the fact that the EU Data Protection Directive is not, in and of itself, a law. It is a directive to the EU Member States to pass their own implementing legislation in accordance with the Directive. The result is that each Member State's specific rules vary. Some

Member States interpret the Directive broadly, allowing significant leeway to US litigants facing this dilemma. Other states' implementing legislation takes a much harsher view, creating greater conflicts for US litigants. The specific differences among EU Member States' laws are beyond the scope of this article. It is worth remembering, however, that the specific solutions to dealing with the conflict of laws discussed here will vary depending on which EU Member State's laws apply.

This conflict of laws is not absolute. The EU Data Protection Directive includes several exceptions. At first glance, several of these exceptions appear as solutions to EU-US conflicts of law. These include data transfers and processing necessary:

1. for legal claims;
2. for the prevention and detection of offences; and
3. with the notice and permission of the affected individuals.

However, on closer examination, it appears that none of these exceptions is broad enough to resolve the conflict.

Exception for legal claims

The wording of this exception seems completely to resolve the conflict of laws. However, its interpretation by EU authorities reveals that the opposite is the case. The exception only applies in practice to legal claims occurring in EU jurisdictions – not to US legal claims. Thus, this exception provides little grounds to resolve the EU-US legal conflict.

Exception for the prevention and detection of offences

This exception is also unlikely to provide much assistance in resolving the conflict. It only applies to potential fraud or other criminal behaviour, and thus is not applicable to most purely civil litigation issues. Moreover, like the exception for legal claims, it only applies to the prevention and detection of European offences. Once again, this exception provides little grounds to resolve the EU-US legal conflict.

Notice and permission of affected individuals

This is the most important exception for addressing the EU-US conflict of laws. However, it is an incomplete one. Often, the most abundant source of personal information contained in a corporate dataset will be the personal information of a company's own employees. When this is the case, getting their informed consent to transfer the data to the US should be possible. However, this does

not completely resolve the conflict. First, some European countries doubt whether employees can really provide voluntary consent to their employers for a request of this type, assuming that the employer-employee relationship makes such a request at least partially coercive. Moreover, it is likely that some of the relevant data will include personal information of former employees, customers or suppliers, from whom permission may be significantly harder to obtain. Moreover, there may be some circumstances in which the company wants to avoid notifying employees of the underlying lawsuit that gives rise to the request, which can make obtaining their consent challenging. And, of course, the relevant people may simply refuse to provide consent. Thus, this exception at best only provides a partial solution to the conflict.

Blocking statutes and employment laws

Before discussing possible resolution of the conflict between the EU Data Protection Directive and US discovery obligations, it is worth considering two other potential obstacles that US litigants may face when collecting and reviewing data located outside the United States.

Blocking statutes

Blocking statutes are laws specifically designed to prevent cross-border discovery. They are an entirely separate issue from data protection regimes, and implicate all types of discovery – regardless of whether the discovery concerns sensitive or confidential information. They are therefore significantly greater obstacles to compliance with US discovery requirements than data protection statutes.

Several European countries insist that all court-ordered discovery occur only under supervision of their own courts – essentially requiring compliance with the Hague Convention on Taking Evidence Abroad in Civil or Commercial Matters, even if the entity gathering the data is the data's owner. In other words, several countries prevent a corporation from collecting its own data, or interviewing its own employees, if the purpose of that data gathering is to comply with US discovery demands. This can present virtually insurmountable problems for US litigants. In December 2007, a French court provided a dramatic illustration of the risks blocking statutes create for US litigants and their lawyers. The French Supreme Court decided the case of *In re Advocat 'Christopher X'*, which concerned a French lawyer who attempted to obtain discovery in France on behalf of a US-based litigation. In a decision subsequently upheld by the French Supreme Court, the lower court convicted the lawyer for violating a French statute that

prohibits 'requesting, seeking, or disclosing in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature for the purposes of constituting evidence in view of foreign judicial or administrative proceedings'.

The French lawyer was fined €10,000 or about US\$15,000. Many observers believe that if the lawyer involved in the incident had not been a French national, he might have been sentenced to jail. Obviously, when US litigants are forced to collect data or conduct other discovery in France or other countries with blocking statutes, they must do so only after consulting with competent local counsel and complying with the required procedures.

Relevant labour laws

In addition to blocking statutes, some jurisdictions have labour laws that make compliance with US discovery requirements difficult. In general, US law assumes that a corporation has the right to search and turn over virtually any data in its possession. In most instances, this includes even the personal data of its employees that they have saved on the corporate network. In other words, US law generally holds that by choosing to use the corporate network or corporate computers to conduct personal communication or other activities, employees waive the right to keep this information private from their employer. Not all countries take this view.

Several European countries have labour laws that specifically prevent an employer from viewing an employee's private information, even if that information is stored on the corporate network. Some jurisdictions require that employers identify and set aside (without reviewing) any documents marked 'personal' or 'private'. Other countries require that employees or their works council be notified of any effort to process or review their data. Though these types of laws are unlikely to prevent a corporation from gathering its own data, it can make that process more complex and costly. It is the sort of legal issue that will require consulting competent local counsel to ensure that a methodology can be developed to comply with both US discovery obligations and local labour laws.

US view of foreign laws preventing US discovery

The obvious first choice when faced with the conflict between US discovery requirements and foreign laws making that discovery difficult, expensive or illegal is to ask the US court for relief from the discovery obligation. Asking for relief may be a necessary first step to minimising the conflict, and in some instances it may help reduce the scope of the problem. However, litigants

cannot expect that US courts will be quick to solve this dilemma for them. If the court believes that the relevant data is crucial to the case, it is highly unlikely to let the litigant hide behind foreign law to avoid its US legal obligations. In 1987, in *Société Nationale Industrielle Aerospatiale v United States*, the United States Supreme Court held that foreign parties to US litigation may be compelled to produce evidence in a US court, even if doing so violates a blocking statute. Presumably the same precedent will cause a US court to force a litigant to provide discovery even if doing so violates the EU Data Protection Directive or similar laws.

European view of the conflict

The European Union is aware that the territorial limits on data transfer imposed by the EU Data Protection Directive are somewhat inconsistent not only with US discovery rules, but also with the normal business needs of multinational corporations. Indeed, on 11 February 2009, the EU published a paper, with the wonderfully bureaucratic title of the ‘Article 29 Working Group, Working Paper 158’, in an attempt to address this dilemma. The Working Paper begins by correctly laying out the nature of the dilemma discussed above. It recognises that the territoriality of the EU rules does not reflect the reality of the multinational nature of many businesses, and that it creates a potential conflict with discovery obligations under US rules.

Though it recognises the dilemma, the Working Paper does not provide a solution to it. Instead, it provides guidance to entities facing the issue, but not a safe harbour. In other words, even if a company strictly follows the Working Paper’s guidance, there is no guarantee that it will not be found to have violated the implementing statutes of the Data Protection Directive. In essence, the Working Paper recommends that companies must themselves engage in a balancing test to determine whether the transfer of the protected data is appropriate. The party must balance the proportionality of the disclosure against the need for the disclosure. The company must also consider the relevance of the personal data to the subject of the litigation and the consequences of the disclosure to the data subject. Of course, the reasonableness of a balancing test is in the eye of the beholder, so it is not clear how much help this guidance provides.

The Working Paper does make a few procedural suggestions, which provide clearer guidance. It suggests that the data controller (in other words, the corporation that needs to provide US discovery of the relevant data) should redact or use pseudonyms to obscure the personal data; use a trusted third party to filter the data; avoid providing unnecessary personal data; and carry out the culling and redaction within the EU before the data is transferred to the US.

Dealing with the conflict

Checklist for dealing with the dilemma

There is no simple solution for dealing with the conflict between US discovery obligations and conflicting foreign laws. However, there are several strategies that companies can pursue to minimise the risk of legal troubles on either side of the Atlantic.

The following checklist is based on the guidance provided in the Article 29 Working Paper, as well as the work of the Sedona Conference, the premier US-based think tank on issues of electronic discovery in US courts, as well as the author's own experience. It is intended to provide a basis from which litigants, lawyers and their computer forensic consultants can draft a workable plan. Of course, every case is unique, and not all of these options will be practical, or even advisable in every case:

- *Overall considerations for diagnosing the scope of the conflict:*
 - Does the US court have jurisdiction over the data in question?
 - Is there a blocking statute or other law that prevents gathering the data?
 - Must the Hague Convention procedures be used to obtain the data?
 - Does the data contain personal information that is protected by the EU Data Protection Directive or similar law?
- *Steps for resolving the conflict:*
 - In the US:
 - Educate opposing counsel and seek to limit the scope of the proposed discovery
 - Seek a protective order from the US court limiting the scope of the discovery
 - Seek permission to redact the names or provide pseudonyms for the data subjects
 - Raise these issues early in the litigation to prevent surprises to the court
 - In the EU:
 - Seek consent from the data subjects if at all practical
 - Inform European-based managers and employees of the process and the attempts to protect their data
 - Cull the data within the EU
 - Process, review and redact the data within the EU, thereby minimising the volume of protected data that must be transferred to the US
 - Engage in and document the balancing tests suggested by the Working Group
 - Document the efforts made to protect the data
 - Use safe harbour certified consultants.

Final thoughts

The Sedona Conference checklist is a useful starting point for thinking through how to resolve the conflict. Its central insight is that often the conflict seems worse at first glance than it turns out to be in practice. Most of the time, the initial requests for production of data from the opposing party are overly broad. Most of the time, reasonable litigants – or at least reasonable US judges – can be persuaded to narrow the scope of the request so that it does not conflict with the EU Data Protection Directive. Alternatively, in most instances, US litigation will allow redaction of the sensitive information that creates the conflict.

Similarly, steps taken by litigants within Europe will often be sufficient to limit the exposure to the EU Data Protection Directive. Most employees and other affected individuals will give consent to the transfer or disclosure of the sensitive data if they understand why it is necessary and that it is being sufficiently protected from further disclosure. It is usually possible (if expensive) to do the initial review, culling and redaction within the EU, to minimise the amount of data transferred to the opposing party in the US. Typically, the steps taken to document efforts made to protect the data will meet EU data protection requirements.

The problem with these suggestions is obvious from the hedging language in the paragraphs above: ‘most of the time’. There will be occasions (hopefully rare) when these steps are insufficient to resolve the dispute. Sometimes, US courts will refuse to limit the scope of discovery, and the key sensitive information will be too crucial to the meaning of the document to redact. Some European employees will refuse to cooperate – indeed they may well alert the data protection authorities to what they perceive to be a violation of the data protection regime. In these cases, the clash of law may be unavoidable. This obviously puts litigants into an impossible position, from which there is (by definition) no good solution. Assuming that the US lawsuit is sufficiently important (or costly) that its requirements cannot be avoided, the best that can then be done is to comply as much as possible with the EU Data Protection Directive, and hope that this evidence of good faith will deter the authorities from punishing the litigant. Alternatively, a European litigant may decide that the reputation risk of being perceived to have violated the EU Data Protection Directive is so great that it is worth the cost associated with appealing the discovery order within the US system, or even worth the risk of losing the US lawsuit to avoid disclosure. Such decisions can only be made on a case-by-case basis in consultation with expert legal and technical advisers.