Electronic Discovery

(EU versus US)

GENEVA GROUP INTERNATIONAL

European Conference - Lisbon, Portugal - April 19, 2013

Att. Patrizia GIANNINI

GIANNINI
STUDIO LEGALE

GENEVA GROUP INTERNATIONAL

S4B

Discovery is

the process of:

identifying

preserving

collecting

preparing

reviewing

producing **information** in the context of litigation.

Electronic Discovery (E-Discovery)

is the same, but includes

Electronically Stored Information

("ESI")

Some examples of ESI

- electronically stored information - are:

emails

word documents

power point presentations

excel sheets

social media posts

voice mail and videos

All official records (medical, banking, tax, property)

E-discovery in the European Union

The EU has one of the strictest data protection systems in the world.

In the EU data protection is

A HUMAN RIGHT

and is protected by article 8 of the

Charter of Fundamental Rights of The EU.

The controlling law in the EU is the

Data Protection Directive 95/46/EC

All national member States have adopted this directive; some States have gone further in personal data protection.

There are quite a lot of differences in implementation of the Directive:

France, Germany, Spain, and Italy

have stricter rules, while the

UK has a broader interpretation.

As with many EU directives, individual States differ in the application of this directive, so one must determine which national law is applicable in any given situation.

On January 25, 2012, the European Commission proposed a new Data Protection Regulation, which should replace Directive 95/46/EC.

Directive 95/46/EC regulates the processing of

"personal data"

that is *"any information relating to an identified or identifiable natural person or "data subject""* (Art. 2 (a) Dir. 95/46/EC).

For example, in EU

an email address is *"personal data".*

"*Sensitive Personal Data"* is personal data that reveals *"racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life".*

Processing such data is, in principle, prohibited, (with few exceptions - Art. 8 of Dir. 95/46/EC).

There must be a legal basis to discover personal data.

There are only two legitimate bases for processing personal data under 95/46/EC:

1. informed and freely given consent by the person/entity
2. legitimate interest of the data controller, balanced with the fundamental rights of the person/entity.

E-discovery is a "legitimate interest", but for *sensitive* personal data, consent is the only legitimate basis for e-discovery, and it must be explicit, not implied.

E-discovery in the US

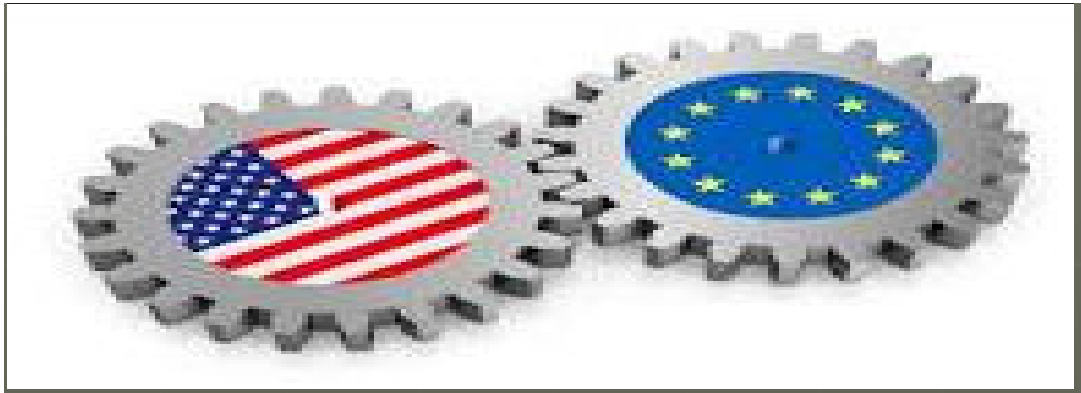
The US Rules of Civil Procedure control discovery—and E-discovery—of documents and things in a party's possession, custody or control.

In general, a party may request the other party to produce (inspect, copy, test) the following items:

- any requested documents or electronically stored information, including translation thereof
- any requested tangible things

to permit entry and inspection onto identified land, buildings, or other property.

In principle, any non-confidential matter that is relevant, is discoverable even if it is not admissible as evidence, as long as it "may lead to the discovery of admissible evidence".



EU vs US – The differences in discovery

The US has the broadest civil discovery procedure in the world.

None of the other Common Law countries, such as

the United Kingdom, Australia and Canada, have such a wide scope of discovery and in most of the Civil Code countries, such as Europe and Latin America, the concept of discovery obligations is almost unknown.

When e-Discovery is conducted outside of the US, for example in a foreign affiliate of a US company, the basic procedure is the same. However, there are many complications due to different laws that apply when data is requested from other countries. Many non-US countries have laws protecting data from being collected from/exported to another country.

To a US lawyer, working with such broad discovery rules, the EU system seems

toooooooooooo closed off!!!

There is a serious problem for US firms with affiliates in EU countries, when they get involved in civil litigation within the US:

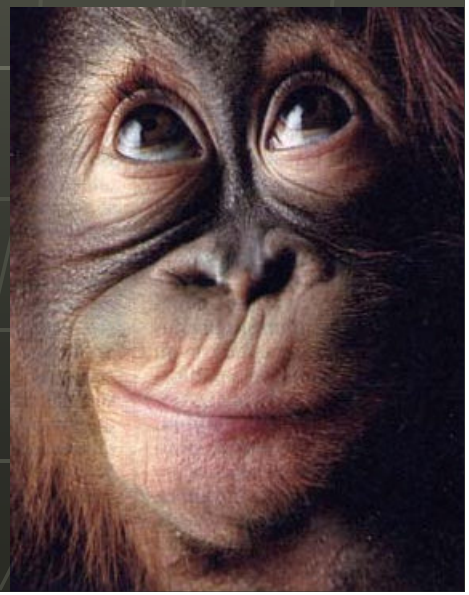
On one hand, US rules require retention and production of all relevant data, even data located outside of the US, or risk severe penalties by the Courts in case of "spoliation" (failure to preserve data)

On the other hand, EU data protection laws require strict data protection rules for "personal data" of their residents, which seriously restricts processing of this data and transfer of this data to "non-adequate" countries (US) outside of the EU, with risks of costly fines in case of violation.

So, what can we do????

Possible solutions to this DILEMMA

1) The EU should filter and review ESI for relevance.
2) Personal data should be anonymized.
3) The parties should obtain protective orders and "filings under seal" from US courts to protect data from outsiders.
4) A notice should be sent to all employees/customers whose emails or other data are collected. These people have a right to know that information is being collected about him/her.
5) Data Controllers (parties, law firms and courts) should take reasonable measures to protect personal data from unauthorized access.
6) If the collection of e-discovery is delegated to an outsider, there must be a written agreement for confidentiality and security, including how the data is used, kept and retained.



Transfer of Personal data from EU to US

How it works

As stated above, there must be a legal basis for transfer of personal data outside the EU, which can be done by consent from the person involved transferring the data to a

"Safe Harbor"-certified company in the US,

- transferring the data under standard contractual clauses,
- transferring them to companies that have binding corporate rules in place.

The question remains, however, as to how this personal data may be legally transferred to opposing counsel and to the Court; you should request a protective order from the Court to guarantee a degree of privacy.

Conclusion

US affiliate firms in the EU who have to follow e-discovery rules, and simultaneously follow EU data protections laws, are in a conflict.

Under the US Rules, including the spoliation rule (failure to preserve data), US Courts have great power to apply whatever punishment they choose, including costly fines, "adverse inferences" (jury assumes missing ESI is adverse to the person who lost the evidence), and even dismissing the case.

Over the past few years, case law has shown that US Judges are imposing more sanctions on parties who have "spoiled" ESI.

These rules apply to all relevant ESI issues in the US, regardless of their geographical location or local laws.

Therefore, US affiliates in the EU must have a discovery preservation procedure, since the mere expectation of a lawsuit obligates a party to preserve ESI data.

US affiliate firms must also have proper management systems for "information governance."

Since storage of ESI has become so inexpensive, the tendency has been to store everything, forever.

This can be disastrous since, after a lawsuit begins, nothing potentially relevant may be deleted. Therefore, a company may have to pay a high price to process enormous amounts of useless information.

To save money, these affiliates should invest in "information governance," (deciding which data will be preserved for how long). This should be tailored to the company, and the type of industry and its regulatory/ business requirements.

In the context of EU data protection rules, US affiliates risk investigation and fines/sanctions by local data protection authorities.

The extent of the risk depends on the country where the ESI is located; for example, if the ESI is in Germany, the risk is much higher than if it is in the UK.

Most data protection authorities are understaffed and underfinanced, and there have been complaints about lack of compliance and/or enforcement.

For example, a 2011 study in France showed that 82% of French enterprises do not obey the French Data Protection Act of 2004.

But with the recent major changes to EU data protection laws, including strengthening the ESI subject's rights and increasing enforcement of the law, companies should make sure they have the right ESI preservation systems.

US courts have decided that merely because a company has outsourced ESI data, the company still must comply with the rules for E-discovery.

Companies will have to do a case-by-case "balancing test" between the risks of compliance with the US rules, and the risks of non-compliance with the EU data protection laws.

Perhaps the US courts and the EU data protection authorities should do this balancing test, when companies find themselves in this conflict ...

perhaps!