FROM LEGALTECH NY 2010: International e-discovery — the legal complexities of collecting, culling and reviewing data from multiple countries

Feb 9th, 2010 | By Gregory P. Bufithis, Esq.

This post is one of several summarizing our coverage of LegalTech New York 2010. For our other posts click here.

Reporter: Christian Aust

Trilantic is a leading U.K.-based legal support provider that focuses on electronic discovery services. They sponsored a double-panel for the International E-Discovery track at LegalTech. The panels introduced and discussed EU data protection rules and their practical implementation, including how corporations must respond to U.S. litigation and regulatory matters involving data held in the EU.

The importance of understanding EU data privacy issues when embarking on electronic discovery outside of the U.S. cannot be understated. Litigation, regulatory and compliance matters often require rapid data collections, which if not done according to the rules, could result in breaking criminal laws. Corporate and law firm attorneys therefore must stay abreast of current laws and regulations governing that data to ensure it is handled properly throughout every step of the process.

The panel was moderated by Nigel Murray, Managing Director of Trilantic. Participants in the session panels included:

From the EU: Senior Master Whitaker(Senior Master of the Supreme Court and committee member of the Hague Convention); Chris Dale (founder of the e-Disclosure Information Project); and Vince Neicho (Litigation Support Manager, Allen & Overy)

From the U.S. : Judge Andrew Peck (Magistrate Judge, Southern District of New York); Browning Marean (partner, DLA Piper); George Rudoy (Director of Practice Support, Shearman & Sterling); Maura R. Grossman (Counsel, Wachtell, Lipton)

Part 1

It is necessary for U.S. companies to understand the legal complexities of collecting, culling and reviewing data from multiple countries. And it is a two step process:

The first step is to create and implement a solid litigation readiness and response plan. When litigation hits, the second step is to harvest and process the data.

What should organizations be doing? In the US, the need for corporations to create and implement a solid litigation readiness plan is ever increasing due to both the sheer volume of litigation that corporations are facing and the costs associated with eDiscovery. Outside the US though, this need may not necessarily be so acute. For example within the EU outside of the UK, any litigation which a corporation is involved in that is to be heard by the local courts involves no discovery. So, if there is no obligation to find and hand over documents, then why spend the cost of preparing for such an eventuality?

The exception to this though is when corporations are facing regulatory enquiries, whether these be under the Foreign Corrupt Practices Act, competition inquiries or other agencies.

Historically, many corporations based in Europe have taken the view to "self-insure" – i.e. spending money in preparing for an unlikely eventuality is not viable and if such an eventuality was to hit them, then to accept that the associated costs are part of doing business. This however is slowly starting to change as corporations are increasingly facing regulatory enquiries. So, European subsidiaries are having to adopt some of the processes and procedures being used in the US.

The real first step for any organization is to have a document retention policy (for instance, determining what documents should be retained, for how long and where these documents should be stored, etc). Their document retention policy should also include the procedures for systematic destruction of documents. They should also have procedures to monitor and enforce compliance with these policies.

The company then needs to establish a protocol for responding to requests for electronic documents. The protocol should encompass identifying potential sources for relevant information and preservation of this information. It should also address the methods for extracting the data, and identifying and reviewing relevant documents.

As part of this plan you need to choose whether you have the resources and wherewithal in-house to collect and process elements of the electronic discovery or whether you need a partner who can work with you in a highly collaborative approach to meet your needs, one which is locally based and who understands the local rules and regulations.

Harvesting and processing the data. Now, how is this done within the EU? The European Union's Data Protection Directive prevents companies sending personal data outside of the EU except when the destination country has been pre-approved as having adequate data protection. Only a handful of countries – Argentina, Canada, Switzerland, Guernsey, the Isle of Man and Jersey – have qualified as having adequate protection.

Despite these European provisions to protect personal data and restrict the transfer and use of that data, U.S. courts have been largely unsympathetic to defendants facing these obstacles and have even sanctioned companies who have failed to comply with discovery requests that violated local and international data privacy laws.

All countries of the EU have their own data protection acts however over the last year there have been two key realizations: data is being collected wholesale and shipped to the US with total disregard to the individual country rules; and there needs to be a mechanism in place to ensure that court requests for documents can be met without compromising the fundamentals of the right to privacy of the individual. There has been a lot of discussion as to how these conflicting requirements (US courts versus the rights of the individual) are going to be resolved.

The panel noted there have been two recent announcements in this area:

On 1 September 2009, Germany made some important amendments to their Federal Data Protection Act (The BDSG). The most relevant amendment: data controllers who engage a third party to process data will be guilty of a regulatory offence punishable by a fine if the data processing agreement is incomplete in contravention of Section 11(2) of the BDSG (Section 43(1) No. 2b). These new guidelines are more stringent than was the case before – when even the old ones were regarded as draconian by a lot of data controllers.

On 19 August 2009, the French Data Protection Authority (CNIL) released a new "opinion" on the transfer of data from France to a country outside Europe. The Opinion is noteworthy for describing how personal data can be transferred from France to the United States pursuant to U.S. discovery proceedings.

So, until there is clarity what can corporations do? There are 3 options:

Option 1. The first method is for the corporation to adopt Binding Corporate Rules (BCR). This involves a company submitting its data protection processes to a data protection watchdog and having them approved for use. But the process is both lengthy and costly.

Option 2. A second method is to allow the transfer of data across borders under the "Safe Harbor" framework. In order to bridge the different approaches to privacy between the US and the EU and to provide a streamlined means to allow US organizations to operate in Europe, the

US Department of Commerce and the EU Commission developed a "safe harbor" framework which was approved by the EU in 2000.

Not all of this sit easily because there a commonly held believe that because a company has Safe Harbo data can be collected wholesale from the EU and transferred to the US.

Option 3. A third method is to obtain a letter of request under the Hague Evidence Convention from a district court. The Hague Evidence Convention is a treaty that allows the transmission of evidence from one state to another under certain guidelines. Obtaining an approved letter of request permits the transfer and processing of data. However, this process can take 6-12 months, often rendering this solution inapplicable to e-discovery requests with strict court-appointed deadlines.

Part 2

There was more discussion on Safe Harbor, the Hague Convention and recent guidelines and rules within the EU and more of a to-and-fro amongst the panelists. Maura Grossman opined that "compliance" is not possible; the aim can only be risk mitigation via a set of "unpalatable alternatives": And she suggested consent – simply ask the subjects of the data if it can be released. But she also noted that consent is often not possible to obtain and is "inherently coercive" and is only practicable where the number of subjects is limited and the data is not co-mingled.

Jumping in, Browning Marean noted that the consent must be: informed, given before the transfer of data, revocable.

The more problematic issues are those surrounding the Safe Harbor rramework. Developed in 2000 by the U.S. Department of Commerce in consultation with the EU Commission as a streamlined approach for U.S. companies with frequent data transfers to comply with the EU's 1998 data protection directive.

Participation in the safe harbor is voluntary and requires self-certification by the participating company that it agrees to adhere to the rules. Under those rules, the company must tell the custodian: what data, for what purpose the data will be used, to whom the information will be disclosed, etc.

But there are limitations: currently it is only possible if the organization/company falls under the jurisdiction of the FTC. And certain industries are not eligible (e.g. telecomm)

Also, Safe Harbor only permits transfer into the U.S. but not onward transfer to 3rd parties (even the DOJ or SEC). However, an organization can get affirmation in writing from the receiving party that it will follow the same rules.

As George Rudoy said, in reality Safe Harbor certification is not much use in the EU and is definitely not a "free pass".

The panel then turned its attention to the Hague Convention (or as it is "popularly" known "The Taking of Evidence Abroad in Civil or Commercial Matters, 18 March, 1970).

Senior Master Whitaker said it is a multi-lateral treaty and there are two types of situations where requests for documents are made in the EU:

1. Where the data are in the control of one party and there exist blocking statutes or data protection laws

2. The data are not in control of one the parties but in the control of a 3rd party in the EU

He said that he is responsible in the U.K. for dealing with requests under the convention. In the past 2 years he has only had one request. Generally all requests are only for type #2 above. And he commented "the Hague Convention is longwinded, a costly procedure that doesn't always produce what you want".

There are two methods to get documents/evidence:

Chapter 1 – Letters of Request: a request by the court where the action is pending to the designated "Central Authority" of the contracting state where the evidence is located. The "Central Authority" passes the request on to the appropriate body. You must use the procedure of the requested state

Chapter 2 – Taking of Evidence by Diplomatic Officers, Consular Agents or Commissioners

Senior Master Whitaker's experience, Chapter 2 is only used by mistake. In practice only Chapter 1 is used.

Key issues/tips:

1. Timing: the key to success is using an agent, e.g. a solicitor, to make the application for you and to do it early.

2. Best thing to do is organize everything with the witness that is located in the EU.

In many instances, the opponent will only make a fuss once the matter is with Senior Master Whitaker and then pay for the 3rd party's legal counsel to contest the request. Purpose? to bog you down.

3. Key: make sure the documents are needed at trial — and not a U.S-type deposition!

This is not about discovery/disclosure but to get documents you know they have. When applying for documents, do not use "All documents relating to…" because this looks like a deposition request (fishing expedition).

This may seem like a semantic argument, but it is necessary to specify exactly the documents you are seeking — if only by the time period, subject matter etc.

Conclusion? if you need to use the Hague Convention then do it quickly and early and cancel if you need to because the discovery period may close before it is processed.

Judge Peck noted that a US District Court may order a party to provide a detailed description of documents in a deposition or interrogatory manner and then put that information into a Hague Convention request. But nobody on the panel could recall having used the Hague Convention successfully.

Maura Grossman also discussed the use of Binding Corporate Rules (BCR) mentioned in Part 1 which allows group of companies to transfer data amongst each other. The downside: it requires the approval of all data protection authorities in all localities and no company has yet achieved approval in all countries. But approximately 6 companies have implemented some form of this so far.

And there is ad hoc adequacy which requires proof that data would receive the same level of protection as it would receive in its home jurisdiction. Example: Hong Kong data, hosted in U.K., reviewed in India. To ensure protection, the data is batched to reduce risk. Each reviewer receives two batches (a main one and a "spare") and batches had to be returned before new ones were issued.

European Data Protection Working Party paper 158 (adopted February 2009) contains suggestions for data controllers subject to EU law and has two parts: (1) comparison of common and civil law jurisdictions and (2) practical steps and guidelines. In general, data may only be stored and processed for specific, anticipated litigation. In addition there must be a legitimate reason for processing the data and a legitimate reason for transfer.

Concluding remarks by the panel:

- consent is not a good basis because it's not unequivocal, etc.

- it is always a balancing test between the custodian and requester

- involve the data protection authorities as early as possible

- "notice" is critically important

- use Rule 30(b)(6) depositions as these are often more successful

- also refer to **Mancia v. Mayflower** case by Judge Grimm which is an excellent overview of the federal rules and other law that require a cooperative approach to discovery. The opinion establishes a solid legal foundation for the new Sedona Conference Cooperation Proclamation. The Mayflower opinion shows that far from being a Utopian ideal, the cooperative approach to discovery promoted by Sedona is already mandated by the law.

- Murray noted that in-country review is best as has been borne out by the spike in e-discovery work and document review across Europe.

- Vince Neicho suggested that parties should "think about other sources for the same data. The data may already be here!"

- Judge Peck noted that with the exception of the Hague Convention it is very difficult to comply with both U.S. disclosure rules and EU protections. You must do risk analysis. And cooperation among counsel from both sides is crucial.

- Maura Grossman suggested reference to the Working Group 6 publication **Framework for Analysis of Cross-Border Discovery Conflicts**

The panel concluded by saying that It is clear that the current approaches to cross-border e-discovery each have their challenges in light of the vague and perilous data privacy landscape. As a result, corporations are having to look at alternative ways of meeting the conflicting requirements of the courts and the EU rules. The first step is to collect, process, search, cull-down, and review data in country. This dramatically reduces the size of the dataset, allowing local counsel to quickly remove irrelevant documents and focus on the relevant data and custodians involved.

Gregory P. Bufithis is the founder and chairman of The Posse List and its sister sites The Electronic Discovery Reading Room (http://www.ediscoveryreadingroom.com) and The Posse Ranch (www.theposseranch.com). He is also founder and chairman of Project Counsel (www.projectcounsel.com).