



An interview with Nigel Murray of TRILANTIC; the nuts & bolts of European e-discovery

Jan 22nd, 2010 | By Gregory P. Bufithis, Esq.

This interview is part of our new series “Data! Data! Data!” — Cures for a General Counsel’s ESI Nightmares”. For our introduction to the series [click here](#).

As we have indicated in numerous posts, if we are to believe the prognosis of many economists, the current recession is on the verge of ending. The rebounding economy will most likely re-invigorate corporations to push their markets globally. This, in turn, will further push litigation and regulatory inquiries globally. But as our Posse List Europe membership knows we have already seen a surge of e-discovery work in Europe, much if it already due to governmental investigations and inquiries. So we turned to our colleague, Nigel Murray, to discuss the e-discovery market in Europe.

*Nigel Murray is the founder and Managing Director of **TRILANTIC** and he has long been at the forefront of providing electronic document management services since the early 1990s. He began his career in legal technology as litigation support manager at a major London law firm. He then started the first British litigation support company in 1993 — Bowhawk. There, he worked on the massive cases of the 90’s – Tobacco, BCCI etc. From there, Nigel brought the electronic side of litigation support into an existing document management company by way of a merger. Having worked on the first UK eDisclosure matter in 2001, Nigel has been at the forefront of the development of the industry within the law firms in the UK. Nigel launched TRILANTIC in May of 2005. He is a long-time member of The Sedona Conference.*

TRILANTIC has been cited as a top e-discovery provider by the influential Socha-Gelbmann Annual Electronic Discovery Survey from Socha Consulting and Gelbmann & Associates. TRILANTIC is the only non-US provider to get such a ranking, reflecting both the increase in cases which have a European or UK dimension as well as TRILANTIC’s increasing involvement on both sides of the Atlantic. In fact the survey called him “a founder of the litigation support industry in Europe”.

We caught up with Nigel at the ACC Annual Meeting in Boston last year, and then again at his offices in London.

TPL: To quote [Chris Dale](#) “in the e-discovery world, most Americans have seen Europe as a cross between a modest museum and a commercial colony full of obstructive civil servants obsessed with data privacy”. Granted, that is changing. Your take on this?

NM: [laughing] I’ll avoid addressing Chris’ comment directly. Let me say that 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 e-discovery. Outside the US though, this need may not necessarily be so acute. For example within the EU (outside of the UK) most litigation with which a corporation is involved will be heard by the local courts and involves no discovery. So, if there is no obligation to find and hand over documents. Why spend the cost of preparing for such an eventuality? Well, the two big exceptions to this being when corporations are facing regulatory inquiries from their own or other European regulators or if they face Litigation of regulatory enquiries from the United States whether these enquiries be under the Foreign Corrupt Practices Act, competition inquiries or other agencies.

TPL: But 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.

NM: This however is slowly starting to change as corporations are increasingly facing regulatory enquiries. European subsidiaries are having to adopt some of the processes and procedures being used in the US and European regulators are becoming more active since the recent credit crisis. 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.

TPL: Ok, but we suppose that part of this plan means 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?

NM: Of course. That’s why you need to hire TRILANTIC!

TPL: Ok, I walked into that one. So, I now have a locally based partner who understands the local rules and regulations. Now what?

NM: The second step is harvesting and processing the data.

TPL: How is this done within the EU?

NM: Ah, this is where the fun starts. 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.

TPL: Hold on. 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.

NM: I'll give you that one. All countries of the EU have their own data protection acts however over the last year there have been two key realizations: data is often 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. There have been two recent announcements in this area. But I do not want to clog up this interview with a recitation so let me give you this pdf [[link](#)].

TPL: So, until there is clarity what can corporations do?

NM: In brief, there are 3 options: (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; (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, although this is not necessarily the answer as once in the US it cannot be passed onto any other organisation unless that too is "safe harbor" certified; and (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. This latter though can be very time consuming.

I have only skimmed the surface on this. The link I gave you above has more information.

TPL: Thanks. So, to summarize: it seems 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.

NM: Correct.

TPL: Let's chat more about the mechanics. The challenge with conducting e-discovery in-country is that it is perceived to be very costly and time consuming, especially when the expertise has to be flown to Europe from the US. Which is why you need locally engaged support.

NM: Obviously I totally agree. In order for e-discovery in-country to be a viable option, corporations need to work with service providers who have the capability either in-country or with the ability to rapidly set up a facility in-country. These service providers should be able to react quickly and be able to deploy the right number of skilled people with the appropriate hardware and software with a minimum time delay. These solutions must provide advanced search and analysis capabilities that enable early case analysis, rapid cull-down, and quick review. And these systems must be able to work with any language or character set by being Unicode compliant. Organizations facing these cross-border e-discovery challenges must ensure that their people and processes match the technologies being utilized and are appropriate in their specific legal environment.

TPL: And the use of local counsel?

NM: The best way to ensure it all gets done right is to solicit local counsel in the country in which e-discovery is being conducted. Not only can they advise on the local data privacy requirements that exist in addition to those dictated by the EU's Data Protection Directive, but they can add unique insight when interpreting email and document data that often contains local colloquialisms and contexts. This can prove invaluable when culling irrelevant data, conducting searches, and performing early case assessments. A plug here, TRILANTIC has built up a network of local counsel in 27 countries of Europe who are able to provide local advice on such matters.

TPL: You also have software familiar to US attorneys, yes?

NM: We do. We use a range of industry leading software for early case assessment, email threading, and review which will all be familiar names to those who follow this industry in the States. Such familiarity gives the US clients the comfort that by using a local service provider they will be using software and processes which have been tried and tested in the US.

TPL: E-discovery vendors have had much success over the last 2 years moving into the e-discovery space across the whole EDRM model, especially in the area of document review, a success due to the continuing move by corporations to move EDD directly in-house. Document review is a nice piece of change. Are you planning any moves to the "right side" of the model?

NM: Since I started TRILANTIC we have offered document review. What we are seeing now though is the need to be able to offer review locally – i.e. placing the servers behind the client's "firewall" so that not only is the processing taking place at the client's offices, but the resulting data does not leave their control until the review team have reduced the overall volume to only the most relevant documents.

TPL: Do you staff your document review projects directly, use a staffing agency, or is there a mix? How do you choose these agencies?

NM: We do not offer review directly but partner with companies who specialise in such services such as [Project Counsel](#).

TPL: E-discovery costs are skyrocketing. Yet much of EDD is now a commodity – and that has changed the structure of the market. Prices are — shall we say — more predictable and probably more realistic. E-discovery vendors have capped fees, set flat fees or worked with various forms of pricing estimators. Have you changed your pricing?

NM: We certainly have and for the last 18 months we have offered a fixed priced model for the early stages of a matter, which combined with our competitive pricing structure and forecasting model gives the client the comfort that they can keep control of the costs at all stages of the matter.

TPL: Going back to the EU data privacy rules, you have kindly pointed us in the direction of a couple of articles, however where can practitioners in the United States learn more about the practicalities of handling European data?

NM: From our website resources page which you can access by [clicking here](#).

TPL: Nigel, we greatly appreciate your time.

NM: Thank you and I appreciate the opportunity to talk to you as I am always impressed by the practical stance taken by the regular postings from the Posse List. See you at LegalTech.

Note to readers and attendees of LegalTech in New York: On 1 February, in New York, as part of the Legal Tech show TRILANTIC has laid on a double session where they have brought together a US panel of experts, including a New York judge and an EU panel consisting of a UK judge who is on the committee for the Hague Convention and other experts. Subjects covered will include privacy considerations and EU data protection rules, compliance with them, and the proper response by corporations to US litigation and regulatory matters involving data held in the EU. For the press release [click here](#). And for a post by Chris Dale, one of the participants, [click here](#).

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).