The Metropolitan
Corporate Counsel®
National Edition
www.metrocorpcounsel.com
Volume 22, No. 3 March 2014

Issues In Global Discovery In The Wake Of Heightened Privacy Concerns

The Editor interviews ***Craig Earnshaw,*** *FTI Consulting, Inc.*

Editor: Please tell us about your background and the types of matters you commonly work on.

Earnshaw: I have 17 years of experience in helping clients with computer forensics, fraud investigations and e-discovery, or e-disclosure as we say here in the UK. In 2006, I founded the London practice of FTI Technology, the business practice within FTI Consulting focused on e-discovery. In 2011 I was part of a team that launched FTI Investigate, a mobile offering that allows companies to collect, process and review data on-site and in accordance with local data privacy laws. Through this, much of my practice relates to cross-border work, including regulatory investigations, litigation and, lately, many antitrust investigations, which are increasingly cross-border in nature.

Editor: You spoke recently on the topic of multinational matters on a panel at LegalTech New York. Who participated on the panel?

Earnshaw: I was very fortunate to share a panel with some impressive people from a range of backgrounds. Gareth Evans, a litigation partner from Gibson Dunn & Crutcher LLP in Orange County, and Ellen Frye, a litigation and antitrust associate with Simpson Thacher & Bartlett LLP in New York, both offered outside counsel perspectives. Jennifer Hamilton, global discovery counsel at John Deere, provided an in-house viewpoint, while David Horrigan, an analyst in e-Discovery and Information Governance from 451 Research, served as an industry commentator. I moderated the session as the outside e-discovery consultant. Together we offered different viewpoints on data privacy in cross-border investigations and disputes. We had a wonderful audience.

Editor: One of the issues your panel discussed was the Matthew Snowden revelations and how they are impacting multinational matters. Have you seen any changes?

Craig Earnshaw

Earnshaw: Very much so, and in various ways. I think the most significant impact has not necessarily been on the legal level, but on the level of general public awareness. In the U.S., the conversation about data privacy and information security has moved from the boardroom table to the dinner table. It's in the day-to-day national consciousness that personal data is being stored, collected and perhaps even reviewed, and it's brought Americans to an inflection point about attitudes towards privacy.

Meanwhile, over recent years, data protection legislation has been enacted all over the globe – some of it more developed and robust in certain jurisdictions and legal systems than in others. We've got data privacy legislation not just in Europe, but also now in the Middle East; numerous countries in Southeast Asia and now Latin America are following suit. So, the Snowden revelations gave rise to significant political tensions around data privacy in relation to the transfer of data from international jurisdictions to the U.S. Where a U.S. parent company engages a U.S. law firm to conduct a cross-border investigation or respond to a regulatory inquiry from a government agency, a subsidiary in Germany, France or even Indonesia will now be even more concerned about moving any of its data to the U.S.

Editor: What were some of the other key takeaways from the session?

Earnshaw: For one, when working on international matters, consider the more challenging international aspect first. Due to legislation within a particular jurisdiction, you may be taking a step into the unknown and having to deal with new time frames, processes and protocols.

Next, put some thought into the culture of the foreign jurisdictions, as they may be quite different from what you're used to in the U.S. Paris, France is not the same as Paris, Texas. In addition to a different legal system, you've got different languages, different cultures and different attitudes to privacy. They will all impact how you should handle the situation.

Another key takeaway was to inform the judge and the other side (if it's litigation) or the regulator or government agency you're responding to that there are international aspects to your work. If you've got to deal with French blocking statutes and European data privacy legislation, you're much more likely to receive a better response from a U.S. judge if you raise the fact on day one rather than on day minus one of your discovery deadline.

The panel also advised maintaining a steady, open dialogue between the organization, outside counsel and any technical provider because each of those parties brings a unique skill set to the table. The combination of experience and viewpoints from all three groups can help ensure a more cost-effective and defensible response that adheres to the jurisdiction's legal framework as well as to the corporation's procedures and protocols.

Another important discussion point was around the technical framework. What are the technical solutions that can be put in place to enable compliance with that legal framework? How much work do we need to do in-country, and at what point can we transfer the data across the border? Where do we feel comfortable moving it?

Lastly, you must ensure that the technology that you utilize is actually going to work in the region where you are conducting your review. If you've got a service provider, make sure their data processing and document

Please email the interviewee at craig.earnshaw@fticonsulting.com with questions about this interview.

review technology can handle language-specific issues such as multi-byte characters (as in Chinese or Japanese characters).

Editor: How is technology helping the e-discovery process for multinational matters?

Earnshaw: You might say that technology is solving the problems it created, but that said, no doubt technology offers capabilities to solve the challenge of global e-discovery. And by capability I don't just mean a piece of software, but rather a combination of software, hardware and people with the appropriate experience to work in a mobile environment. Traditionally, e-discovery document review required that you collect the data from wherever it was residing and bring it back to a large data center for processing and hosting. The development of the right technology allows you to turn that process on its head: instead of taking the data to the data center, you take the data center to the data.

Conducting the review within the four walls of the corporation helps you comply with data privacy regulations, and it helps you with the cultural issues. It also assists with the softer points, specifically that employees can rest assured that their data isn't being collected and shipped off to a data center 3,000 miles away. Instead it's in the conference room down the hall, and only those documents that are relevant will be taken out of the country.

You can also then take it one stage further and actually apply advanced technology such as concept clustering, predictive coding and data analytics in the mobile document environment, thereby shortening the process, making it less intrusive and reducing the overall cost. Also on the rise is the utilization of managed review services, which can be employed just as easily in an in-country solution as in a domestic scenario, resulting again in lower costs.

Editor: What is the intersection between these data privacy concerns and the emerging awareness around information governance?

Earnshaw: On a macro level, because corporations are increasingly global, the regulatory investigations and litigation they are facing are likewise increasingly global. So these cross-border privacy matters are becoming much more commonplace. Forward-thinking corporations are looking at the jurisdictions where they operate, considering the potential risks they face and developing response plans accordingly. Some are storing and retaining their own data with a view to being able to respond to these types of cross-border investigations. Overall, they are trying to balance the requirements of investigations with local data privacy requirements.

Another key point centers on employee engagement and management and should not be underestimated. During the panel, Jennifer Hamilton noted that John Deere has a process of engagement with its employees to ensure that those who are data custodians are aware of what's happening in an investigation and why, giving them the ability to review documents before they are moved out of a particular jurisdiction and informing them of the protections their documents are being afforded when sent to international jurisdictions. The process recognizes the role of the employee as a custodian of the data in jurisdictions where there is a greater expectation of privacy and personal ownership of information.

Editor: Are you seeing an increase in e-discovery matters in Asia?

Earnshaw: Definitely. Certain issues arise with matters that are *within* the region, as well as cross-border and international matters that *involve* the region. In the former case, you must deal with recently enacted legislation with which many people are still coming to grips. You've also got significant concerns around the Chinese state's secrecy legislation, which significantly limits the information that can be taken outside of China. For example, recently Big Four firms conducting audits of Chinese subsidiaries on the part of their American parent companies have been banned from taking those audit working papers out of the country. Meanwhile, U.S. regulators have stated they need access to those working papers, causing a lot of tension.

We see in the region a significant increase in the requirements for in-country review. So within China, where you're dealing with a Chinese subsidiary of a U.S. company with documents that are resident in China, those documents are typically required to be reviewed in-country. This ensures that anything under consideration for taking out of the jurisdiction is responsive to the requirements of the litigation or the investigation, and also that the documents are appropriate under the confines of the Chinese state secrecy legislation. That piece of legislation gives many people a great deal of concern because the law is broad and somewhat vague, and there are potentially harsh penalties should you breach it. If you breach the data protection legislation in the UK, you're likely to receive a fine from the Information Commissioner's office. The panel discussed how if you breach Chinese state secrecy legislation, you could face jail. The stakes are therefore significantly higher and unfortunately the guidance is significantly less.

Pivoting to the technology, I've already referenced ensuring that your technology is capable of dealing with multi-byte languages. There are also language-specific word and sentence breaks within CJK (Chinese, Japanese and Korean) documents that require specific indexing and searching capabilities.

Editor: What about Latin American?

Earnshaw: The panel discussed how in the next five years, Latin America will probably be the hot region, as Asia is now. There's an increase in awareness of data privacy and a general movements towards development of data privacy legislation within the region.

We're now starting to see more businesses focus on the region – which means investigations and litigation will likely follow, which in turn means companies will need to address the handling of data in the region as well.

Editor: Can you share any recent examples of cases you've worked on and how technology and process ensured defensibility?

Earnshaw: Yes. Again, a key consideration is the ability to perform work in-country to ensure the defensibility of the process because you're at least complying with the data privacy requirements by not moving the material across borders. In many of the jurisdictions in Asia and especially Latin America, there are no e-discovery data centers, so having a mobile e-discovery capability is paramount.

We've recently been involved in a piece of U.S. litigation where data resident in China needed review. The review was performed not only within the country but, critically, completely *on the client's site* to comply with the client's own layers of security and data protection.

We also recently conducted an internal investigation in the French subsidiary of a U.S. corporation. Again, the data was collected, processed and reviewed and the investigative report was prepared in-country. Only the report was sent back to the U.S. parent company, solving any privacy challenges.

Editor: What are some of the best resources for legal teams hoping to learn more about this topic?

Earnshaw: First, I would say Working Group 6 of The Sedona Conference, which specifically focuses on international challenges associated with data privacy and protection in cross-border investigations and litigation. I would also guide people to The Article 29 Working Party, which publishes papers, reports and briefing notes about some of the challenges you face in relation to European data privacy.