ExecutiveCOUNSEL

THE MAGAZINE FOR THE GENERAL COUNSEL, CEO & CFO

When European Data Privacy Meets U.S. Discovery

Supreme Court Could Recalibrate IP Portfolios

Making Corporate Social Responsibility Systemic

CANADA /CROSS-BORDER

- *Canadian Corruption Laws*
- *Robust M&A*

INTELLECTUAL PROPERTY

THE STRANGE PHENOMENON OF "GENERICIDE"

GOVERNANCE

Federalization and D&O Exposure

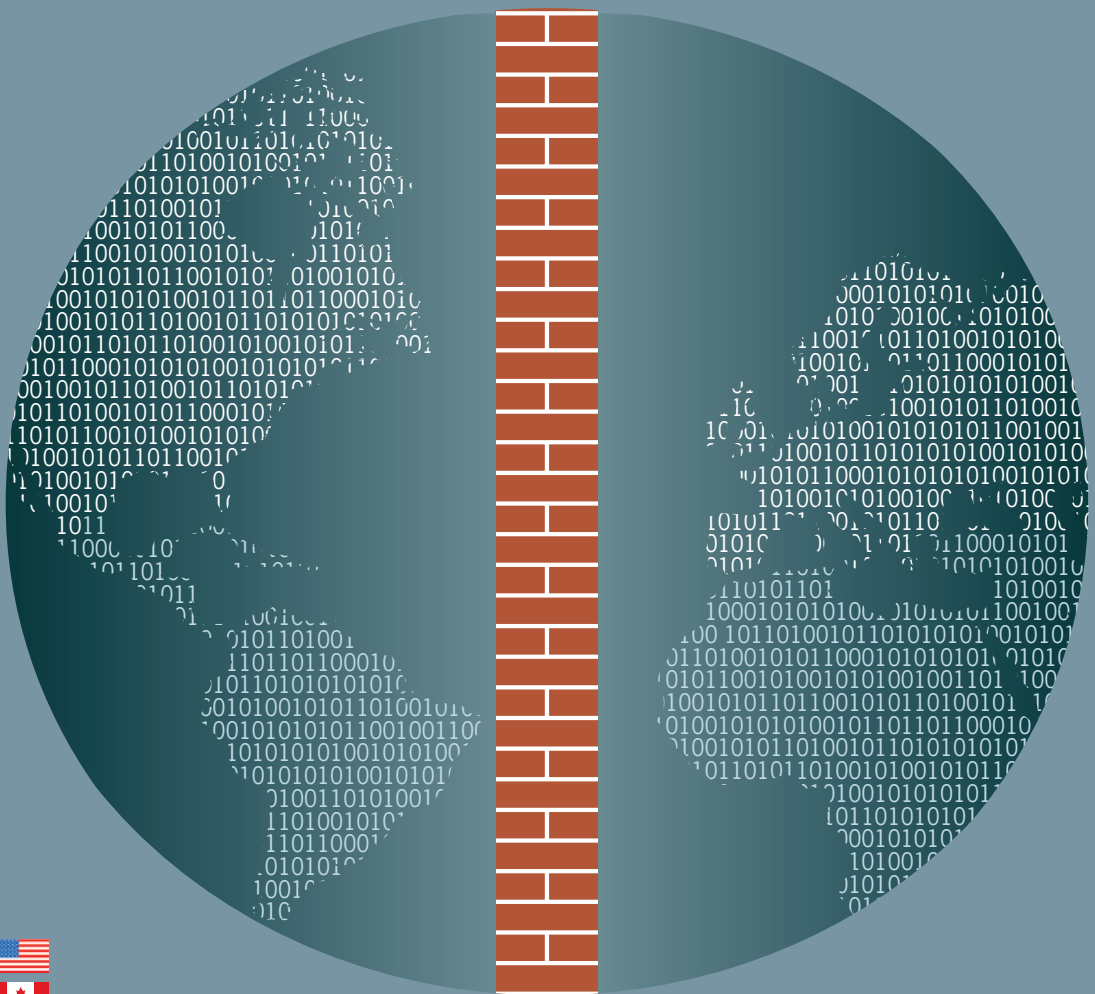
HUMAN RESOURCES

After the Facebook Firing

E-DISCOVERY

Outsource or In-House?

- THE EEOC'S CLASS ACTIONS
- KEY DNA PATENT CASE BEFORE THE FEDERAL CIRCUIT
- THE DODD-FRANK BOUNTY PROVISIONS
- IP PRIMER FOR ENERGY START-UPS



International Data Privacy and Mobile Electronic Discovery

By Craig Earnshaw

International privacy laws and restrictions on cross-border data mobility can make it difficult for lawyers to conduct electronic document searches and reviews outside the jurisdictions in which data resides. Advances in electronic discovery mean that mobile solutions can now take the technology to the data rather than the other way around.

Take a typical investigation into a potential violation of the U.S. Foreign Corrupt Practices Act (FCPA). A whistleblower's letter alleges that employees working for the Italian subsidiary of a U.S. publicly listed corporation are paying bribes to a local government official to win a lucrative infrastructure construction contract. To establish the substance of the claim, electronically stored information (ESI) contained within the email accounts of the implicated employees is investigated.

In the usual process, an electronic discovery service provider, working on behalf of the company's appointed law firm and typically based within the United States, conducts the investigation. In this instance, the firm sends an electronic evidence specialist to Italy to handle the forensic preservation of ESI from computers, email accounts and areas of the corporate network used by the Italian subsidiary employees. The ESI is collected on site, taken to a forensic laboratory or data center, whittled down and loaded into a review environment. Now the data can be searched, reviewed and flagged as evidence from any country in the world.

That approach is all well and good when the ESI resides in the same jurisdiction as the data center and the forensic specialist. But what if an organization is thought to be involved in a cartel, implicating multiple offices in other jurisdictions? And what if such actions breech European data protection laws and other legislation designed to protect personal information?

THE COST OF CONTRAVENTION

Organizations should tread very carefully. The costs of breeching data privacy rules in some jurisdictions can be significant and there has been an increase in the frequency of such cases.

In Europe, data protection authorities have levied multi-million dollar fines on corporations for failing to appropriately protect personal information. Remedies are not only financial. Breeches of the so-called "French Blocking Statue," which is designed to prevent the international transfer of documents, can result in jail sentences.

In the United States, during the first quarter of 2010, the Department of Justice and the Securities and Exchange Commission initiated or resolved 37 investigations into breeches of the Foreign Corrupt Practices Act, compared with just nine in the first quarter of 2009. Fines and penalties are rising too. Between 2002 and 2006, the average fine per incident was $5 million. This jumped to $45 million between 2007 and 2009.

Companies are subject to further risk by virtue of the fact that FCPA investigations by their very nature involve documents that reside in multiple international jurisdictions. Companies, therefore, must be very mindful of differences in data privacy laws, and ensure that they adapt their document collection and review procedures accordingly.

Other restrictions, such as banking secrecy or healthcare information protection legislation, can also complicate multinational litigation and investigations, by requiring that ESI be processed and reviewed within the jurisdiction in which it originally resides.

THE MOBILE SOLUTION

Given the complex challenges in moving data between jurisdictions, a technical solution that circumvents the need for data to cross borders can greatly facilitate multinational document review. By taking the technology to the documents rather than the documents to the technology, investigations can be undertaken rapidly and with minimal interruption to day-to-day business activities. Lawyers and investigators can review sifted and relevant documents as they are uncovered and in real time. The completion of high-pressure investigations in days rather than in weeks or months can be critical in regulatory and certain litigation scenarios.

Technical solutions developed by electronic evidence specialists for collecting, processing and reviewing documents on site range from installing servers at the company's data center or IT hub, to the use of discrete hand-luggage-sized mobile solutions that are configured in a conference room for the duration of the investigation.

These solutions are proving effective in multiple scenarios. Primarily, they enable investigations to be carried out in situ, without violating data privacy laws or other legislation. They support internal investigations, as well as facilitating discovery obligations in multinational litigation.

In addition, regulatory and cartel investigations by bodies such as the European Commission, the U.S. DOJ or the German Cartel Office, the transfer of non-relevant data to a data center in the UK or the United States for analysis may not be an option. In such instances, mobile solutions can save valuable time when a company is under pressure to locate documents to support a leniency application filing.

Mobile solutions are especially useful where discretion is crucial to avoid employees being alerted to an investigation inadvertently and where sensitive data needs to remain secure. By their very nature, mobile solutions are highly flexible and can be deployed on site at short notice, in client or counsel's offices or in a serviced office within the jurisdiction.

Just like the large data-center format, these solutions take ESI and perform operations to cull what could be millions of documents down to the ones that matter the most. This process facilitates the defensible preservation, culling and review of documents on site, using advanced technology to enable these key processes:

1. De-duplication. Reduces data sets by identifying and eliminating multiple instances of identical documents or emails so that a single copy is retained.

2. Near de-duplication. Identifies and removes all but the last message in a thread of emails.

3. Concept clustering. Brings together conceptually similar documents to enable faster review.

4. Keyword searching. Locates documents that include certain keywords or combinations of keywords. These can be combined with date ranges and specific senders or recipients of emails for more targeted identification.

5. Language identification: Identifies the languages in which a document is written to enable routing to the appropriate foreign-language speaking reviewer.

Mobile electronic discovery solutions are not silver bullets that purport to resolve all data protection issues. Rather, they can be an effective means of reducing data down to the most relevant documents for review.

Without portable electronic discovery technology, many investigations may come down to two simple choices where a corporation doesn't have the in-house capability to assist: to transfer all collected ESI out of a jurisdiction (and run the risk of contravening data protection laws) or to transfer none at all.

Mobile technologies sit between these extremes, enabling all materials that are not business documents or personal emails to be filtered out, for the remaining documents to be de-duplicated and searched for keywords and date ranges, and even fully reviewed within the four walls of the corporation in a foreign jurisdiction.

CRAIG EARNSHAW is a managing director in the FTI Technology segment. Based in London, he manages the Electronic Evidence Consulting, Document Analytics and Data Processing sub-segments within the UK. Since 1997, he has worked solely in the electronic evidence field, in areas such as forensic computing, electronic disclosure, internet investigations and electronic evidence. In 2006, he founded FTI's Technology Consulting segment in Europe.
craig.earnshaw@fticonsulting.com

Reprinted with permission from Executive Counsel, February/March 2011. On the Web at www.executivecounsel.info.