

“Flat World” Electronic Discovery: A Cyber-Tower of Babel?

KENNETH RASHBAUM, KEITH CASTO, STEPHEN WHETSTONE, AND
MICHAEL SIMON

The speed and convenience of electronic communication have, in the words of the author Thomas Friedman, flattened the business world. The proverbial “back office” or “branch office” may now be situated thousands of miles from corporate headquarters. Technological advances often entail technology headaches, and the need to preserve and produce electronic data for regulatory or litigation purposes, from disparate countries and cultures and in different languages can induce a technology migraine. This article outlines the “condition” and offers suggestions for analgesic solutions.

When the world starts to move from a primarily vertical value-creation model to an increasing horizontal creation model, it doesn't affect just how business gets done. It affects everything.

- Thomas L. Friedman, *The World is Flat*, p. 201

Of course, business does not always “get done” – sometimes it goes wrong – and that leads to litigation or governmental investigatory proceedings. Those actions increasingly involve records spread about many countries, which must be identified, preserved, gathered, reviewed, and turned over to government agencies and corporate adversaries. And because nearly 99 percent of all documents created by

Kenneth Rashbaum and Keith Casto are attorneys with Sedgwick Detert, Moran & Arnold, LLP. Stephen Whetstone and Michael Simon are with Stratify, Inc. The authors would like to acknowledge the assistance of Michael Goff of Stratify and Amy Chung of Sedgwick in connection with the preparation of this article.

businesses today exist in electronic form, litigation discovery requests are often more concerned with seeking data than paper copies. And as the outsourcing of U.S. jobs has led to the creation of offshore databases and data warehouses, much of the data sought is not written in English or even familiar “Latin” character sets.

While the outsourcing of jobs and data has significantly decreased ordinary business costs, it has given rise to serious new legal, cultural, and technical challenges. Even if data is not shared outside of a corporate enterprise, foreign local laws will have something to say about the *internal* transfer of data from abroad to the U.S. While the American legal system treats most information created, stored, or sent via corporate computers as the exclusive property of that company, much of the world thinks otherwise. For example, because human resource files typically contain a plethora of personal information they often are afforded special protection under many local privacy laws and the European Union’s data privacy provisions.

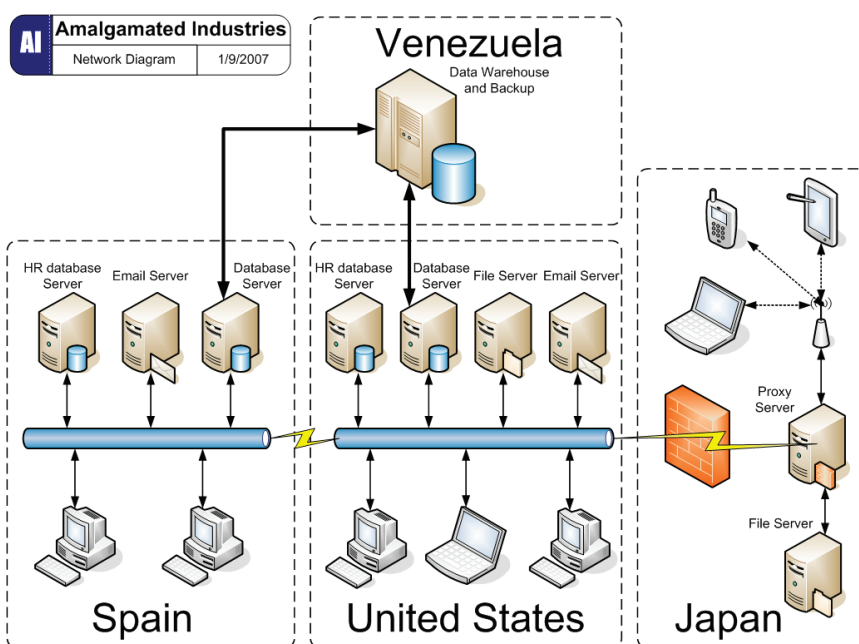
In contrast, the recent amendments to the U.S. Federal Rules of Civil Procedure put added pressure on U.S. companies to preserve and produce relevant data wherever it may reside. Similarly, U.S. government agencies usually have little tolerance for U.S. companies refusing to turn over data because of foreign privacy laws. Yet, unknowing breaches of local rules and regulations in pursuit of satisfying U.S. discovery or regulatory requests can lead to severe penalties, and even jail time. Ignorance of the law, whether in the U.S. or in some far-flung foreign land, is no excuse.

IT CAN HAPPEN TO YOU

Using French-made airplane design software, the Russian engineers collaborate with their colleagues at Boeing America – in both Seattle and Wichita, Kansas – in computer-aided airplane designs.
- Friedman, *The World is Flat*, p. 195

The following scenario demonstrates just how “flat” the corpo-

rate world has become. "Amalgamated Industries, Inc." is a fictitious Fortune 100 global corporation with corporate headquarters in the U.S. Amalgamated also has facilities in Tokyo and Madrid. Some of the data processing and hosting is done in Venezuela.



Amalgamated has a basic document management and retention policy. But, like many companies, compliance with these policies in its U.S. offices is far from perfect, and it is even more wanting in the satellite offices. Also like many other companies, Amalgamated does not have an established litigation preparedness policy or protocols; document preservation and collection occurs only on an *ad hoc* basis in response to a specific, perceived litigation threat.

The U.S. Department of Justice has just informed Amalgamated that

it is the subject of a formal investigation as a result of certain alleged conduct in its American, Japanese and Spanish offices. The preservation and collection of electronic files across the corporate enterprise for this investigation should be done with an eye toward the new FRCP requirements so that the efforts will withstand scrutiny in any eventual litigation filed in federal court. Thus, Amalgamated and its counsel need to take the right actions at the right time because they may get just one chance to prepare the right way for electronic discovery.

CROSS-BORDER LEGAL ISSUES

Every morning in Africa a gazelle wakes up.
It knows it must run faster than the fastest lion or be killed.
Every morning a lion wakes up.
It knows it must outrun the slowest gazelle or it will starve to death.
It doesn't matter whether you are a lion or a gazelle.
When the sun comes up, you better start running.
- Friedman, *The World Is Flat*, p. 114 (quoting African proverb)

To stay alive in the ever-flatter world of international business, Amalgamated, like the gazelle and the lion, must know the international and legal landscape in which it must run to survive.

Production of data from Spain poses two significant obstacles: European Union Privacy Directives and Spanish privacy law. E.U. Directives 95/46/EC and 97/66 EC set forth the principle that personal data (data which identifies or concerns a named individual) cannot be transmitted outside the European Economic Area (the E.U. nations plus Iceland, Norway and Lichtenstein) to a country which does not provide, by national law, protection commensurate with the E.U. At present, the only non-E.U. countries which meet this standard are Canada and Argentina. Of course e-mail, the most desired of all electronic evidence, almost always contains the name and location of the author, and thus

qualifies as "personal data."

There are exceptions to this provision of the Directives, however. Data may be exported with the consent of the data subject (difficult to obtain and, in any event, certain countries consider consent sought by an employer to be *per se* involuntary), or an order of the court in which the data reside. In addition, personal data may be exported from the E.U. if the importing corporation has a Data Protection Agreement in place. This Agreement can take any of three forms: one which utilizes model contract clauses (which have been approved by all E.U. nations), a Safe Harbor agreement filed with the U.S. Department of Commerce, or a set of Binding Corporate rules. Each format requires that Amalgamated certify that its policies and practices protect personal data to the same extent as in the E.U.

Outside counsel for Amalgamated should undertake, as its first task, to ascertain whether the company has such an agreement in place. Amalgamated's data is routinely transferred to the United States for business purposes, and thus one would hope that the company's in-house counsel saw to it that the agreement was in place and current (the Safe Harbor Agreement requires re-certification to the Department of Commerce annually).

The inquiry does not end with the E.U. Privacy Directives, however. Each E.U. member nation must implement the Directives by enabling legislation, and these statutes and regulations are often more exacting than the Directives themselves. In Spain, the enabling legislation, Organic Law 15/1999, defines personal data as "any information relating to an identified or identifiable natural person," and reiterates the provisions of the E.U. Directives. In addition, there are other provisions of Spanish law which restrict the use and disclosure of personal data by such means as requiring warrants or court orders to search an individual's computer without the individual's consent.

Japan poses a different and highly complex challenge. Its Personal Information Protection Act ("PIPA") also defines "personal data" broadly, comprising: name, date of birth, or other description which, when

easily compared with other individuals, can identify specific individuals.” Data may be shared with third parties on a consent, or “opt-out” basis, pursuant to Article 23, paragraph 2, but only if the individual is provided with notice of the purpose of use of the data, the contents of the data, and that the provision of the data will cease upon the request of the individual (a principle, as we shall see below, that is followed in certain Latin American countries).

In Japan, delegation, or outsourcing of data processing services is permissible and service vendors may transfer data without consent, so long as they enter into an agreement with the data importer to protect the data. There are strict guidelines for such agreements, and it is worth noting, with some alarm, that eleven different ministries share responsibility for administering PIPA. Violations of PIPA may result in a fine of up to 300,000 yen (approximately \$2,500) or imprisonment for up to six months.

As if this cyber-Tower of Babel were not perplexing enough, more compliance headaches await Amalgamated when it crosses the Pacific Ocean from Japan to Venezuela. The principle of “Habeas Data” is followed in Venezuela; that is, the individual may ask that the data on himself or herself be produced. Article 28 of the 1999 Constitution states that “any person has the right to access the information or data over himself. . . as well as learn of its use and purpose and to request. . . its update, correction or destruction if erroneous or were to illegitimately affect their rights,” subject to certain exceptions.

Clearly, Venezuelan laws place severe restrictions on access to and disclosure of data. Violations of these provisions and other privacy laws, including use or disclosure of personal data without consent are punishable by fines and imprisonment. To illustrate, *Petroleos de Venezuela, S.A.*, the national oil agency that dominates Venezuela’s oil production and is the fifth-largest oil producer in the world, in the matter of *Lyondell-Citgo Refining, P.P. v. Petroleos de Venezuela, S.A.*, endured an adverse inference instruction at trial rather than disclose its board of directors minutes and related documents and risk running afoul of Venezuela’s Special Law Against Information Systems Crimes.

TECHNICAL AND PRACTICAL ISSUES

You can flourish in this flat world, but it does take the right imagination and the right motivation.

- Friedman, *The World is Flat*, p. 469

All electronic discovery work shares common attributes, regardless of the country, culture, or language in which the work is done. For example, in every electronic discovery project, someone must locate and collect documents from various storage media, such as laptops, desktops, central servers, backup tapes and system archives. Before collection can even begin, someone must carefully consider the scope of the document request, map the company network, and identify pertinent programs and key custodians.

But there are also key differences between data preservation and collection efforts in the U.S. and abroad. The scope of permissible discovery in the U.S. is very broad. By contrast, in most foreign jurisdictions there is far less discovery of information prior to trial or hearing. As a result, foreign businesses, as a rule, are not as accustomed to or driven by discovery concerns.

In addition, the practical challenges of gathering data that resides thousands of miles away from U.S. offices can be daunting. Much has been made of the recent failures of Phillip Morris, Merrill Lynch, Unum Provident, and dozens of other leading U.S. companies to preserve and produce relevant data located entirely within the U.S. in response to government investigations and private litigation. The decisions in such matters can read like a "Keystone Cops" script: Outside counsel, in-house lawyers, IT teams and vendors all scramble about and trip over one another while the target of the pursuit (in this story, the data) slips through their fingers. The plot, however, can become much thicker when the target data is spread about in multiple offices in multiple countries and in multiple languages.

Even if the local privacy laws are understood and a foolproof game plan has been put in place for gathering data, unanticipated technical challenges can still botch the effort. Local settings, such as the foreign

language page settings on computers, should be noted and preserved so that the alpha characters can be accurately captured and displayed. Extraction tools and container files (such as .pst files for Microsoft Outlook email) must match up with the foreign language programs – U.S. tools and container file programs often cannot capture all foreign data. Data collection teams should map the types of computer systems and programs at issue prior to their departure from the U.S. so they arrive with the right tools in hand.

Documents collected in Amalgamated's Madrid offices likely will contain large volumes of Spanish and English. Amalgamated therefore will need translators - or some type of machine translation software backed by human translators – to make sense of its collection. Evidentiary documents will need certified translations, which take even more time and are far more costly. In addition, although Spanish, like English, uses the Latin-A character set, some characters are unique to Spanish, such as “~” and “¿.” Unless properly trained, American reviewers may overlook these unique characters or fail to use the proper keyboard or keyboard emulation software required to capture them.

Also, Amalgamated's management team in Madrid may be less concerned about U.S. legal deadlines than their American peers and, thus, less diligent in collecting the necessary documents. There also may be particular technical issues associated with gathering the Spanish data. European businesses increasingly are turning to open source systems, including Linux, to avoid the costs, security problems, and potential privacy issues associated with commercial software. Ironically, Microsoft itself was fined the equivalent of \$60,000 by Spanish data protection authorities in 1999 for transferring personal data of Spanish consumers to the U.S. without proper disclosures. Thus, Amalgamated's data collectors will need to be on the look out for these open source documents, as the standard approaches for capturing Microsoft documents, particularly Outlook email, will miss them.

To a degree that is hard to comprehend in the U.S., honor, social hierarchy, and avoiding offense are powerful factors in the Japanese workplace. Thus, Amalgamated may need to handle its Tokyo collection

with greater discretion and adopt procedures that rely on the goodwill and direct efforts of the data custodians and other non-legal personnel. If foreign data collectors are not involved, Amalgamated's attorneys must clearly communicate the types of documents sought and work hard to ensure that the field level personnel are properly trained to preserve and collect them. U.S. regulatory agencies and courts will not excuse a rigorous data collection merely to facilitate Amalgamated's deferential treatment of its Japanese personnel.

Amalgamated will also need to deal with some technical issues peculiar to Japanese language. Japanese written language uses three different, intimately connected, character sets, all of which can co-exist within a single document. Unless Amalgamated is careful and accounts for this "triple encoding" during its collection efforts it could wind up with documents that do not display all character sets. In addition, because most Japanese characters are "double-byte" – that is one character inhabits two bytes of space within a document -- Amalgamated can lose basic, but critical metadata, such as file names, unless certain prophylactic steps are taken during collection. Even if the data is properly captured and processed, Amalgamated and its attorneys need to consider that the Japanese language typically has word breaks only at the start and end of a sentence, which affects search and machine translation.

As in Spain, documents collected by Amalgamated in Venezuela likely will contain both Spanish and English. Still, Amalgamated cannot blindly rely upon the same translators or techniques for making sense out of both data sets. Different Spanish cultures have different idioms, phrases and, on occasion, even different words, to describe the same object or concept. For example, in Madrid, a computer is referred to as an "ordenador," while in Caracas it is called a "computadora." Amalgamated's translators and translation software will need to understand these subtle culture differences and adjust their efforts accordingly.

Amalgamated may face even further technical challenges in Venezuela. Latin American countries are also embracing open source technologies to avoid rising commercial software costs – far more so than in the U.S. or even Europe. Venezuela, with its increasing anti-capitalist rhetoric is lead-

ing this movement. Pursuant to a recent presidential decree, Venezuela's government and public entities have two years from January 2006 to convert fully to open source software systems. While this decree does not directly affect private businesses, Venezuela is nationalizing many of its major industries, including the oil and gas, electric, and telecommunications industries. As many of Venezuela's major industries convert to open source, many other private businesses may follow suit. Local self-reliance is an overriding theme of this nationalization movement, and so Venezuela's open source scheme may soon differ from other such systems around the world. As a result, if the U.S. investigation extends out over a period of time, Amalgamated may need to hire local consultants familiar with these technological structural shifts to help ensure that all of its data is correctly preserved and collected.

Getting the job done right and on time in just one of these countries would be a formidable challenge. But, coordinating Amalgamated's combined efforts requires steady and experienced legal and technical hands to ensure that the disparate and competing local requirements are harmonized with the demands of U.S. law.

CONCLUSION

Every day the world grows flatter, as companies and their information systems flow across blurred transnational boundaries. In the wake of the recent federal rules changes and more rigorous U.S. government pursuit of electronic data, companies, and their legal counsel can no longer risk hiding behind these fading boundary lines or their own technical deficiencies. Rather, they must confront head-on the various legal, cultural and technical changes and challenges so they can capture and preserve all pertinent electronic data, wherever it may reside.