

## North v. South: A Look at Data Discovery and Privacy Conflicts Between the U.S. and South America

By Kenneth N. Rashbaum, Esq

The globalization of commerce is increasing at an accelerating rate. With trade, of course, comes trade disputes, and complicating these already intricate matters are conflicts in the dissemination of business data for use in litigation in the United States. This trend in the European Union, has been the subject of numerous trade journal articles and law review analyses, and has been discussed for hours on end at seminars and legal organization conferences. South America, though, has privacy and data protection laws that rival those of Europe. South American businesses continue to expand their footprints in the United States. Consider the proliferation of regional jets in recent years, a great percentage of them manufactured by Embraer, a Brazilian corporation. As these companies find themselves enmeshed in U.S. litigation and regulatory proceedings, data disclosure conflicts between those countries and the United States will become as nettlesome and vexatious to American litigants and courts as those involving countries in Europe.

There are similarities in the stringency of personal information protection between the member states of the European Union and certain South American nations. "Personal Information," in the European Union is, put simply, information that may be traced to an identifiable Individual. It may not be sent outside the European Economic Area (the 27 member states plus Norway, Iceland and Liechtenstein) to a country with lesser data protection, without consent. (See, *Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data.*)

As more businesses expand globally more business information will be found outside the U.S., and litigation discovery demands and court orders will conflict with local privacy regulations, leaving the client to ask, "In which country should I risk jail — my own, if I provide the information and violate privacy laws, or the U.S. if I fail to comply with the judge's Order?"

The definition of "Personal Information" includes company emails, as they bear the names of the sender, the recipient and, frequently, individuals who are the subject of the communication. Yet, other company documents may fall within this category of protected information as well. In *Lyondell Refining v. Petroleos de Venezuela S.A.* (2005 U.S. Dist. LEXIS 6533 (S.D.N.Y., Apr. 18, 2005)) the defendant, faced with a court order to produce minutes of the Board of Directors, declined to produce the document because doing so would subject it to criminal liability. Venezuela's Special Law Against Information Systems Crimes prohibited the disclosure of "personal information," and the corporate minutes, identifying directors by name and placing them at a defined location on a certain date, fell into Venezuela's definition of that term. Facing potential adverse judgment, the defendant accepted the sanction of an Adverse Inference jury instruction, in which the jury was advised that they may presume that the document, if produced, would be adverse to the positions the defendant was propounding at trial.

Of course, one cannot generalize about privacy and data protection in a continent from one country's laws and one U.S. lawsuit. Accordingly, this article will discuss privacy protections in three countries, Brazil, Chile and Argentina, to provide an overview of U.S. data disclosure conflicts between the U.S. and South America, and how they may impact trial preparation

This article appeared originally in the Spring 2010 *ALSP Update*, the publication of the Association of Litigation Support Professionals and is reprinted with permission. Read more about this nonprofit membership organization at [www.alsponline.org](http://www.alsponline.org).

involving electronic evidence from those jurisdictions. Certainly, one would be advised to seek local counsel with regard to the implications of the privacy and data protection laws prior to transferring data to the U.S., as well as U.S. counsel experienced in litigating these matters and explaining data discovery conflicts to judges (and, before that, to adversary counsel in an effort to avoid motion practice).

### **Brazil**

Brazil's form of data protection is known as "Habeas Data," and it is enshrined in its Constitution (Article 5, LXII (a) and (b)). In this manifestation of data protection, the data subject possesses the ability to exercise some degree of control over his or her personal data. An individual may, upon request, access data on himself or herself contained in government or private databases and request that it be amended, corrected or deleted. Brazil's Consumer Code (Law 8,078/90) extends this right to those whose personal data may be stored in consumer databases. "Personal Data" is defined broadly, similar to the European Union Privacy Directives.

The effect of Habeas Data upon foreign discovery requests is not directly clear, yet the constitutional mandate cannot be ignored when consideration is given to foreign judicial requests. Brazil, contrary to E.U. member states, has no central data protection authority. Brazil is not a signatory to the Hague Convention on the Taking of Evidence Abroad, which sets out procedures for obtaining documentary evidence by Letters Rogatory (letters of request) submitted by a foreign court to judicial authorities in the country from which the data is sought. In the absence of such procedures, Letters Rogatory submitted to a Brazilian court can take as long as six months to two years to process. American courts, which take quite seriously the mandate of Rule 1 of the Federal Rules of Civil Procedure that the Rules be construed to "secure the just, *speedy* and *inexpensive*" (emphasis supplied) resolution of the case, may be disinclined to follow the requirements of Brazilian law, and may insist upon production of the data in Brazil regardless of the consequences to Brazilian parties.

The Brazilian Civil Code, Sections 186, 927, 1521 and 1522 provide civil remedies for those damaged by improper dissemination of their personal data. These provisions also hold that personal data cannot be used

for a purpose beyond which it was obtained and/or processed, without the consent of the data subject. It may, though, be impractical to obtain the consent of hundreds or thousands of employees whose emails are sought, for example, in a U.S. products liability case. For this reason, counsel may advise the corporation to obtain consent for transfer of emails and other personal data outside Brazil proactively, i.e., as part of the employment contract.

### **Chile**

Privacy laws in Chile begin with its Constitution. Article 19 of the Chilean constitution provides protection for the private and public life and honor of the individual and his family. All forms of private communication are included in this category and can only be made available to others in ways prescribed by law. This principle finds legislative implementation with regard to data privacy issues in the Law for the Protection of Private Life (Law 19,628, 1999), which was enacted in October 1999 and amended in 2002. The statute protects the personal data of individuals, in addition to commercial, financial, banking, and criminal history information.

The Chilean law is not as restrictive as privacy laws in the European Union or Argentina, but it does provide several obstacles for companies in the United States that wish to collaborate with local Chilean corporations or that find themselves in the midst of litigation in U.S. courts. The law applies to both "personal" and "sensitive" data. Personal data is that which contains identifiable information about the individual. E-mails that contain many of these identifying characteristics, such as the names and/or e-mail addresses of the sender and Chilean recipient, are covered by this definition. Sensitive data refers to personal data containing more intimate details about the individual, such as personal habits, ideologies and political opinions and physical or mental health, among other things. This means that a U.S. company would require data protection protocols tailored to these provisions in its collaboration with a local corporation, or even with its own local office or subsidiary.

The Law for the Protection of Private Life specifies certain requirements that must be met before personal data may be collected or transmitted. Personal data may be collected when authorized by law or by the subject of the data (consent of the data subject). The collector of the data (e.g. a U.S. company trying to

collect e-mail correspondence between employees at its local Chilean counterpart) must receive authorization in writing. The authorization can be revoked at any point, though revocation does not apply retroactively. The collector must also notify the data subject of whether or not the information will be shared with a third party.

This has clear implications for data demanded in U.S. litigation or regulatory proceedings. Where a third party requests information, it must identify itself, state the reason and purpose for the request, and specify the type of data it wishes to transmit. Once the third party receives approval to receive the data, it cannot use it for any purpose other than the one it specified. However, unlike the European Union and Argentina, Chile does not have a central data protection authority, and all enforcement occurs on the judicial level (that is, when the data subject complains about the export of his or her data).

Article 16 of the statute sets forth provisions similar to Habeas Data: the data subjects may access their personal information, and may request modification, correction, or deletion. Significantly, Title I states that personal data is to be deleted when it is no longer required for its purpose. This means that data needed for US. Litigation may no longer be extant when demanded. Given the emphasis US. Courts place on preservation of data, and the importance of implementation of Legal Hold when litigation is reasonably anticipated (See, *Pension Committee of the University of Montreal v. Banc of America Securities, LLC*, No. 05 Civ. 9016 (SAS) January 11, 2010 (S.D.N.Y.)), it may well be necessary to obtain local counsel and U.S. counsel to prepare Certifications to the U.S. court as to why certain data could not be preserved in Chile (See also, *Adams v. Dell*, 621 F.Supp. 2d 1173 (D. Utah 2009) in which the court considered spoliation sanctions against a Taiwanese defendant whose retention practice did not require long-term preservation).

### **Argentina**

Argentina's privacy and data protection schemes are so stringent that the country is considered by the European Union as one of only four nations to have privacy protection commensurate with that of the E.U. (the other three are Switzerland, Canada and, as of February 2010, Israel).

As in Chile and Brazil, the right to privacy of personal data is enshrined in the Constitution. Articles 18 and 43 set up the right to data privacy by requiring protection for correspondence and private papers, to be determined by law. Article 43's Habeas Data principle requires that information about an individual to be available to that individual upon request. Argentina has specific legislation that implements data privacy, the Law for the Protection of Personal Data. This law was enacted in 2000 (Law n.25,326), and regulations for implementation were promulgated in 2001 (Decree 1,558/2001).

The Law for the Protection of Personal Data is modeled upon the European Union Privacy Directives. It requires express consent for use of personal data. Of great significance for the issue of transfer of data needed in litigation to the U.S., Argentina's statute prohibits the export of personal data (defined in a similar fashion as the E.U. Directives) to a country with lesser data protection — such as the U.S. The statute provides exceptions, including transfers where a data transfer agreement may provide a level of protection equivalent to that in Argentina. Such an agreement is certainly advisable for U.S. enterprises with facilities in Argentina.

Following the European model, Argentina has a central data protection authority, the National Data Protection Commissioner, which is charged with enforcement of the privacy and data protection provisions. It should come as little surprise, then, that U.S. corporations seeking email and other electronic evidence which falls under the rubric of "personal data" would face complications similar to those one would encounter in seeking such data from the E.U.

### **Conclusion**

The proliferation of electronic business communication and, with it, the emphasis placed on those communications in business collaboration and litigation, require documented policies and procedures to assure that the transmission of this data — much of it "personal" — complies with local law in South America. In the area of daily business conduct, this requires the assistance of local counsel well-versed in local data protection expert practices, as well as U.S. counsel working with corporation to institute required levels of data protection in the U.S. Similarly, when email and other "personal data" is demanded in litigation, it is

advisable to form a four-pronged working group: in-house counsel, IT/Records personnel, local counsel in the country from which the data is sought, and U.S. counsel experienced in litigating matters involving data discovery conflicts. U.S. litigants and their counsel are often unaware that just “getting the data off the server from here (the U.S.)” can have severe, often criminal, consequences. U.S. judges, similarly, may never have had issues of data production or preservation in South America in their courts. Awareness of the discovery conflict issues described above can go a long way toward assisting the client faced with requirements for data when she asks, “In which country should I risk a jail sentence?”

*Kenneth N. Rashbaum, Esq., is principal of Rashbaum Associates, LLC, in New York ([www.rashbaumassociates.com](http://www.rashbaumassociates.com)). Rashbaum’s practice focuses upon counsel to multinational corporations and others facing the challenges of information governance in an increasingly regulated global environment. He is a member of The Sedona Conference and the American Bar Association’s International Law Section. A frequent speaker and writer in the area of cross-border data disclosure conflicts, Rashbaum is co-editor-in-chief of the The Sedona Conference Framework for Analysis of Cross-Border data Discovery Conflicts. Rimma Bukhbinder, a law student at Brooklyn Law School, J.D. expected May 2011, assisted in the research for and preparation of this article.*