BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

It unclear if emerging data protection law in Latin America will be more influenced by the Asia-Pacific Economic Cooperation privacy framework or the European Union system, writes Peggy Eisenhauer, founder of Privacy & Information Management Services. But it is critical for companies operating in the region to monitor developments, as data protection continues to develop and expand.

Developments in Latin America Privacy Laws

BY MARGARET P. EISENHAUER

Multinational companies historically focused their privacy law compliance resources in the United States and Europe. Today, however, companies are forced to view privacy compliance as a truly global commitment. Not only are data protection regimes mushrooming across Asia, Latin America, and even Africa, but many new regimes impose the same types of onerous process-intensive restrictions found in Europe.

Peggy Eisenhauer, founder of Privacy & Information Management Services–Margaret P. Eisenhauer, P.C., helps companies develop, implement, and assess privacy programs that comply with United States and international laws. She is a Fellow of the Ponemon Institute, a Certified Information Privacy Professional (CIPP) and a member of the International Association of Privacy Professionals CIPP Advisory Board. Eisenhauer is admitted to practice law in Georgia and Florida. She can be reached via e-mail at peggy@privacystudio.com or via telephone at (404) 914-1163.

In Latin America, modern privacy rights have developed from the concept of "*habeas data*." *Habeas data* articulates the fundamental human right that individuals have to know what information is archived about them by government and, in some cases, commercial entities. The doctrine varies across Latin America, but generally is designed to protect the image, privacy, honor, information, self-determination and freedom of the individuals.

Habeas data rights are being supplemented with statutory rights in traditional data protection legislation in some Latin America jurisdictions. Other countries provide for *habeas data* rights in sectoral laws (regulating credit reporting, for example) or in consumer protection laws.

The Habeas Data Foundation

While the origins of *habeas data* rights are unclear, some trace their origin to discussions of European constitutional scholars in the 1980s that suggested that freedom and self-determination required control of one's identity, much as they required freedom of the

physical person under the traditional *habeas corpus* writs.[1] The phrase ''*habeas data*'' first appears in law in the Brazilian Constitution in 1988.[2] These rights now appear in most national constitutions in the region.

At their core, *habeas data* rights provide individuals with the ability to ''have the data'' about themselves. This translates into individual rights to compel organizations to provide access to personal information. These access rights generally are complemented by rights to mandate correction of inaccurate data and to the limit distribution (or mandate destruction) of the data. *Habeas data* rights can apply both to consumer and employee data files.

Habeas data rights do not generally imply other types of data protection restrictions. For example, *habeas data* does not require any specific restrictions on the international transfer of personal information. Instead, organizations subject to these rules would likely be required to provide access and respect the other *habeas data* rights without regard to physical location of the information.

Chile's data protection regime embodies the prototypical *habeas data*-based approach to privacy. Chile's constitutional privacy rights were supplemented in 1999 by a comprehensive data protection law, the ''Law for the Protection of Private Life.''[3] This law regulates the processing and use of personal information in the public and the private sectors, including human resources data.

Building on its *habeas data* roots, the Law for the Protection of Private Life establishes broad rights to access and correct information in electronic and paper databases. The Law regulates the processing of personal data in general and establishes the rights of data subjects and favors consent as the basis for most data processing. It contains specifics regulating the processing of credit and financial information, medical information, and data processing by public agencies.

Although the Chilean law is very comprehensive in scope, international transfers of personal data are not restricted. Additionally, the law does not establish an independent data protection authority. Privacy rights are enforced by the individuals themselves in Chilean courts, via a private right of action. These are not requirements that naturally stem from the *habeas data* model.

[1] See, *e.g.*, *Habeas Data: The Latin-American Response to Data Protection*, Andres Guadamuz, The Journal of Information, Law and Technology (JILT) (2000-1).

[2] See, *e.g.*, Brazilian Constitution, Title 2, Chapter 1, Article 5 (1988): ''All persons are equal before the law, without any distinction whatsoever, Brazilians and foreigners residing in the country being ensured of inviolability of the right to life, to liberty, to equality, to security and to property, on the following terms: X-the privacy, private life, honour and image of persons are inviolable, and the right to compensation for property or moral damages resulting from their violation is ensured; XIV-access to information is ensured to everyone and the confidentiality of the source shall be safeguarded, whenever necessary to the professional activity; LXXII-*habeas data* shall be granted: a) to ensure the knowledge of information related to the person of the petitioner, contained in records or data banks of government agencies or of agencies of a public character; b) for the correction of data, when the petitioner does not prefer to do so through a confidential process, either judicial or administrative; [*et. seq.*].

[3] Ley Sobre Protección de la Vida Privada, Law No.19628 of August 30, 1999.

The Iberoamerican Data Protection Network

In the late 1990s, European scholars began to exert influence over data protection developments in Latin America. In particular, the Spanish data protection authority initiated outreach efforts to advance EU-style concepts across the Spanish-speaking countries in the region. These efforts led directly to the passage of the Argentine data protection law in 2000 and the creation of a formal Iberoamerican Data Protection Network (IDPN) in 2003.[4]

Founded by the Spanish data protection authority, the IDPN offers an advisory forum for national data protection efforts in Latin America. The Director of the Spanish Data Protection Agency, José Luis Piñar Mañas, serves as President of the IDPN as well as vice-chairmen of the Article 29 Working Party.

The IDPN offers model data protection legislation (based on the Spanish law) as well as policy advice and debate resources, all in Spanish. By bringing EU-style concepts to the region, the group hopes to ensure that trade between Europe and Latin American countries is not disrupted by the lack of adequate protection for personal information in the region.

The IDPN has successfully encouraged many Latin American countries (including Mexico) to consider EU-style laws. Political and economic forces have generally prevented these bills from advancing, but the IDPN attracted over 200 delegates to its annual conference last fall, and it is expected to continue to try to influence legislation in the region.

Argentina's experience with a true EU-style law is being closely watched. As noted above, Argentina supplemented its constitutional guarantee of *habeas data* rights with a comprehensive data protection law[5] in 2000. This law generally mirrors the data protection law in Spain, establishing EU-style rights for data subjects and obligations for data controllers.

The Argentine law created an independent data protection authority, the National Directorate for the Protection of Personal Data (NDPPD). The NDPPD is developing EU-style process requirements and enforcement protocols as well. For example, mandatory database registration was ordered last year, with the initial registration phase ending this past March 31.[6]

All databases in Argentina (other than those for purely personal purposes) must now be registered with the NDPPD. New databases must be registered before they are implemented. This requirement extends to both computerized and paper-based repositories of personal information. Significant fines can be imposed on companies that fail to comply with the registration decree.

The registration requirement has proven to be very resource-intensive for both the NDPPD and companies faced with registration. (The registration deadline had to be extended to allow companies to complete the process.) It is unclear if the costs associated with the registration process will provide citizens with a corresponding increase in their ability to exercise their rights. Given the breadth of the registration initiative, it is also

[4] For more information, see https://www.agpd.es/ (in Spanish, with limited English resources).

[5] National Act 25,326

[6] For more information about the database registration requirements, see http://www2.jus.gov.ar/dnpdp/ (in Spanish only).

  PVLR ISSN 1538-3423

unclear if the process will enable the NDPPD to better enforce the substantive provisions of the law to the benefit of the people.

With regard to substantive requirements, the Argentine law imposes strict limits on data collection and use. As with its EU-model, consent is generally necessary (although not always sufficient, if the processing is otherwise unfair) to collect, use and transfer personal information. The law also includes additional restrictions for sensitive data.

The Argentine law prohibits international transfers of personal information unless the recipient is in a country that offers adequate protection (as determined by the NDPPD), the data subject has consented to the transfer, or another exception exists. To date, the NDPPD has not made any adequacy findings, although in practice companies are using EU-approved data transfer mechanisms, such as the model contracts.

An Alternative Model: the APEC Privacy Framework

Partly in response to the proliferation of EU-style data protection laws, the Asia-Pacific Economic Cooperation (APEC) undertook a process to develop a privacy regulatory framework that protected individual rights without the economic-dampening effects of EU-style legislation.

APEC is a multinational organization with 21 Pacific-coast members in Asia and the Americas, including the United States and Canada, Chile, Mexico, and Peru.[7] The word ''economies'' is used to describe APEC members because the APEC cooperative process is predominantly concerned with trade and economic issues, with members engaging with one another as economic entities.

In February 2003, the APEC Data Privacy Subgroup was established under the auspices of the Electronic Commerce Steering Group with the mandate to develop an APEC Privacy Framework. The Privacy Framework was finalized in November 2004.[8]

The Privacy Framework is designed to provide a vehicle to support member economy legislation on privacy that can both protect individual interests and ensure the economic development of the member countries. The APEC economies are now developing implementation materials and other guidance to countries wishing to adopt privacy legislation based on the Framework.

The Privacy Framework consists of nine Information Privacy Principles, along with a preamble, definitions, a facing-page commentary, and implementation guidance. The Principles consist of: (1) Preventing Harm, (2) Notice, (3) Collection Limitation, (4) Uses of Personal Information, (5) Choice, (6) Integrity of Personal Information, (7) Security Safeguards, (9) Access and Correction, and (9) Accountability.

With regard to international transfers, the APEC Principles explicitly recognize the necessity of appropriate processing and transfer of personal information within a privacy-protective environment. The Framework notes that robust data flows are needed to support 21st century global business and e-commerce, and strives toward the dual goals of promoting and enforcing privacy rights while maintaining the continuity of information flows among the APEC economies and their trading partners.

Mexico is currently considering legislation based on the APEC approach. It is unclear if this law will be enacted prior to the July elections, but if it is, it will likely serve as a model for the region. An APEC-based Mexican law would stand as welcome contrast to the Argentine regime.

Anticipated Trends

There is no question that privacy regulation will continue to bloom in Latin America, although it is unclear if the laws will be more influenced by APEC or the IDPN. The privacy climate in Latin America is influenced by many other political, economic and cultural forces. In particular, economic instability (and lack of economic resources generally) make legislation with costly compliance burdens (such as the Argentine law) undesirable.

As a practical matter, many of the economies in the region are driven by very small businesses which cannot afford to comply with costly regulations. This means that the impact of EU-style laws will fall much more harshly on those multinationals that can (and are expected to) comply than on the family businesses that are the backbone of most economies. It also means that regulations which impose costs on small businesses must be strongly justified politically. This justification is difficult given the cultural lack of privacy concern across the Latin American citizens, who are themselves concerned primarily with access to economic and educational opportunities rather than data protection rights.

Additionally, where citizens do have concerns, such as the shared concerns that all people have regarding inappropriate marketing or the processing of sensitive data, it is politically more expedient to marry the *habeas data* concepts with specific laws to address these issues. This approach is seen in many regional regulations, from the Brazilian and Mexican consumer protection laws [9] to regional anti-spam laws [10]

Given economic and cultural considerations, this industry/application-centric approach to regulation is likely to continue to be the preferred method in the region. As in the United States, this approach provides for narrowly tailored laws that address specific harms, but it makes development of multinational compliance program more challenging.

Conclusions

The regulatory regime in Latin America—like that of Asia—will continue to develop and expand. *Habeas data* rights will certainly form the basis for additional statutory protections, which will add rules to address specific harms and concerns and to protect fundamental privacy rights.

---

[7] For more information, see www.apec.org.

[8] See: http://www.apec.org/apec/news__media/2005_media_releases/161105_kor_minsapproveapecprivacyframewrk.html

[9] See, *e.g.* Federal Law No. 8,078, Article 43, September 11, 1990 (Brazil) and Ley Federal de Proteccion al Consumido (Federal Consumer Protection Law, Mexico). See also, link to PROFECO Web site: http://www.profeco.gob.mx/ (Mexico, in Spanish).

[10] See, *e.g,* Ley Que Regula el Uso del Correo Electrònico Comercial No Solicitado (2005, Peru)

From a corporate perspective, the APEC Privacy Framework provides a model for balanced privacy legislation that supports both individual and business goals—protecting privacy while enabling global commerce. The possibility of restrictive EU-style regulation cannot be discounted, however.

The APEC Privacy Framework offers a clear alternative to the onerous EU-approach articulated by the IDPN. By focusing on the prevention of harm and controller accountability, countries can protect their citizens while enabling appropriate processing and transfer of personal information. APEC-inspired laws will recognize that data flows benefit individuals and the economies, and will prohibit data flows only when the harms outweigh the benefits. This means that companies will be able to use consolidated databases and data processing programs, as long as appropriate (but not overly burdensome) protections are in place.

It is critical for companies operating in the region to monitor for changes in the regulatory environment. It also may be prudent to devote some advocacy and compliance resources to the region in advance of new laws, so that the laws can be shaped and anticipated.[11]

---

[11] The author wishes to express her deep gratitude to Mauricio Domingo Donovan, legal counsel, Microsoft Mexico, for his contributions to the International Association of Privacy Professionals Latin American privacy session that sparked this article.

  PVLR ISSN 1538-3423