E-Commerce Best Practices: Online Privacy

(Ten Keys To Latin American Data Privacy)

By Luis Salazar*

Back in 1965, Frank Tannenbauem wrote a short but influential book, *Ten Keys to Latin America.* His ten keys, he promised, were "ten windows through which the reader may examine the grandeur, the mystery, the poverty, and the promise of Latin America." With so many countries, cultures, and legal systems, it is a challenge to present any definitive guide to Latin American Data Privacy that really covers the field. So, following Tannenbaum's lead, I offer my 10 keys to Latin America Data Privacy.

Key One: Habeas Data

Perhaps no single concept is more fundamental to understanding Latin American data privacy law than Habeas Data. Habeas Data, literally translated as 'you should have the data,' is a constitutional right granted individuals in many Latin American countries and is probably the predominant force in the region's data privacy law.

The right of Habeas Data originated in certain decisions of the German Constitutional Tribunal involving an individual's data stored third-party in databases. Although its details vary by country, Habeas Data is generally the right of an individual to petition a court to help it protect his or her privacy, including his or her image, privacy, honor, and freedom of information. The action can be brought against anyone holding

* Luis Salazar is a shareholder with the international law firm of Greenberg Traurig, and a founding member of its Data Privacy and Security Law Taskforce. A Certified Information Privacy Professional, Luis is also a member of the firm's Latin American Practice Group and is based in Miami – The Capital of the Americas. He may be reached at 305-579-0751, or at *salazarl@gtlaw.com*.

information, and it empowers the complaining party to request a correction or even destruction of personal data held by a third party.

More specifically, Habeas Data actions are typically asserted by the party whose data is effected. The complainant may seek injunctive relief, damages, or both, but must seek to access their personal data in the target database, and may ask that the data be maintained confidential, private, corrected, or updated. The complaining part must typically also identify the database and its owner and controller with particularity. Finally, there often must be some allegation of damages.

Brazil. Brazil became the first country to officially enact a Habeas Data law in 1988, when it passed a new constitution and gave Habeas Data full constitutional authority. Thereafter, Columbia adopted the Habeas Data right in its new constitution in 1991, Paraguay in 1992, Peru in 1993, Argentina in 1994, Equator in 1996, and Bolivia in 2004. With each subsequent enactment, Habeas Data rights became clearer.

In Brazil, the power of Habeas Data is limited to the right of an individual to access and correct data, but not to update or destroy it. A subsequently enacted Habeas Data enabling law granted individuals the additional power to add an annotation to their data stored in a database to note that it is under legal dispute. Enforcement of the Habeas Data right in Brazil, however, can be a challenge, because venue for the action changes depending on the defendant.

Paraguay. When Paraguay passed its version of Habeas Data, it enhanced the definition and simplified the procedural elements. Its Habeas Data constitutional provisions not only allow an individual to access information and data available on himself, but also to know how the information is used and for what purpose. A petitioner

can request that a court of competent jurisdiction update, correct, or destroy entities if they are wrong or if they are illegally affecting his rights. Paraguay designated allows only one court – the constitutional chamber of the Supreme Court – to hear and decide all Habeas Data cases.

Peru. The Peruvian Habeas Data provisions are similar to the Paraguayan ones, but do not allow for the correction or removal of erroneous data stored in a database. It does, however, forbid the broadcast, copy, transfer, or distribution of that erroneous data.

Argentina. The Argentinean Habeas Data provisions further refined Habeas Data rights. Actually referred to as an "amparo," the traditional label for certain constitutional guarantees in the Latin American civil system, the provisions include most of the above Habeas Data enactments, including the right to access data, correct it, update it, or destroy it. It also forbids the broadcast or transmission of incorrect or false information, but explicitly excludes the press from such actions.

Traditionally, Habeas Data has been seen as an individual right that can only be brought and asserted by the effected individuals. More recently, Latin American courts have begun to take a broader view. For example, the Supreme Court of Argentina ruled in *Urteaga v. Estado Nacional* (1999), that an individual had standing to assert a Habeas Data claim for information about his brother, who was killed during Argentina's "dirty war." In subsequent cases, the Court has reinforced this trend. It may be possible, then, that Habeas Data will eventually become one way to seek privacy remedies for groups or classes of individuals.

It is worth noting that Mexico, which does have fairly broad constitutional privacy rights, does not have Habeas Data. But there is a law pending the Mexican Congress that would enact a habeas data style law.

Key Two: Argentina and Its Data Privacy Law

Of all the Latin American countries, it seems that Argentina is perhaps the most "advanced" in dealing with data privacy and data protection issues. It has certainly embraced Habeas Data and can boast of being the only country in Latin America that is considered adequate for data protection purposes under the EU Data Privacy Directive.

There are several reasons why Argentina has distinguished itself in this regard. Certainly, the legacy of its "Dirty Wars" have weighed heavily in its adoption of Habeas Data constitutional provisions in 1994. Simply put, Argentineans desire for access to public and private databases was driven in part by their desire to determine the whereabouts of lost family members or to never be denied that information again. After the enacting of this data privacy foundation, the government engaged in a series of actions that triggered various privacy laws in response. For example, to enforce new tax-collection laws, the government began surreptitiously reviewing taxpayers credit card histories, insurance records, and more. This prompted the passage of a law that allows private causes of action for invasion of privacy for an unauthorized review of credit records. Later, a number of high-profile political figures had their telephones tapped, which resulted in the passage and ultimate enforcement of a law barring that type of invasion of privacy.

By the late 1990's, the ground was thus fertile for the passage of more comprehensive laws to address data privacy – there was both a legal landscape that addressed privacy and public attitudes valuing privacy.

Passed in 2000, the Law for the Protection of Personal Data ("LPPD") went into effect in 2001, with passage of related regulations under decree 1,558/2001. It is comprised of 48 sections organized into 7 chapters, with only the last chapter dealing with habeas data. The LLPD vests enforcement in a new body, the Dirección Nacional de Protección de Datos Personales (the "**DNPDP**"), while establishing sanctions for its violation. The LPPD is a federal law enforceable throughout Argentina, but provincial governments are encouraged to enact local regulations to ensure compliance, and many have done so.

The LPPD requires all data banks and depositories to register with the DNPDP, and provide specific information such as the name and domicile of the person in charge of the data, the purpose and characteristics of the data file, the nature of the data, and the form in which it must be collected and updated, entities who may receive it, ways in which the data is to be secured, categories of people with access to it, the length of time for which it will be used, and the conditions under which data owners will have rights to access and update the data. Some 15,000 databases have been registered.

The LPPD empowers individuals to seek injunctive relief by accessing their personal data kept in either public or private databases or by requesting that personal data be maintained confidential, private, corrected, or even updated. The LPPD requires plaintiffs filing habeas data complaints to identify with as much particularity as possible the name and domicile of either the data file or register and the data user, and,

if a public data bank is involved, identify the appropriate government body. The plaintiff must also describe why he believes a particular database has information concerning him, why that information is discriminatory, false, or inaccurate, and why the data owner is obligated to comply with the LPPD. The burden of proof for meeting these criteria is relatively low.

The LPPD's sanctions range from warnings to fines ranging between $1,000 and $100,000 pesos, to complete closure of a data file or base. Of course, the level of sanction should be in proportion to the seriousness and extent of the violation shown and the damages caused. The LPPD also imposes criminal sanctions for violation of certain of its provisions, including knowingly inserting false information into a personal data file, breaking into a data bank, or disclosing confidential data to a third party.

Subsequent enforcement of the LPPD in Argentinean courts has somewhat expanded its reach. For example, courts have expanded the law's authorization to bring actions against data banks and users and those responsible for the data banks, to include assignees using the information. And courts have seemed willing to compensate plaintiffs for emotional harm arising from the use of their data, and to hear cases arising from transactions with financial institutions.

As noted, the EU determined that the provisions of the Argentinean constitution when combined with the LPPD provided adequate data privacy protection sufficient to meet the standards of the EU directive. While there are in fact many similarities between the LPPD and the EU directive, there are also a number of remarkable differences. For examples, while both define personal data in a similar manner, the LPPD separately defines "sensitive data," which is data that reveals racial or ethnic

origin, religious, political, or philosophical beliefs, union membership, or information about health or sexual behavior. As further examples, the LPPD describes a "data owner" while the EU directive uses the term "data subject," the LPPD uses a "person responsible" while the EU directives uses "controller."

The LPPD also requires that data collected about persons be "certain, appropriate, pertinent, and not excessive," as well as accurate and updated, limited in purpose, and destroyed when no longer necessary.

The LPPD vests certain rights in the data owner such as: (a) the right to information (allowing data owners to inquire about and confirm the existence of their personal data and related details); (b) the right to rectification, updating, or suppression (the right of data owner to control the accuracy and amount of information available about them); and (c) the right of access permitting data owners to request and obtain their personal information within ten days.

The LPPD also regulates international transfers of data, and its provisions are modeled on EU directive article 25. The LPPD provides no safe harbor provision for the U.S. for transferring information to and from Argentina. It prohibits the transfer of personal data to countries with inadequate levels of protection, subject to a number of exceptions for national security, medical reasons, pre-existing treaties, etc. But data owners may give their express consent to the transfer of information to an "inadequate country." The DNPDP has yet to name any country adequate or inadequate.

The DNPDP is the controlling body created by the LPPD. It is an agency under the Ministry of Justice and Human Rights, and is funded primarily from taxes and fines it collects and from the national budget. Its duties include assisting parties in

understanding the LPPD, issuing applicable rules and regulations, maintaining data file records, pursuing and enforcing administrative sanctions, monitoring private databases, and standing in the place of plaintiffs in habeas data actions. Further, at the request of an interested party, the DNPDP must investigate the legality of the gathering, exchanging, delivering, and controlling of personal data.

Argentina is one of the ten keys to Latin American Data Privacy because it is in fact leading the way on data privacy issues and has taken a leadership role in urging its fellow Latin American countries to adopt modern and comprehensive data privacy laws.

Key Three: Spain and the Red Iberoamericana

It is perhaps appropriate that this Key follows closely that of Argentina. Spain's role in fomenting data privacy concerns throughout Latin America can hardly be understated – Argentina's EU-style data privacy laws are certainly one result of its efforts.

The key player in this effort has been the Spanish Data Protection Agency – La Agencia Española de Proteccion de Datos ("AEPD"). Each year, the AEPD organizes and promotes an Iberoamerican Data Protection Conference, and, in 2003, this conference lead to the formation of the Red Iberoamericana de Protección de Datos, or the Latin American Data Protection Network, an organization dedicated to promoting data privacy issues, and whose membership consists of Argentina, Brazil, Chile, Colombia, Costa Rica, El Salvador, Spain, Guatemala, México, Nicaragua, Perú, Portugal, and Uruguay. Spain assumed the presidency of the Red during the first two years of its existence.

Among the Red's goals is promoting and maintaining open channels of dialogue and communication among the Latin American countries and their data protection agencies to promote open and constant exchange of information, experiences and know-how.

Thus Spain and the Red Iberoamericano is a Key to understanding Latin American Data Privacy because they are a constant force in the development of data privacy laws throughout the region.

Key Four: El Spam

This much breaks across all language barriers - everyone hates "El Spam." It is as pernicious and wasteful a problem in Latin America as it is here in the US, in Europe, or Asia. A number of Latin American countries have passed laws to respond to the Spam challenge, with perhaps the most well-known of these being Section 27 of the 2000 Argentinean Data Protection Law. Among other things, that law gives recipients the right to opt out of Spam. In a recent case, plaintiffs successfully sued a Spammer who did not comply with the law and continued to send them Spam. The Court enjoined the spammer and awarded damages.

Peru enacted a "Ley AntiSpam" that was recently the subject of what most hope will be precedent-setting decision fining a Peruvian Spammer US$5,458 for repeated violations. Notably, this successful effort was made possible by the dedication and persistence of the author of the "Peru Sin Spam" (Pero Without Spam) blog.

Anti-Spam laws have been introduced in Brazil, Chile, and Colombia.

Likewise, Spyware is no less a problem in the region than in the US or the EU. In Argentina, the LPDP makes spyware illegal because it bars the surreptitious

collection of data. Enforcement of these restrictions, however, would likely be by means of an individual bringing a Habeas Data action against a spyware user – probably a fruitless effort. In Chile, Spyware would likely be covered by The Ley Contra Delitos Informáticos (The Law Against Information Crimes), which makes the destruction of a computer or unlawful access to its contents a crime punishable by 1½ to 5 years in prison.

Thus, El Spam is a Key to Latin American Data Privacy because it too drives changes in the way Latin American countries manage data privacy.

Key Five: El Celular and M-Commerce

Here's a telling statistic: in Colombia, internet penetration hovers around 10% of the population, but mobile phones enjoy a 64% penetration rate. By some estimates, there are over 300 million cell phone users in Latin America, and as many as 50 million use their phones to surf the internet. More than just talking with friends, Latin Americans are using their phones for Mobile Banking, to buy products, and, increasingly, to make Mobile Remittances.

For many Latin Americans, then, the frontline for data privacy is that all phone in their hand. It's where they get spam, get information and control their bank accounts, pay their bills, pay for taxis, and so on.

Cellular phones and M-Commerce are thus an important key to Latin American Data Privacy because it is the primary point of contact between the average consumer and data privacy issues.

Key Six: Anti-Colonialism

Latin America countries spent many years as colonies of foreign powers, and many more years as virtual colonies of others. It should be no surprise, then, that anti-colonialism can still be an incredibly fierce motivating factor in the development of Data Privacy in Latin America.

Case in point - in April 2002, EPIC obtained documents under FOIA that indicated that the Immigration and Naturalization Service (INS) had purchased personal information from the national ID databases of several Latin American countries. ChoicePoint, a data brokerage company, has a contract with INS to provide citizen registry, motor vehicle, and other information for Brazil, Argentina, Mexico, Columbia, and Costa Rica. U.S. drug and immigration investigators prized the data, according to the Department of Homeland Security and other law enforcement sources, because it gave them latitude to track suspects inside Mexico without alerting local authorities.

In April 2003, the Associated Press wrote an article about the sale of this information that ran in newspapers internationally. From there, the documents sparked inquiries in Mexico and other Central and South American countries regarding the sale of foreign citizens' personal information to the US government by information broker ChoicePoint.

Latin American privacy experts claimed that the acquisition of the information by ChoicePoint may have been illegal, and that the sale infringes on national sovereignty. Costa Rican, Nicaraguan, and Mexican authorities investigated the matter, and the Mexican Federal Electoral Institute filed a criminal complaint against persons who sold voter data to ChoicePoint.

As a result of this uproar, ChoicePoint's database is no longer available to help U.S. authorities. After the Mexican government complained that its federal voter rolls were the source, and were likely obtained illegally by a Mexican company that sold them to ChoicePoint, the suburban Atlanta company cut off access to that information. In June, ChoicePoint wiped its hard drives of Mexicans' home addresses, passport numbers and even unlisted phone numbers. The company also backed out of Costa Rica and Argentina.

The revelations spurred privacy movements in at least six countries where the company operates. Government officials have ordered — or threatened — inquiries into the data sales, saying ChoicePoint and the U.S. government violated national sovereignty.

Anti-colonialism, then, as a driver of data privacy sentiment, is yet another Key to Latin American Data Privacy.

Key Seven: Mexico

Mexico is the slumbering giant of Latin America Data Privacy. It has struggled for years to decide upon and pass appropriate data privacy legislation, but for a variety of reasons has been unable to do so. Because of its economic resources, the extent of its existing internet use by its Mexican consumers, and its geographical proximity to the U.S., Mexico can be a critical key to the development. In Mexico alone, for example, ecommerce surpassed $38 billion last year, with estimates for the entire region to reach over $100 billion by 2007.

Mexico does have a number of data privacy laws. For example, its constitution provides guarantees to the privacy of private communications and protects against

unlawful searches and seizures. The government must keep tax returns, payments and audits in strict confidence, and there is a law similar to the U.S.'s Freedom of Information Act.

The Credit Institutions Act establishes bank secrecy, barring financial institutions from disclosing any information relating to the deposits or any other bank services of their customers to any person, except the taxing authority or by court order. Likewise, Articles 136, 137 and 138 of the General Health Act give patients the right to have all medical information and clinical records kept in strict confidence and barred from any disclosure without his or her authorization.

On the other hand, privacy in the workplace is very much upheld, contrary to the trend in the United States. Employers are required to respect the dignity of an employee's working conditions of the workplace, and the employees may not waive those rights, according to Articles 3 and 56 of the Labor Law. Thus, surveillance, monitoring emails, and even internet use can be risky for Mexican employers.

In recent years, data privacy developments have seemed to come at a faster pace in Mexico. For example, in 2002, the Mexican Congress passed the Credit Bureaus Act, which allows consumers to access their own credit records, request corrections, and even request elimination of some of their personal data from credit bureaus. In 2004, the Congress passed the Federal Consumer Protection Act, which contains certain provisions for consumers doing business "online." For example, vendors are obligated to keep consumer information confidential, and are barred from disclosing, transferring, or disseminating that information to other vendors, unless the consumer provides prior authorization. Vendors are required to advise the consumer on

the security technology used to protect any information submitted, and vendors are required to inform consumers of their physical address, telephone numbers, and other pertinent information concerning warranty instructions before any transactions are concluded. The Federal Consumers Protection Agency is authorized to monitor websites in order to confirm that they are obeying the provisions of the law.

The law also contains spam provisions, and it requires all advertising sent to consumers, either on or off line, to indicate the name, address, telephone, and the email to vendor. Consumers may request that messages not be sent to them, making this effectively an anti-spam bill. The law also authorizes the FCPA to keep a public registry of consumers who have opted out of receiving mailed advertising materials, what is effectively a "Do Not Call" registry. Before sending advertising messages to consumers, vendors are required to verify their lists to make sure they are not sending to any opt-out consumers.

Corporate data privacy practices still vary widely, even though some organizations have attempted to promote some basic privacy codes, including the Mexican IT Association, the Mexican Internet Industry Association, and others.

Finally, some major data privacy legislation still looms on the horizon, with many expecting a comprehensive new law in this Congressional session (2006-2012). That law will likely have many Habas Data protections, such as the right to access, correct, and update personal data, the right to be informed about data collection practices, and restrictions on cross-border data transfers. Such a law would also very likely create a new Data Privacy Agency.

Key Eight: Key Players/Shapers

There are a number of entities that are actively shaping the future of data privacy in Latin America. The Ibero American Data Protection Network (IDPN), in particular, appears to have the broadest impact across the region. Founded by the Spanish Data Protection Agency, and formerly headed by Dr. José Luis Piñar Mañas, an IAPP member, it conducts various outreach efforts to promote data protection laws similar to the EU Directive. Its efforts credited with leading to the passage of Argentina's LPDP and qualifications as an acceptable country under the EU Directive.

The LPDP's passage also created another influential body – the Argentinian Data Protection Agency. It is charged with enforcement of the law and is generally thought to have the potential to take precedent setting actions with potentially region-wide repercussions.

Chambers of Commerce and other business associations have also actively promoted good privacy principles. In Mexico, for example, the Mexican Internet Association (AMIPCI), along with the Ministry of the Economy and the Office of the Federal Attorney for Consumer Protection, introduced the "AMIPCO" trusted site seal, designed to identify sites that comply with data privacy regulations, properly using personal data, and reducing bad Internet practices.

Finally, there are a number of private commentators and critics who champion data privacy, and closely monitor the many twists and turns of its development. Perhaps the best known of these is Habeasdata.org and its related state specific Habeas Data blogs. These sites deserve credit for raising the profile of data privacy throughout the region.

Key Nine: Transnationalism and Immigration

Transnational residence and immigration continues to be a powerful force in Latin America. Some studies estimate there are now more than 20 million transnational residents alone – those that maintain homes in Latin America and in a foreign country, such as United States. Although a large number of immigrants from Latin America to the United States, for example, are workers with relatively low levels of education, an increasingly higher majority of immigrants have advanced degrees and are highly educated.

Another factor to consider is that Latin American immigrants in the United States remit nearly $30 billion to friends and family in their home countries.

Both travel and remittances between United States and Latin America have become more regulated over time, with United States border-entry becoming more difficult and involving more tracking. Anti-money laundering and Banks Secrecy Act regulations likewise closely track and restrict the remittances that can be sent to Latin America.

For this reason, transnational living and immigration continued to be a key to Latin American data privacy because they continue to drive consumer's data privacy concerns.

Key Ten: All Data Privacy is Local

There is an old saying in politics – all politics is local. The same is true for managing Data Privacy in Latin America. Hopefully, this article and the related presentation has given you some basic information that will allow you to spot issues critical to managing data flows in Latin America. But to truly understand and manage data privacy in the region, you need someone with local knowledge and contacts.