

February 10, 2003

Lic. Sergio Carrera Rivapalacio
Director General de Fomento al Comercio Interior
SECRETARIA DE ECONOMIA
Av. Insurgentes Sur No. 1940 4o. Piso
Col. Florida
01030 Mexico, D.F.

Dear Mr. Carrera,

As you may know, the United States is closely following developments in data protection policymaking in Mexico including the law presented by Senator Garcia Torres in the Mexican Congress. We would like to commend the Government of Mexico and Senator Torres for their attention to the issue of personal data protection. The United States shares the belief that measures to facilitate and bolster on and off-line privacy are essential to consumer protection. Appropriate measures, whether legislative, self-regulatory, or a combination of the approaches, coupled with privacy and security-enhancing technologies, can fuel trust and the broader growth of cross-border trade and on-line communications.

With respect to proposed legislative measures to address data protection issues, we are concerned about the unintended consequences of broadly prescriptive legislative measures. While we appreciate Mexico's attention to the issue of data protection, we believe that it is important to express our concern that, if passed, the legislation presented by Senator Torres would negatively impact the ability of U.S. and Mexican companies to receive and send trans-border flows of personally identifiable data, thereby weakening cross-border e-commerce and services between our two countries. Therefore, we would like to take this opportunity to present our comments on the provisions of the draft bill.

It is our understanding that private sector interests on both sides of our border have recently expressed similar concerns with the draft bill. We believe that these concerns are valid and that all stakeholders, including the Government of Mexico and the private sector, should work together to develop a more balanced and internationally compatible approach to data protection that addresses what concerns individuals most, the misuse of their personal information and resulting harm.

As neighbors and important trade partners, Mexico and the United States must work together on approaches for addressing legitimate concerns about data protection and relevant cross-border issues. While national approaches to data protection vary, the United States currently utilizes a mix of sector specific legislation (to protect certain

highly sensitive personal information, including children’s information, medical records and financial data) and self-regulation. We believe that self-regulatory initiatives (including company codes of conduct, web “seal” programs and alternative dispute resolution mechanisms), coupled with governmental backstop enforcement, are effective tools for achieving meaningful data protection.

Multilateral and private-sector initiatives, such as the Organization for Economic Cooperation and Development (OECD) and the Global Business Dialogue on Electronic Commerce (GBDe) also have an important role to play in encouraging the development and use of privacy-enhancing technologies and in promoting consumer education and awareness about online privacy issues. These two organizations have developed data protection guidelines that serve as useful alternatives to “one-size-fits-all” legislative approaches to data protection. We encourage Mexico to actively consider these efforts and the role that self-regulatory programs can play in bolstering data protection.

The United States looks forward to working with Mexico in order to achieve internationally compatible standards for data protection. Our cooperation in this regard will have the added benefit of helping to ensure the continued flow of trans-border data and cross-border trade and services. As a next step, we would like to work with you to organize a workshop in Mexico City later this year. We envision this workshop as an opportunity for the public and private sectors to exchange views on data protection; how regulation may impact trade between Mexico and the United States; and alternative approaches for dealing with data protection concerns. We look forward to your partnership in this dialogue.

Please feel free to contact me with any questions on the attached comments or the proposed workshop.

Warm Regards,

Michelle O’Neill
Deputy Assistant Secretary
for Information Technology Industries

CC: Mr. Jesus Orta
Mr. Jerry Mitchell
Mr. Daniel Olivera Pomar

United States Government Staff Comments on Draft Federal Personal Data Protection Law

Preamble

The proposed legislation's preamble focuses on addressing consumer harm. The preamble begins with an assessment of the benefits of the information economy, but recognizes potential risks from the misuse of information that could result in actual harm to individuals. Examples of harmful use of personal information noted by the draft Torres bill include the distribution of information about a person that may not be truthful or accurate, or which is so sensitive that the interested person may not wish to have it disclosed without prior consent. Other examples concern the automatic processing of information, including incomplete, erroneous or out-of-date information processing, the results of which when used could cause harm to individuals and consumers. As a result of this information economy benefit-risk analysis, Senator Torres and the Joint Committees on Constitutional Issues and Legislative Studies noted their conclusion that gaps exist in Mexican law for providing legal means for expeditious, specific action and resources to respond to errors, omissions or improper handling of personal information in order to avert harm to individuals.

Consistent with this conclusion, we believe that a targeted approach to data protection enforcement and, indeed, data protection legislation, focusing on actual harms that are likely to result from the misuse of personal information, will most directly and effectively protect individual data protection interests while at the same time supporting the growth of cross-border commerce. Indeed, the concept of such a targeted approach to data protection is gaining acceptance internationally. As you may be aware, five countries in the European Union have recently put forth a written proposal that would shift the emphasis of EU legislation from its broad focus on protection of personal data to the actual use or misuse of personal data. Similarly, the OECD countries participating in the Working Party on Information Security and Privacy, including Mexico and the United States, are completing a report on online privacy enforcement that recommends that member countries should focus on measures where individual users suffer the most harm as a consequence of misuse of their personal data.

Title I – General Provisions

Scope of the Definition of “Sensitive Data”

The proposed legislation imposes different requirements on the treatment of data based on whether it is deemed to be “sensitive data” or otherwise. Attempting to draw such distinctions seems to be fraught with difficulty, particularly in thinking about drafting regulations and assuring business compliance. For instance, Article 4 defines “sensitive

data” to include “all data that reveal the racial or ethnic origin; political opinions; religious, philosophical or moral beliefs; labor union membership; health or sex life of a person”. As written, this definition is overly broad and allows too much room for inference. For example, information on a customer’s book purchase or a passenger’s meal selection on an airplane could be deemed “sensitive” since they can theoretically imply a person’s religious, health or sex life.

Collection of Data

Article 5 sets forth several rules pertaining to the collection of data. As written, the standards articulated in Article 5 for the collection of data lack sufficient clarity for businesses to follow. For example, while the article states that all data collected shall be “adequate, certain...” it is not clear what level of “certainty” is required.

In addition, Article 5 appears to exclude a reasonableness standard. Instead of requiring all processed data to be “accurate and up to date in agreement with the actual data concerning each interested person involved”, we recommend simply requiring reasonable steps be taken to maintain the accuracy of information. Similarly, we urge Mexico to strike the requirement that all data must be stored “so as to enable the right of access to be exercised by each interested person involved” and instead allow data subjects reasonable access to personal information about them that an organization holds and be able to correct, amend or delete that information where it is inaccurate.

Access

Article 5, paragraph 6 requires all data to be stored “so as to enable the right of access to be exercised by each interested person involved”. Additional access requirements appear to be detailed in Articles 15-18. While allowing customers to access and correct information collected about them can greatly increase customer’s confidence, the requirements set forth in the draft bill may have the consequence of encouraging frivolous and vexatious requests for access and may raise certain information security issues.

We believe that the obligation of an organization to provide access to the personal information it holds about an individual should be subject to the principle of proportionality or reasonableness and has to be tempered in certain instances. Therefore, we encourage Mexico to adopt a clear and concise access provision that allows data controllers to deny access where the expense and burden of providing such a request are disproportionate to the data subject’s right to such information. We also encourage consideration of how the legislation might address balancing the benefits of convenient consumer access to their information with the inherent risks to security that greater access could create.

Title II – Interested Persons Involved and Persons Responsible for Data Records

Notice

The draft bill appears to provide a notice requirement for the collection, processing and use of personal data. Indeed, notice is a key element of any privacy policy. However, the notice requirements set forth in the draft bill proposed by Senator Torres would far exceed provisions in data protection models adopted elsewhere. For instance, it appears unreasonable to require a data controller to disclose, “all possibilities of exercising rights of access, or of including supplementing, correcting, withholding making confidential and eliminating personal data to that person and how and when such rights can be exercised”. Since it is impossible for a data controller to foresee all such situations, it would be advisable to simply require policies to clearly articulate the data subjects’ rights to access, review and correct data and the necessary procedures for doing so.

In addition, it would be impractical to require a data controller to disclose “the identities and addresses of the persons responsible for the data file, record, database or data bank”. In some cases, several hundred handlers of the data may be involved. Rather, the data controller should simply be required to disclose who is responsible for data protection and compliance within the organization.

Consent

The draft bill’s requirement that “all gathering and processing of data require the prior consent of each person involved” (Article 7) may have the consequence of stifling electronic commerce. Such a provision would seem to preclude the use of certain Internet technology, such as “cookies”, in almost any circumstance and may significantly raise the cost of electronic commerce, as the data controller would be required to obtain consent on an individual basis at every point of collection.

This burdensome requirement can place small and medium sized firms at a severe disadvantage. Therefore, we encourage Mexico to adopt the more internationally compatible approach of “opt-out” consent for most types of data and “opt-in” consent for sensitive information. This is the approach favored in data protection legislation enacted elsewhere, namely in Canada and Australia.

Sensitive Data

As previously noted, we encourage Mexico to adopt a narrower definition of “sensitive data” in Article 4 in order to reduce the ambiguity of the current definition and to allow data subjects and controllers a clearer picture of what is actually considered “sensitive” under the bill. We also believe that more clarification can be added to Article 8, which

details rights and responsibilities concerning sensitive data under the act. For example, in paragraph 2, we are not certain what is meant by “reasons of general interest”. Secondly, we suggest striking paragraph 3, which prohibits “the formation of data files, records, databases or data banks that disclose sensitive data...” Files, records and databases store rather than disclose data, so this provision would seem unnecessary.

Finally, we encourage Mexico to strike paragraph 5, which prohibits data controllers from making “value judgments” regarding data processed automatically. Sales transactions often require “value judgments” based on personal information provided in order to determine the creditworthiness of consumers. To prohibit such practices would seriously undermine current sales practices in a number of sectors.

Data Integrity & Security

Article 10 of the draft bill makes reference to “technical standards” for the integrity and security of data. However, Article 10 does not provide enough clarity regarding the responsibilities of data controllers under this provision. In particular, how are the “technical requirements” for integrity and security to be determined? Will these requirements be based on accepted international standards and practices? Will the private sector be consulted during the development of these requirements?

We agree that organizations should minimize the risk that personal information would be misused or compromised and ensure that any data collected is relevant to the purpose identified. Additionally, organizations should take steps to secure personally identifiable information and should take more care when sensitive information is at stake. At the same time, it is important that the private sector leads on securing its networks. For their part, governments should promote a technology-neutral approach to security, which allows the private sector to choose the appropriate technical solutions.

Release of Personal Data

Article 12 of the draft bill appears to place limitations on the release of personal data held by a data controller. The provision conditions any release on the affirmative consent of the data subject. We encourage Mexico to modify this provision to allow subsequent transfers of data that are contemplated and/or specified in the initial collection of the data. Additionally, transfer or release of personal data to third parties acting as agents should be allowed without further consent if it is ascertained that the third party/agent provides similar data protections.

Transborder Data Flows

We are quite troubled by the draft bill’s transborder data flow provision (Article 13) and its imposition of an “equivalency” standard for data protection regimes in other countries. This provision would presumably prohibit transfers to nations that do not exactly match the requirements set forth by the draft bill. As a result, the bill would impose a standard

far more stringent than data protection laws elsewhere, including those in Argentina, Canada and Australia. Even the European Union Directive on Data Protection allows transfers to non-European Union countries that have demonstrated “adequate” protections. Therefore, if passed, the draft bill would have the consequence of prohibiting transfers of personal data to anywhere outside of Mexico since it is highly unlikely and unfair to assume that data protection regimes elsewhere can exactly meet Mexico’s requirements. We highly encourage Mexico to strike this “equivalency” standard and to require organizations outside of Mexico to follow reasonable measures of data protection consistent with Mexico’s requirements.

Registration and Reporting Requirements

As written in Articles 14-26, the draft bill appears to set forth overly broad and burdensome registration and reporting requirements. In addition, it appears that the majority of the information required by the Federal Institute for the Protection of Personal Data under this draft bill is simply not necessary in order to track compliance with the law. Finally, certain questions concerning how the registration and recording systems are intended to operate remain unanswered. For instance, how are data records to be registered with the agency? What will data subjects be allowed to see? How would this system be monitored or enforced for accountability?

Title V: Legal Actions

Article 30

This article lists several circumstances in which legal action for the protection of personal data may be warranted. We encourage Mexico to establish a reasonableness test for determining whether a company or data subject should have known that the information was false or incorrect.

Alternative Dispute Resolution

While the draft bill sets forth provisions relating to the adjudication of complaints and disputes involving personal data under the act, it does not appear to encourage parties to utilize alternative dispute resolution (ADR) systems, including negotiation, mediation and arbitration. In both the online and offline worlds, ADR systems are being used quite successfully as effective, quick and efficient means for addressing complaints from data subjects. In addition, we believe that the use of ADR avoids overburdening administrative and/or judicial systems and can preserve the data subject’s right to seek legal redress should they be dissatisfied with the results of the ADR process. Finally, ADR systems can offer more flexibility in finding solutions that satisfy both parties. Therefore, we encourage Mexico to offer incentives for the use of ADR systems under this act.

