Submission by the United States Department of Commerce's International Trade Administration on Singapore's Proposed Data Protection Bill
April 27, 2012

Introduction

The U.S. Department of Commerce International Trade Administration (ITA) submits the following comments on the commercial aspects of Singapore's proposed data protection bill. ITA welcomes the opportunity to provide comments and appreciates the Government of Singapore's efforts to seek and consider comments from all stakeholders, including U.S. interests. Please note that these comments touch broadly on only a few issues, but that should not be interpreted as a lack of interest in many of the other topics raised in the proposal. The comments include several requests for clarification. Further clarification of some of these issues will most likely contribute to successful implementation of these regulations and ensure there is no unintended adverse impact.

Comments on Singapore's Proposed Bill

We appreciate our engagement with the Government of Singapore and look forward to continuing this dialogue on the proposed Data Protection Bill. The protection of data and consumer's personal privacy is an objective that, when achieved, will stimulate continued economic prosperity in Singapore and abroad. In addition, the proposed data protection bill goes a long way towards ensuring there is a balance between the protection of consumer data and business interests. Also included in the proposed legislation is a Do Not Call registry that is similar to the one already in place in several counties, e.g. Australia, New Zealand and the United States.

Below are several recommendations and requests for clarification ITA staff respectfully presents to the Government of Singapore. We are eager to discuss ways that we can further facilitate interoperable privacy frameworks between our two countries.

Section 5: (Jurisdictional Scope -- "Singapore link")

Staff believes the condition in section (2)(a)(i) – "personal data is collected from an individual who is physically present in Singapore at the time of collection" – may be difficult for companies to ascertain. Staff would appreciate clarification about how companies will know where an individual is physically located when data is collected. Moreover, this standard would subject companies to jurisdiction in Singapore even when they have made no purposeful connection to Singapore's laws or citizens. Staff would like more clarity as to whether other elements of the laws of Singapore would limit the application of this section to companies that display some degree of knowledge that they are directing their activities toward Singapore, or at least require more than incidental collection of personal data from a person who happens to be in Singapore.

Section 10: Data Protection Fund :

Staff feels it would also be useful to further consider whether any sort of unintended incentive to fine organizations may result from the proposal to "provide financing or incentives to any public authority, enterprise or education institution or other person undertaking or facilitating any programme to promote data protection awareness or implementation" out of funds collected through fines deposited into the Data Protection Fund.

Sections 13(1): Reasonable Person Clause:

Staff believes there is a lack of certainty as to how Singaporean authorities and courts would interpret the reasonable person clause. We believe the standard provides flexibility, which is something we appreciate as we have also emphasized this as a key property of any privacy law. Staff believes that many core commercial activities may fall under the reasonable person standard or the reasonableness standard included in the accompanying schedules. Therefore, staff would like more clarity as to what activities are subject to the reasonable person clause, and whether there are means by which authorities might provide additional clarity after legislation is enacted, for example, through enforcement guidance.

Section 13(4): An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act:

Staff believes that requiring an organization to hire or repurpose existing personnel could be detrimental to small and medium enterprises. Therefore, staff would like to know whether an organization would need to hire additional employees to ensure compliance with the requirement of Section 13(4).

Sections 24: Right to Request Correction of Personal Data:

Staff welcomes the inclusion of a right to request the correction of personal data but believes that the proposal could be further developed. For example, the Obama Administration's Consumer Privacy Bill of Rights states that "In determining what measures [companies] may use to maintain accuracy and to provide access, correction, deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm."

Section 25: Accuracy of Personal Data:

Staff supports the Bill in its protections and care of personal data. However, staff would like additional clarification of the use of the word "decision" in Section 25 subsection (a).

Section 31: Power to Give Directions:

Staff feels it would be helpful to obtain additional information about the circumstances that would merit that an organization "pay a financial penalty of such amount not exceeding SGD 1 million as the Commission sees fit".

Section 33: Power to Investigate or Conduct Inquiry:

The draft bill endows the Data Protection Commission with extensive investigative powers that appear to be similar to European Union style investigative powers. These extensive powers may be ill-suited to violations of privacy law, where evidence is unlikely to be perishable and perpetrators are unlikely to flee. Staff would appreciate clarification on the need for the Data Protection Commission to have these extensive investigative powers.

Section 36: Right of Private Action:

Staff would appreciate additional clarification as to how Section 36 might potentially affect business and industry. Has MICA analyzed the extent to which companies could be subject to frivolous claims, and what safeguards may be considered to prevent such frivolous claims?

Sections 60, 63: Power to Exempt, Power to Make Regulations:

The DPC and Minister are given authority to craft rules for specific sectors, or to grant them carve-outs. Staff feels that this authority creates flexibility that the administrators will find practical and beneficial. However, such authority could also be used to distort competition. Staff would appreciate further clarification as to how the DPC and Minister will use this authority.

Schedules 1-10:

We appreciate the inclusion of Schedules 1-10 in the proposed Data Protection Bill. The schedules provide detailed rules that describe how the Law will work. Staff feels the schedules also make the "reasonable person" standard more concrete. However, staff feels it would be helpful to obtain additional clarification explaining how the schedules at the end of the draft bill will be used to implement and administer the Law.

ITA appreciates the opportunity to provide these comments and would welcome the opportunity to discuss these issues further. Following for your consideration and reference are brief descriptions and links to the Administration's Privacy Blueprint and the Federal Trade Commission Privacy report. ITA has welcomed Singapore's participation in the development of the APEC Cross Border Privacy Rules system and provides a brief description of that initiative below.

Any questions or comments may be directed to: Joshua Harris, Associate Director, Office of Technology and Electronic Commerce at the U.S. Department of Commerce's International Trade Administration, joshua.harris@trade.gov, 202-482-0142.

Administration's Privacy Blueprint and Federal Trade Commission Privacy Report

On February 23, the Administration released its Privacy Blueprint including a Consumer Privacy Bill of Rights which provides a baseline of clear protections for consumers and greater certainty for companies. A central goal of the Privacy Blueprint is to promote international interoperability of privacy frameworks. The Administration places a high priority on facilitating trade while protecting consumer privacy. The Blueprint highlights the work of the Asia Pacific Economic Cooperation Cross Border Privacy Rules system as a model for implementing global interoperability. The Privacy Blueprint is available at: http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

The Privacy Blueprint sets forth a framework that enhances consumer privacy while at the same time promoting innovation and continued growth of the digital economy. The Administration believes that unduly prescriptive regulation such as technical mandates, data location requirements, and universal opt-in consent requirements burden domestic and international commerce without advancing consumer privacy protection. The proposed legislation recognizes the need for flexibility in a number of provisions, which we welcome and encourage.

On March 26, the Federal Trade Commission issued a final report entitled "Protecting Consumer Privacy in an Era of Rapid Change" setting forth best practices for businesses to protect the privacy of American consumers and give them greater control over the collection and use of their personal data. In the report, the FTC also recommends that Congress consider enacting general privacy legislation, data security and breach notification legislation, and data broker legislation. The report is available at: http://ftc.gov/opa/2012/03/privacyframework.shtm.

Asia Pacific Economic Cooperation (APEC) Cross Border Privacy Rules System (CBPRs)

CBPRs are a set of voluntary rules developed by an organization based on the APEC Privacy Principles. An organization then commits to apply these rules to its activities involving transfers of personal information across borders. This system is founded on the principal of accountability. Specifically, businesses must be able to ensure consumers that the information they collect is used in accordance with stated objectives and not misused or misdirected. Consumers must be assured of the fact that their information will not be disclosed without their consent and will be protected by the CBPR system in any APEC member economy. The CBPR system was endorsed by Ministers and Leaders in November 2011 and was a major development in international data protection. The willingness of the Singapore Government to participate in this system is a positive sign of its commitment to honoring data protection principals.