COMMENTS ON THE

THIRD PUBLIC CONSULATION ISSUED BY
MINISTRY OF INFORMATION, COMMUNICATION AND THE ARTS

PROPOSED PERSONAL DATA PROTECTION BILL

SUBMITTED BY:

IBM SINGAPORE PTE. LTD.
9 Changi Business Park Central 1
The IBM Place
Singapore 486048

CONTACT PERSONS:

MS. ERLYNNE ESPENILLA UY
COUNSEL, DATA PROTECTION & PRIVACY OFFICER, IBM ASEAN
+65 6418 1457
erlynne@sg.ibm.com

MR. KIM FATT LAI
CONSULTING GOVERNMENT PROGRAMS LEADER, IBM SINGAPORE
+65 6418 9551
laikf@sg.ibm.com

MS. ANICK FORTIN-COUSENS
MANAGER, GLOBAL PRIVACY & DATA PROTECTION AND PRIVACY OFFICER, GROWTH MARKETS, IBM

MS. HARRIET PEARSON
VICE PRESIDENT, SECURITY COUNSEL & CHIEF PRIVACY OFFICER, IBM CORPORATION

30 APRIL 2012

30 April 2012

Ministry of Information Communication and the Arts
140 Hill Street #02-02
MICA Building
Singapore 179369

Via E-Mail

Re: Proposed Personal Data Protection Bill (the "Bill")

Dear Sir / Madam:

IBM Singapore Pte. Ltd. ("IBM Singapore") welcomes the opportunity to further participate in the consultation undertaken by the Ministry of Information, Communication and the Arts ("MICA") regarding the proposed Personal Data Protection Bill.

IBM and Data Privacy

IBM has been at the forefront of privacy issues for decades. For example, IBM was one of the first companies to create and implement a data privacy policy to govern its internal handling of personal information in the 1970s, and one of the first to appoint a Chief Privacy Officer.[1]

IBM has received many recognitions for its privacy programs over the years. For example, IBM was named one of the most trusted companies for privacy in the US and Canada several years in a row[2], and its privacy programs are pointed to as an example of how Privacy by Design can be implemented by the Ontario Privacy Commissioner.[3]

IBM routinely collaborates with public policy makers, industry, academia and other thought leaders on initiatives to promote privacy and responsible business practices. For example, IBM actively participates in the work of the Asia Pacific Economic Cooperation (APEC) organization, and engages in dialogues in multiple countries around the world aimed at designing sound privacy regulatory frameworks.

We offer our perspective on the draft Bill in our capacity as a data controller who processes personal information of over 400,000 employees world-wide (including a several thousand–person workforce in Singapore) and of tens of thousands of clients, prospective clients and suppliers, as well as in our capacity as a data intermediary (IBM is one of the largest IT and business service providers in the world).

General Comments

We commend MICA for its in-depth work in the area as evidenced by the thoughtful consultation papers and the draft Bill, and for its openness and willingness to collaborate with stakeholders to create a balanced and workable privacy legal framework. We are pleased with the general direction the proposed data protection

---

[1] http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/geneticprivacy/
[2] www.ibmprivacy.com
[3] http://privacybydesign.ca/content/uploads/2011/09/pbd-policy-practice-aug10.pdf

framework is taking, and would like at this time to take advantage of this opportunity to discuss specific areas of the draft Bill that, in our view, require further review.

Specific Comments

(1) Definition of "Personal Data"

The definition of "personal data" under section 2 of the draft Bill appears to be over-reaching, and would nullify the benefits of personal information anonymization or de-identification.

As currently drafted, "personal data" is defined as "data, whether true or not, about an individual who can be identified ... (b) from that data and other information to which the organization is likely to have access".

Organizations will often collect personal information for a given purpose (e.g.. fulfilling an order from a consumer), and strip such data of all identifiers so that it can be used for other purposes (e.g. product development or inventory management). When identifiers are removed, the data being processed is no longer "personal data", but rather mere data. Under the current definition, information stripped of its identifiers would still be considered "personal data", as it is likely that organizations would still have access to the identifiers (e.g. the whole consumer record, including name, will likely be retained in the customer management database of the organization, although it will not be used as part of the organization's inventory management process). As such, it is likely that organizations would no longer go through the additional, privacy-enhancing, step of removing identifiers from data sets, thus lessening the privacy protection afforded to the information.

In light of this, we suggest that subsection (b) be dropped entirely.

(2) Application of the Act

Under subsection 4(2), "Application of Act", we suggest that the words "or other arrangements" be inserted after the words "pursuant to a contract," in recognition of the fact that data controllers and data intermediaries that are part of the same group of companies and that are bound by the same corporate policies do not typically enter into contracts with one another, but rather rely on internal governance structures to ensure that personal information collected by a data controller and processed by a data intermediary is adequately handled by the latter.

(3) Scope of the Draft Bill

Section 5 is, in our view, very complex and over reaching, as it suggests, for example, that the Act will apply to 1) data that was located in Singapore at the time of collection, 2) instances where organizations use personal data in Singapore, and 3) instances where personal information is disclosed in Singapore.

As highlighted in our previous submission, personal data should be subject to the law where the individual to whom it pertains is located, and these local obligations should stay with the data when it is processed in non-home economies. Non-home economies where data is being processed should not add any further or conflicting obligations on the processing of that data. This is one of the principles upon which the APEC Data Privacy Framework was created.

Thus we believe that the draft Bill should apply to organizations that collect and process personal information of individuals located in Singapore.

(4) Accountable Individual

While we agree with the intent of subsection 13(5), we believe that requiring the publication of a specific person's name and contact information may make him or her more susceptible to spam and cyber attacks, not to mention the unnecessary administrative burden having to keep this published information up-to-date would impose on organizations.

We suggest that providing general contact information for the organization be deemed sufficient for the purpose of this subsection.

(5) Consent

A. The draft Bill relies heavily on notice and consent as the mechanism by which individuals will be given control over their personal information, and organizations will be permitted to process personal information.

However, it is now recognized that in some contexts individuals are not capable of exercising meaningful control over personal information via notice and consent mechanisms. In the rapidly-evolving global information economy, while data is still often collected directly from individuals, it is also collected indirectly for example from observation of individuals' behaviors (such as their interactions with others) or from calculations that come from personal data. In such contexts, therefore, it may not be possible to provide notice directly to an individual. In addition, the data processing that may be taking place in certain cases is too complex to describe in the brief and clear format such notice should take in order to be the basis for meaningful consent.

Thus while notice and consent still have a place in modern data privacy laws, and should be sought where possible and effective, any modern data privacy law needs to recognize that where consent is not possible or effective, business should still be able to process personal information for legitimate business purposes provided that such organizations implement measures to protect personal information against risks to the individuals and remain answerable for the integrity of the risk assessments and mitigation measures they perform and implement.

B. We support section 17, which explicitly recognizes that implied or deemed consent is a valid form of consent, as it is in line with individuals' expectations and today's business practices.

We would suggest, however, that a forrmal recognition that consent can be inferred from the action of individuals be added to this section. For example, when an individual posts messages on a Web site that is publicly available (such as Twitter) for the world to read, organizations should be able to collect and use this data (assuming other legal obligations—such as intellectual property or contractual restrictions--are met) by inferring consent based on the actions of the individual.

C.We suggest that subsection 16(2) does not recognize the reality of today's Internet, in which products and services are provided free of charge to individuals in exchange for personal data (e.g. social media sites such as Facebook, loyalty programs). Therefore we believe that this section should be removed.

(6) Care of Personal Data

We strongly support MICA's approach to accountability: data controllers should indeed remain responsible for complying with data protection laws, whether they perform this processing in-house, or whether they entrust this processing to data intermediaries. Data controllers should, in light of the obligations imposed to them by applicable law, provide direction to data intermediaries regarding the manner in which the latter must process personal data entrusted to them (e.g. which type of personal information may be collected, how this information may be used, to whom it may be disclosed, how it is to be protected, when it must be returned or disposed of). Data intermediaries should act consistently with the instructions of their clients, i.e. the data controllers.

However, we do not agree that data intermediaries should be jointly responsible with data controllers for determining the security measures to be applied to the information. Blurring the lines of responsibility and accountability between the parties will only lead to confusion and poorer outcomes for individuals' data security. A data controllers should, as with all other provisions of the draft Bill, bear the ultimate responsibility for data security, and in turn seek to ensure itself that its intermediaries protect the data in accordance with its instructions.

(7) Offences and Penalties

A. We do not support the measure contemplated in subsection 31(1)(d) as written, as it would give the Commission absolute discretion to impose fines.

In our view, decisions of the Commission in that regard should be tempered by the checks and balances of a judicial or other appropriate review. In addition, we submit that the proceeds of any fines levied be used to support beneficial activities, but preferably not be used to fund directly the agency responsible for such enforcement, in order to maintain the separation of duties and authorities essential to maintain a high level of trust in the government.

B. The penalties under section 35 are disproportionately severe. We suggest that penalties should be directly proportional to the harm suffered by the individual affected and to the seriousness of the offence. Imprisonment should be reserved for criminal cases such as where an individual commits fraud or identity theft.

CONCLUSION

IBM Singapore would like to thank MICA and the Economic Development Board of Singapore for the opportunity to share its views on the proposed Bill and hold in-person consultations to further refine the draft Bill. We remain available to answer any questions you may have with respect to the substantive points made in this submission, or to assist you otherwise.

Sincerely yours,

Kim Fatt Lai
Consulting Government Programs Leader
Singapore
+65 6418 9551
laikf@sg.ibm.com