MINISTRY OF INFORMATION, COMMUNICATIONS AND THE ARTS

PUBLIC CONSULTATION ON PROPOSED PERSONAL DATA PROTECTION BILL

COMMENTS OF RESEARCH IN MOTION LIMITED

30 APRIL 2012

TABLE OF CONTENTS

1.0 INTRODUCTION

Research In Motion Limited (RIM) is pleased to offer the following comments in response to the Ministry of Information, Communications and the Arts' ("MICA") Public Consultation on the Proposed Personal Data Protection Bill ("PDPB"). In addition to addressing some of the specific provisions of the proposed PDPB, this submission elaborates on some of the themes raised in our earlier submission to MICA, dated 24 October 2011.

This consultation comes at a critical juncture for Singapore's digital communications industries. Customer demands are changing, technologies are converging, competition is intensifying, and telecommunications networks are becoming increasingly global. In this environment, Singapore needs a solid legislative and regulatory framework to protect the privacy of its citizens while strengthening Singapore's position as a trusted hub for global telecommunications and digital industries.

2.0 RIM'S APPROACH TO PRIVACY AND DATA PROTECTION

RIM has a long history of providing secure and privacy-enhanced mobile communications and we are encouraged by the development of new data protection legislation in many countries like Singapore. While data protection legislation must establish rules around personal data practices that recognize the individual's right to privacy and demonstrate respect for their personal information, it must at the same time recognize and balance the need for organisations to collect, use or disclose that information for reasonable business purposes. This focus on balance is important; principle-based data protection legislation will allow technology driven companies to thrive while at the same time improve and strengthen privacy protection for individuals.

As a Canadian-headquartered company operating globally, RIM has benefited from Canada's private sector privacy legislation, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"). PIPEDA is a principle-based, technology-neutral data protection law that was first enacted in January 2001 for federal undertakings within industries such as banking and telecommunications, and then more broadly in January 2004 for industry generally. In large part due to PIPEDA, Canada has been recognized as a leader in global commerce and transborder data flows of personal information. Canada's privacy framework has been recognized by the European Union as providing adequate privacy protections and is therefore granted special provision for transborder data flows from the EU to Canada. RIM believes that PIPEDA has helped define how we incorporate consumer trust in the design of our products. Consumers are comfortable with new technologies if they are confident their personal data is adequately protected via the features and tools built into the products and services they use.

Based on our detailed review of the proposed PDPB, it appears that MICA has concluded that a similar principled-based approach to data protection legislation will benefit Singapore and

enhance its competitiveness as a trusted hub for global data management and processing services. We welcome this approach and believe that the technology-neutral and principle-based approach to data protection set out in the proposed PDPB will make the Singapore data protection regime a model for other forward-looking jurisdictions.

3.0 RECOMMENDED CHANGES AND ADDITIONS TO THE PROPOSED PDPB

RIM believes that the proposed PDPB is fundamentally sound. It provides solid protections for personal data of all individuals that is collected, used or disclosed by organisations within Singapore, while enhancing Singapore's position as a commercial hub for global data management. RIM does not believe that major change is needed to the legislative text. Based on our experience with PIPEDA, we have outlined our suggestions and comments below, which are intended as minor, in order to further improve and clarify the legislative text.

3.1 Scope and Coverage of the Proposed PDPB

We believe that the scope and coverage of the proposed PDPB is balanced and fundamentally sound. In particular, we agree that the proposed PDPB should not prescribe a fixed or "hardwired" list of personal data that should be protected. Also, we agree that it should apply to all private sector organisations, including small companies that have low annual turnover, to ensure a minimum standard of data protection across the private sector. We have provided some minor suggestions to ensure that the proposed PDPB achieves MICA's stated objectives and does not result in unintended consequences.

3.1.1 Definition of Personal Data

In our previous submission, we suggested that the Data Protection framework include the notion of "anonymous" data. The proposed definition of personal data does not make a direct reference to anonymized or aggregated data, but states that the data must be "about an individual who can be identified." While this definition is likely to be interpreted as excluding anonymized and aggregated data, we believe that it would be beneficial to have greater clarity. The use of anonymous or aggregate data to develop or improve products and services for customers is important to industry, especially in the ever changing and evolving online and mobile environment where different business models drive innovation. Also, such a clear statement would temper an increasingly aggressive position that is negatively impacting the ongoing ability of organisations to collect, use or disclose anonymous or aggregate data. We recommend a direct statement that anonymous and aggregated data are not considered personal data.

Also, we note that MICA is proposing that certain prescribed categories of publicly available data be excluded from the scope of the PDPB, similar to what is provided for in PIPEDA. We

agree with this approach and suggest that it be incorporated into the definition of personal data. We suggest language such as:

> *2. In this Act, unless the context otherwise requires —*
> *(…)*
> ***"anonymous or aggregated data" means data that cannot alone or together with other information to which the organisation is likely to have access identify an individual given the means that may be reasonably used by the organisation or any other person and without the need for disproportionate efforts;***
> *(…)*
> *"personal data" means data, whether true or not, about an individual who can be identified —*
> *(a) from that data; or*
> *(b) from that data and other information to which the organisation is likely to have access* ***without the need for disproportionate efforts****;*
> ***and excludes —***
> ***(a) anonymized or aggregated data; and***
> ***(b) data that is publicly available and is specified by the regulations;***

3.1.2 Power to Exempt Organisations

In order to protect the privacy of all individuals in Singapore, no private sector organisations should be exempted from the proposed PDPB, other than common exclusions such as for journalistic or personal purposes. While in certain sectors there may be an ongoing public policy need to have sector-specific rules, such instances should be kept to a minimum. This would limit consumer confusion as to expected standards and avoid unnecessary duplication of regulation for the private sector which can lead to increased costs and potential inconsistent approaches between regulators.

A well crafted data protection framework should be able to meet the needs of the majority of industries within the private sector. For those sectors where additional guidance may be required given the sensitivity of personal data involved, the Data Protection Commission ("DPC" or "Commission") can issue guidelines developed in conjunction with the affected sector and civil society as appropriate. For those instances where separate sector-specific rules continue to be deemed necessary, the DPC should work closely with such regulators to ensure a consistent approach is followed.

In this regard we find the wording of section 60 regarding Power to Exempt somewhat problematic. This is quite a unique power for data protection legislation as it allows for the exemption of not only a class of organisations, but of particular organisations. We have similar concerns around subsection 63(3) regarding Regulation Making Powers.

We believe that it may be more appropriate to re-word these sections to enable the Commission and the Minister to exempt only classes of organisations and not specific organisations to ensure the broadest application of the PDPB and competitive parity across organisations belonging to the same class and industry more broadly. We suggest the following language:

> ***60.*** *The Commission may, with the approval of the Minister, by order, exempt* ~~***any person or organisation or***~~ *any class of persons or organisations from all or any of the provisions of this Act, subject to such terms or conditions as may be specified in the order.*
>
> ***63.****—(1) The Minister may make such regulations as may be necessary or expedient for carrying out the purposes and provisions of this Act and for prescribing anything that may be required or authorised to be prescribed by this Act.*
> *(2) Without prejudice to the generality of subsection (1), the Minister may make regulations for or with respect to all or any of 30 the following matters:*
> *(…)*
> *(3) A regulation made under this section may provide differently for different* ~~***organisations, individuals,***~~ *classes of organisations or classes of individuals.*

3.2 Data Protection Rules and Exclusions

Generally speaking, we believe that the rules and exclusions of the proposed PDPB are in line with internationally accepted privacy best practices and that major changes are not needed. Our comments below are intended as minor suggestions, rather than wholesale changes.

3.2.1 Data Intermediaries

RIM welcomes MICA's decision to exclude "data intermediaries" from the scope of the general rules on protection of personal data, as well as the obligations with respect to the collection, use, disclosure, access and correction, and accuracy and retention of personal data. We believe that this approach is consistent with generally accepted international privacy norms, will reduce compliance costs for data intermediaries and create incentives for these organisations to choose Singapore as their home base.

We note, however, that the proposed exclusion in the PDPB would be limited to personal data processed by data intermediaries "pursuant to a contract which is evidenced or made in writing." In our view, while the use of a contract in such cases is usually standard practice, the PDPB should reflect the possibility that "other means" could be used to achieve the same result (e.g. non-contractual oversight, audit mechanisms). In certain circumstances, the requirement to have a formal contract could be unnecessary and unduly restrictive, imposing unnecessary

burdens on not only data intermediaries but the organisations on whose behalf they are processing personal data that do not operate with such contracts, without giving additional protections to personal data.

RIM considers that the wording adopted in Principle 4.1.3 of Schedule 1 in PIPEDA, which refers to the use of "contractual or other means to provide a comparable level of protection while the information is being processed by a third party," provides additional flexibility to data intermediaries yet ensures sufficient safeguards for personal data. Accordingly, we recommend that subsection 4(2) of the proposed PDPB be modified to specify that a data intermediary may use other means to provide comparable levels of protection to the personal data as follows:

> *(2) Parts III to VI (except for section 26 (Protection of personal data)) shall not impose any obligation on a data intermediary in respect of personal data processed by the data intermediary on behalf of another organisation* ~~***pursuant to a contract which is evidenced or made in writing***~~ ***provided that the other organisation uses contractual or other means to provide a comparable level of protection while the data is being processed by the data intermediary****.*

RIM believes that this modification would provide additional flexibility for organisations and data intermediaries, without sacrificing the level of protection given to the data processed by the data intermediary.

3.2.2 Designation of Organisation's Representative

Accountability has been the cornerstone of Canada's private sector privacy framework for over a decade and has become a critical component of modern privacy and data protection legislation. The designation of an individual or individuals responsible for an organisation's data protection compliance is an important part of any effective accountability framework.

RIM considers that the adoption of the PDPB in Singapore would promote greater accountability amongst organisations handling personal data. However, we believe that the wording of section 13 could be modified to provide greater flexibility for organisations. In our view, organisations should not have to make available business contact information for "each individual designated … or delegated" as this could become quite burdensome in larger organisations, and especially those operating in multiple jurisdictions. There is a difference between making available information about the designated individual within an organisation who is responsible for ensuring the organisation's compliance, other employees who will assist in that role, and a contact to whom the public can reach out. Organisations that have several employees involved in data protection matters should have the flexibility to determine an appropriate contact person (or persons) to manage public inquiries, complaints and access requests depending on their business and organisational structure. The appropriate contact person may vary depending on the circumstances or as the organisation's staffing changes.

We believe that section 13 should be slightly modified to allow organisations to provide contact information for a "Privacy Office" or "Data Protection Department," rather than requiring the public dissemination of a specific person's contact information. Hence, RIM recommends that sections 13 be modified as follows:

> ***13.***—*(1) In meeting its responsibilities under this Act, an organisation shall consider what a reasonable person would consider appropriate in the circumstances.*
> *(2) An organisation is responsible for personal data in its custody or under its control.*
> *(3) An organisation shall designate one or more individuals to be responsible for ensuring that the organisation complies with this Act.* ***Upon request, the identity of the designated individual or individuals shall be made known.***
> *(4)* ***Other individuals within the organisation may be delegated to act on behalf of the designated individual or individuals.*** ~~*An individual designated under subsection (3) may delegate to another individual the duty conferred by that designation.*~~
> *(5) An organisation shall make available to the public the* ***name or title, and the address, to whom inquiries or complaints can be directed.*** ~~*business contact information of each individual designated under subsection (3) or delegated under subsection (4).*~~

3.2.3 Access to Personal Data

Access to personal data is an important component of modern data protection legislation and we applaud MICA for recognizing this. We would however recommend minor changes to the wording of section 23. We recommend that section 23 be amended to: "provide the individual with ***access to***… the individual's personal data." As it reads now, it appears that organisations are required to provide a physical copy of an individual's personal data in each and every case. The language in PIPEDA, for example, makes it reasonable for organisations to provide access to personal data without actually providing a copy, depending on the circumstances. For example, in some cases it may make more sense to provide an opportunity for an individual to listen to a phone call recording or view a video given the medium and potential need to protect the privacy of others involved.

Hence, RIM recommends that subsection 13(5) be modified as follows:

> ***23.***—*(1) Subject to subsections (2) to (4), on request of an individual, an organisation shall, as soon as reasonably possible, provide the individual with* ***access to*** *—*
> *(a) the individual's personal data in the custody or under the control of the organisation;*

(b) information about the ways in which the personal data referred to in paragraph (a) has been or may have been used by the organisation; and
(c) in addition, if the organisation is a credit bureau, the sources from which it received the personal data unless it is reasonable to assume the individual can ascertain those sources.

We also agree that an organisation should have the ability to deny access to personal data in situations where the individual is under investigation. We therefore prefer the alternative wording suggested by MICA in subsection 1(h) of the Sixth Schedule.

3.2.4 Business Asset Transactions

Paragraph 2(3)(c) of the Third Schedule and paragraph 4(3) of the Fifth Schedule "require that, in the event of a transfer of assets from one organisation to another, the employees, customers, directors, officers and shareholders whose personal data is being disclosed to the other organisation must be notified that the business asset transaction has taken place and that the personal data about them has been disclosed to the organisation." While we agree that this requirement is reasonable in the majority of cases, we would like to note that, in certain scenarios, the parties to a business asset transaction may legitimately decide for business reasons not to make an acquisition or sale public (i.e. keep the transaction confidential). This is particularly relevant in some situations where neither the acquirer nor the acquisition target is a publicly listed company. In our view, the PDPB should recognize this type of business transaction by including an exception to the obligation to notify employees/customers/directors/officers/shareholders. We also believe that it would be appropriate to require an organisation relying on this exception to use the data only for the purpose for which it was collected by the original organisation.

Hence, RIM recommends that the Third Schedule and the Fifth Schedule be modified as follows:

Third Schedule paragraph 2:

(3) If the organisation enters into the business asset transaction with the other organisation —
(a) the organisation shall only use or disclose the personal data collected for the same purposes for which the other organisation would have been permitted to use or disclose the data;
(b) if any of the personal data collected does not relate directly to the part of the other organisation or its business assets with which the business asset transaction entered into is concerned, the organisation shall destroy, or return to the other organisation, any such personal data; and
(c) ***any individual, including*** *the employees, customers, directors, officers and shareholders****,*** *whose personal data is disclosed shall be notified* ***by one of the parties***

within a reasonable time after the business asset transaction has been completed *that —*

(i) the business asset transaction has taken place; and
(ii) the personal data about them has been disclosed to the organisation;

Fifth Schedule paragraph 4:

(3) If the organisation enters into the business asset transaction, ***any individual, including*** *the employees, customers, directors, officers and shareholders, whose personal data is disclosed shall be notified* ***by one of the parties within a reasonable time after the business asset transaction has been completed*** *that —*
(a) the business asset transaction has taken place; and
(b) the personal data about them has been disclosed to the party.
(4) In paragraph 1(s) and this paragraph, —
"business asset transaction" means the purchase, sale, lease, merger or amalgamation or any other acquisition, disposal or financing of an organisation or a portion of an organisation or of any of the business or assets of an organisation other than the personal data to be disclosed under paragraph 1(s);
"party" means another organisation that enters the business asset transaction with the organisation.

3.3 Implementation Framework

We believe that the implementation framework proposed by MICA is reasonable. However, we have a few minor recommendations regarding offences, penalties and the appeal mechanism.

3.3.1 Financial Penalties

RIM is generally opposed to calls for increased powers of data protection authorities and the ability to levy significant fines or penalties beyond the awarding of damages for harm suffered. We believe that these fines or penalties will have important unintended consequences. For example, in the face of such significant powers and exposure to significant fines or penalties, organisations are often deterred from being open and transparent with data protection authorities. We also find that issuing fines in this regard may have no bearing on the issue at hand which is the protection of individuals. Should fines be available, they should be levied only in egregious cases of harm or in cases where systemic failures to comply with certain key requirements have occurred, and not be seen as a way to generate revenues.

If the Singapore government decides to create financial penalties in the PDPB, RIM believes that the penalties should seek to serve two purposes: i) to compensate individuals for the harm they may have suffered as a result of an organisation's non-compliance with its data protection

obligations; and ii) to afford the Data Protection Commission ("Commission") the necessary powers to enforce the PDPB. We recommend that the imposition of these penalties be determined based on specific criteria outlined explicitly in the PDPB.

Accordingly, we recommend that section 31 of the PDPB be modified to specify the criteria to be considered by the Commission when imposing these penalties. In particular, we recommend that section 31 be modified as follows:

> ***31.***—*(1) The Commission may, if it is satisfied that an organisation is not complying with any provision in Part III to Part VI, give the organisation such directions as the Commission thinks fit in the circumstances to ensure compliance with that provision.*
> *(2) Without prejudice to the generality of subsection (1), the Commission may, if it thinks fit in the circumstances to ensure compliance with this Act, direct the organisation —*
> *(a) to stop collecting, using or disclosing personal data in contravention of this Act;*
> *(b) to destroy personal data collected in contravention of this Act; and*
> *(c) to comply with any other direction of the Commission under section 30(2); and*
> *(d) to pay a financial penalty of such amount not exceeding $1 million as the Commission thinks fit.*
> *(3) Subsection (2)(d) shall not apply in relation to any failure to comply with a provision of this Act the breach of which is an offence under this Act.*
> ***(4) In assessing the amount of financial penalty under subsection (2)(d), the Commission shall consider –***
> ***(a) whether the organisation has implemented measures in good faith to comply with Part III to Part VI;***
> ***(b) the nature and scope of the failure;***
> ***(c) whether the failure was within the organisation's reasonable ability to control;***
> ***(d) the organisation's history with respect to any other failures to comply with any provision in Part III to Part VI ; and***
> ***(e) the need to deter other failures to comply with any provision in Part III to Part VI.***

3.3.2 Offences and Penalties

Similarly, with respect to offences and penalties, we believe that the PDPB should reserve these actions for behavior that is most egregious, such as intentionally deleting personal data that is the subject of an access request or impeding an investigation by the Commission, and that other matters of non-compliance regarding collection, use and disclosure are best left to the broad powers of the Commission and its ability to levy fines. Such an approach would be consistent with PIPEDA in Canada.

Accordingly, we recommend that section 35 be modified as follows:

> ***35.***—*(1) An organisation or person commits an offence if the organisation or person —*
> ~~*(a) willfully collects, uses or discloses personal data in contravention of this Act;*~~
> *(b) with an intent to evade a request under section 23, disposes of, alters, falsifies, conceals or destroys, or directs another person to dispose of, alter, falsify, conceal or destroy, a record containing —*
> *(i) personal data; or*
> *(ii) information about the use or disclosure of personal data;*
> *(c) obstructs the Commission or an authorised officer in the performance of their duties or powers under this Act; or*
> *(d) knowingly or recklessly makes a false statement to the Commission, or knowingly misleads or attempts to mislead the Commission, in the course of the performance of the duties or powers of the Commission under this Act.*
> *(2) An organisation or person that commits an offence under subsection (1)(a) or (b) is liable —*
> *(a) if an individual, to a fine not exceeding $5,000; and*
> *(b) in any other case, to a fine not exceeding $50,000.*
> *(3) An organisation or person that commits an offence under subsection (1)(c) or (d) is liable —*
> *(a) if an individual, to a fine not exceeding $10,000 or to imprisonment for a term not exceeding 12 months or to both; and*
> *(b) in any other case, to a fine not exceeding $100,000.*

3.3.3 Appeal Mechanism

With regard to sections 37-38, RIM believes that there should be a way for an organisation to request a stay of the decision or direction while an appeal is ongoing. Being required to comply while an appeal takes place could have significant consequences for an organisation's business operations (especially if complying with the Commission's decision is irreversible, e.g. disclosure of information). We do not suggest that a stay be automatic, but recommend that there be a process to request one.

As well, it is unclear whether this appeal process represents a true "appeal," where the appellate body reviews only the legal basis for the decision and does not have the ability to review the factual basis for the decision or whether it is a "trial de novo," similar to what is outlined in PIPEDA, where the appellate body can review both the factual and the legal basis of the decision. As it currently reads, it appears to be the latter; however this mechanism is often incompatible with a scenario where the DPA has order making powers.

Additionally, RIM believes that MICA should consider giving the Commission the authority to review and vary its own decisions upon receipt of an application for review by an organisation, prior to initiating the formal appeals process. The opportunity to apply for reconsideration of a Commission direction or decision would be most appropriate if new or undiscovered facts come to light. We believe this could offer a more efficient and streamlined process than moving directly to the appeals process which, by its nature, will be time consuming and potentially onerous for all parties. In such circumstances, the Commission would develop appropriate procedures for handling reconsideration applications, in accordance with the rule-making power set out in subsection 6(6) of the First Schedule.

Accordingly, we recommend that a new section be added between sections 37 and 38 with the following language:

> ***Any organisation aggrieved by any direction or decision made by the Commission may, within fourteen days of the receipt of the direction or decision, apply in the prescribed manner to the Commission for a reconsideration of that direction or decision.***

4.0 CONCLUSION

We applaud and support the approach articulated in the proposed PDPB and urge MICA to continue its work to strike the right balance between protecting individuals' privacy and legitimate business needs. We believe that Singapore's digital economy is reliant upon strong data protection and requires modern public policies and programs that keep its economy globally competitive. This will ensure the further development of existing Singapore companies and will lay the foundation for future companies yet to be launched.

We believe that our comments and specific suggestions outlined above will assist MICA in improving opportunities for technical innovation and will strengthen Singapore's global standing in this important area of privacy and data protection. We welcome the opportunity to continue this dialogue with MICA and other stakeholders.