Australian
Privacy
Foundation

Submission by the Australian Privacy Foundation to the Singapore Ministry of Information, Communications, and the Arts (MICA) in relation to Singapore's Public Consultation on the Proposed Personal Data Protection Bill

April 2012

For further information, contact:

Dr Dan Svantesson

Vice Chair, Australian Privacy Foundation

dasvante@bond.edu.au

Table of Content

1. Summary of major points

In the view of the Australian Privacy Foundation's International Committee:

- Several aspects of the Bill would benefit from further work and clarification;
- Individuals acting in a personal or domestic capacity should be subject to an abuse regulation, not just be completely exempt;
- The Commission ought to provide training opportunities, and other forms of guidance, for those individuals that are designated as being responsible for the data protection compliance within an organisation;
- The Commission is not structured so as to be sufficiently independent;
- Organisation should typically be required to destroy its documents containing personal data upon the express request of the data subject;
- The right to private action is a major feature of the Bill;
- The proposal fails to adequately address the complexity of transborder data flows; and
- The proposed maximum financial penalty of $ 1 million may be insufficient to deter all sorts of data breaches.

2. Comments

The Australian Privacy Foundation (www.privacy.org.au], through its International Committee[1], welcomes the initiative taken by the Singapore Ministry of Information, Communications, and the Arts in moving to a level of serious consideration of privacy protection.

Several important steps are taken in the proposal, and the introduction of a data protection scheme stands to have several benefits for Singapore; including increased consumer confidence, and economic benefits in the form of a strengthening of Singapore's already prominent position as an international business hub.

The proposed regime nevertheless falls well short of international best practice in some areas and further work is called for.

Due to resource limitations, we have only been able to focus on a limited number of aspects of the proposed Bill. Our silence on other aspects of the Bill should not be seen as endorsement of those aspects.

2.1 Section 2

The proposal introduces the interesting concept of "data intermediary". This is an important step as the traditional distinction between "data controllers" and "data processors" is too simplistic. Having said that, neither the Bill, nor the discussion paper makes sufficiently clear the difference between data intermediaries and data processors. There is consequently scope for greater clarity in this regard.

The definition of "personal data" could also be clarified. For example, a question that still plagues several of the countries with long traditions of privacy protection is whether the test for identifiability refers to the data in the hands of the sender or in the hands of the receiver. Imagine that organisation A discloses data to organisation B. Imagine further that organisation A cannot identify any individual based on the data, but knows that organisation B can identify individuals based on the data. Does that constitute disclosure of personal data? After all the data is not personal when sent, only when received, but the sender know that the data will be personal once received.

[1] The APF International Committee is made up of internationally recognised privacy experts Chris Connolly, Roger Clarke, Graham Greenleaf, Dan Svantesson, David Vaile and Nigel Waters – see http://www.privacy.org.au/About/Contacts.html#Officers.

2.2 Section 4

Section 4 excludes individuals acting in a personal or domestic capacity from the scope of the privacy regulation. Most countries with data protection in place have similar exemptions in place in some form. However, at the same the newspapers are full of stories showcasing the devastating privacy violations individuals engage in a personal or domestic capacity (e.g. through postings on social media sites).

Consequently, an exemption is not satisfactory unless backed up by some form of regulation covering individuals in a personal or domestic capacity. The Swedish abuse regulation may serve as a useful source of inspiration in this context.

2.3 Section 5

Section 5 gives an extraterritorial scope to the regulation. This is similar to how the proposed EU Regulation provides for extraterritoriality. Thus, this approach is in line with current international developments. At the same time, the difficulties of drawing a line between an effective protection of the rights of the people of Singapore, and an exaggerated grab for jurisdiction are well recognised.

Some parts of Section 5 would benefit from further clarification. For example, it is not immediately clear when disclosure takes place “in Singapore” or when an organisation uses personal data “in Singapore”.

It should also be noted here that these extraterritoriality provisions do not overcome the need for data export restrictions, as is recognised in the proposed EU Regulation.

2.4 Sections 6-12

The inclusion of a Data Protection Commission (DPC) is supported strongly, as are the broad powers to enforce the Act that it is to be given. However, this data protection authority is one with no independence, because its members can be sacked with no reason required. This will almost certainly mean that the DPC would be refused accreditation to the global conference of data protection authorities (DPPCC), as was the South Korean applicant (a Ministry) in 2011 because of its lack of independence from government[2]. Because APPA (Asia Pacific Privacy Authorities) uses the same accreditation standards as the DPPCC, this should mean that the DPC will even be refused accreditation to the regional body of DPAs.

[2] Recent decisions of the European Court of Justice concerning German DPAs have also taken a strong approach toward the requirement of independence in the European context.

This would be a loss to Singapore, to the global development of data protection, and to the regional body, and would be particularly unfortunate given the other good aspects of the proposal concerning the DPA. We submit that it would be highly desirable for the DPC provisions to be brought up to international standards concerning independence.

We note that the provision of an appeal right to the Data Protection Appeal Committee (and thence on some grounds to the courts) does provide one of the indicia of independence of a DPA, but we strongly doubt this would be sufficient.

2.5 Section 13

For the reasons discussed in the discussion paper, requiring organisations to designate one or more individuals as being responsible for the data protection compliance is a good idea. Perhaps Section 7 could include an obligation for the Commission to provide training opportunities, and other forms of guidance, for those individuals that are so designated.

2.6 Sections 15-19

Sections 15 to 19 regulate consent. While a common feature of data protection law around the globe, it must always be remembered that the concept of consent is weak indeed, not to say dangerous. From the perspective of the data controller it is often difficult to assess whether valid consent has been provided, and from the perspective of data subjects, the quality of the consent they provide is not always high as it typically is uninformed and given in a 'take it or leave it' setting.

Turning to Section 16(2) specifically, there is no doubt that the issue it seeks to address is an important one, and that its aim – of ensuring that consent is not required to get access to the product or service unless reasonable – is commendable. Our concern relates to how it will be applied on a practical level.

Imagine that a consumer, when seeking to download a game onto his or her smart phone, is asked to consent to the application collecting his or her location, phone call history and so on. Imagine further that such information has no bearing on the game as such and that the only reason the app providers seeks consent to the data collection is that it profits from that data. Read strictly, Section 16(2) would seem to suggest that such consent would not be valid. However, the consequence of such a conclusion may be that the app provider cannot supply the app free of charge. On the other hand, if the app provider's financial interest in getting access to the data in question counts as a reasonable ground for seeking the consent, then Section 16(2) loses its value completely.

Also Section 16(3) – addressing unfair conduct in connection with obtaining consent – is valuable and commendable. However, it seems the only consequence of such deplorable conduct is that the consent is invalid. We argue that there should also be penalties attached to such conduct.

2.7 Section 27

Section 27(2) outlines the circumstances under which an organisation must destroy its documents containing personal data. We suggest that a third ground should be added; that is, in most circumstances it is reasonable to require that an organisation destroys its documents containing personal data upon the express request of the data subject.

2.8 Section 36

We commend the inclusion of a right to private action. Such a right has several obvious benefits as discussed in the discussions paper, and as we have argued in the Australian context.

2.9 Transborder data flows

Perhaps the most serious weakness in the proposal is how it fails to adequately address the complexity of transborder data flows. Simply requiring organisations to secure a "comparable level of protection for data transferred outside Singapore" seriously undermines the entire regulation. A much stronger and more considered approach is needed.

The Public Consultation Paper states that 'MICA proposes to require that organisations comply with the PDPA regardless of where the personal data is transferred', but we cannot see any provisions in the draft Bill that would ensure this in practice, where the recipient of the data is effectively outside Singapore's jurisdiction (though perhaps not in theory because of section 5) and is not an entity related to the transferor (where the agency provisions might apply). In such cases neither transferor nor transferee seem to have any effective liability for a subsequent breach unless the transferee puts itself within reach of the enforcement provisions of Singaporean law. We submit that this is too weak a protection, and that, if this approach is to be taken, the transferee should remain liable for any breaches (analogous to the vicarious liability for actions of an overseas agent, already provided for in the draft Bill).

2.10 Other issues

We welcome the decision to have the data protection scheme apply also to small businesses. Australia should serve as a warning as to what happens when focus is placed only on regulating major companies.

The proposed maximum financial penalty of $ 1 million may be insufficient to deter all sorts of data breaches.

3. Conclusion

The Proposed Personal Data Protection Bill is an important addition to Singaporean law and stand to benefit Singapore in several ways. We appreciate the opportunity to provide input on the final direction of the Bill and hope our contribution can help improve the Bill further so as to give the population of Singapore world leading data protection.