1 April 2013

Chairman
Personal Data Protection Commission
Singapore

Dear Sir,

Symantec Submission to the Proposed Advisory Guidelines on Key Concepts in the Personal Data Protection Act
By the Personal Data Protection Commission, Singapore

Symantec is a global leader in providing security, storage and systems management solutions to help our customers – from consumers and small businesses to the largest global organizations – secure and manage their information and identities independent of device. Symantec does this by bringing together leading software and cloud solutions that work seamlessly across multiple platforms, giving customers the freedom to use the devices of their choice and to access, store and transmit information anytime, anywhere.

Globally, Symantec has also actively worked with a number of Governments on data privacy legislations, with the following notable examples:

- The ePrivacy directive in the EU, and
- The ongoing discussion on the review of the General Data Protection Directive

Symantec welcomes the publication of the Proposed Advisory Guidelines on Key Concepts in the Personal Data Protection Act by the Personal Data Protection Commission of Singapore. With the landmark enactment of the Personal Data Protection Act in Singapore, Symantec sees the Advisory Guidelines as a key document in educating organisations and individuals in Singapore as to their rights and responsibilities under the Act.

Symantec would like to thank the Commission for the opportunity to provide feedback on the proposed Advisory Guidelines. We would be happy to provide more information or any clarifications needed on any of the points raised in this paper. Please direct these queries to the undersigned.

Best Regards,

Ng Kai Koon
Senior Manager, Government Affairs
kaikoon_ng@symantec.com

Symantec.

Symantec Submission to the Proposed Advisory Guidelines on Key Concepts in the Personal Data Protection Act By the Personal Data Protection Commission, Singapore

Summary

The recently enacted Personal Data Protection Act (PDPA) has given Singapore a comprehensive data privacy framework which balances the rights of individuals and the needs of businesses to be able to collect and process data. This is timely in light of a rapidly transforming industry that is harnessing data to power a digital economy. However, it is also apparent that there exist some gaps in the legislation. While it is recognized that the Proposed Advisory Guidelines are not meant to supplement nor modify the PDPA, it is suggested that addressing these within the Guidelines will promote a set of best practices for organisations taking their first steps towards a data privacy regime. It should be noted that the following are part of data privacy legislation in jurisdictions like the European Union and Australia.

Right of Erasure

Within the legislation, there are clear requirements for the collection, use and disclosure of personal data through the provision of consent by the individual. It also allows for the withdrawal of consent by the individual, upon which, the organisation (and its intermediaries and agents) would have to cease collection, use and disclosure of the individual's personal data. However, there is no requirement for the organisation to delete the data from their records in the case of withdrawal of consent. This can create a scenario where a company is holding the personal data of individuals whose consent to use the data the organisation no longer have. This increases the impact of a security breach in terms of the data lost, as well as the risk of the data being used accidentally in breach of the PDPA.

It is suggested that the guidelines could include the advice that upon the receipt of a withdrawal of consent, the organisation should also delete the record.

Data Loss in Security Breach

In the Internet Security Threat Report published by Symantec in April 2012, it was reported that 232 million identities were stolen as a result of security breaches in 2011. On average, each breach had resulted in the loss of 1.1 million identities. In these breaches, 33% had resulted in the loss of the names, addresses and credit card numbers of the affected individuals. While these numbers reflect a global reality, the truth is that Singapore is not sheltered from these attacks and in an increasing globally connected economy, it is expected that Singaporeans will come under greater threat from the loss of personal data in security breaches.

Typically, data protection legislation is effective in addressing the complete life cycle of data, from collection, to processing, to storage, and deletion. However, in many jurisdictions, there exists a gap where the circumstance of data being lost or stolen is not addressed. Increasingly, we are seeing these jurisdictions explore the introduction of mandatory breach notification laws to ensure that in the event of loss of personal data by organisations, customers who are impacted are informed such that appropriate remediation steps are taken.

Symantec recognize that MCI has explored this issue at length and decided that mandatory data breach notification should not be introduced into the legislation at this time. However, it is our recommendation that in a document aimed at educating individuals and organisations of their rights and obligations under the PDPA, it would be important to offer concrete steps that organisations should take in the event of data loss. Symantec would suggest that PDPC could take a leadership role in helping to define a framework, through the Proposed Advisory Guidelines, in helping companies determine the need to notify affected consumers of security breaches which has resulted in the loss of data.

In proposing such a framework, Symantec would caution the Commission in that while an extreme of no notification would not be helpful, the other extreme of requiring all companies declare all breaches (including trivial ones) can also result in 'notification fatigue' which has an undesired side effect of desensitizing the public to breach notifications, and in the worst case, create unnecessary mistrust of online systems.

Symantec would thus suggest the adoption of a harm analysis-based threshold. This would be much more effective in helping organisations determine the seriousness of the breach as it takes into consideration the type of data lost, and its impact. Methodologies solely based on number of records lost will not be as effective as numbers may sometime downplay the high impact a data breach may have on a group of consumers.

In considering the harm threshold, consideration should be given to the following factors.

- Risk of physical harm to the customer,
- Risk of identity theft or fraud,
- Risk of harm to reputation of the customer,
- Number of customers affected,
- Level of financial impact, and
- Risk to information security of other systems.

Symantec would propose a 'safe harbor' provision, where organisations which can demonstrate that there are adequate technical security measures to protect the lost data (such as encryption or similar technologies which would render the stolen data unintelligible) need not notify customers of data loss. This would be consistent with the above principles, since the risks above would be alleviated. It should be noted that this approach is adopted by the EU ePrivacy Directive, and are currently part of the discussion on the review of the General Data Protection Directive in the EU.

Conclusion

Given the nascent field of data protection in Singapore, Symantec believes that the proposed Guidelines will be an important tool for organisations and individuals to better understand their rights and obligations under the PDPA. This is particularly the case for domestic companies who would need to start building a world class data protection framework, which will stand them in good stead as they expand overseas, and will need to handle data in data protection regimes that are more matured. Thus, Symantec would strongly recommend that the Guidelines include some guidance or best practices in the areas of 'Right of Erasure' and 'Data Breach Notification'.