ITI Promoting Innovation Worldwide

Information Technology Industry Council (ITI)
Comment Submission to
Singapore Ministry of Communications and Information (MCI)
Public Consultation on the Draft Personal Data Protection (Amendment) Bill

May 28, 2020

Naomi Wilson
Senior Director of Policy, Asia
Information Technology Industry Council (ITI)
700 K Street, NW Suite 600
Washington, DC 20005
202-626-5733
nwilson@itic.org

Summary of Major Points

- Clarify the pre-requisites for data breach notification and amend notification timeline to "three business days."
- Remove criminal penalties for individual offenses.
- Make clear data portability obligation on "user activity data."
- Add information security as an additional basis for processing without consent.
- Clarify protections for intermediaries on data breach and unsolicited messages.

Statement of Interest

The Information Technology Industry Council (ITI), appreciates the opportunity to submit the following comments to Singapore's Ministry of Communications and Information (MCI) and Personal Data Protection Commission (PDPC) on the draft Personal Data Protection (Amendment) Bill.

ITI is the premier voice, advocate, and thought leader for the global information and communication technology industry. Our over 70 member companies include the world's leading innovation companies, with headquarters worldwide and value chains distributed around the globe. These companies are leading Internet services and e-commerce companies, wireless and fixed network equipment manufacturers and suppliers, computer hardware and software companies, and consumer technology and electronics companies.

One of the elements of our mission throughout every economy in the world is to position our companies to be genuine partners of the government. ITI navigates the relationships between policymakers, companies, and non-governmental organizations, providing creative solutions that advance the development and use of technology around the world. We firmly believe that the interests of our companies and industry are fundamentally aligned with those of the economies and societies in which we operate.

Privacy, security, and trust are central to our member companies' businesses, and we take seriously our obligation to protect and responsibly use the personal information of our customers, users, and employees. Because of our diverse membership and widespread business presence, our companies have direct interaction with the privacy and data protection regimes of nearly every country. ITI encourages Singapore to continue its leadership in amending its privacy framework to protect and responsibly use personal information, encourage innovation, promote the growth of trade, and facilitate the free flow of information.

Comments

Clarify the Pre-requisites for Data Breach Notification and Amend Timeline

ITI recommends revising the definition of "data breach" to clearly link it to the definition of a security incident in Section 26A. The proposed definition of "data breach" is not clearly linked to the occurrence of a security incident. This is problematic as the definition could be extended to non-security incident related events. For example, the definition of "data breach" could be interpreted to cover a network service outage that does not lead to any harm to the individual. Revising the definition of "data breach" to specifically address security incidents would also be consistent with international practices, such as the EU General Data Protection Regulation (GDPR).

Further, we suggest clarification on the meaning of "significant harm" in proposed Section 26B**.** While we support the introduction of the "significant harm" threshold to notify individuals of a data breach, neither the Public Consultation Document nor the Bill makes clear the relevant thresholds and tests for a breach to be considered as having caused "significant harm." The lack of clarity on this threshold could result in the PDPC and individuals being inundated with numerous immaterial notices, resulting in "notification fatigue." This would in turn lead to inconvenience for data subjects, increase in administrative costs and burdens for PDPC, and most importantly, result in a very real possibility that data subjects and regulators will fail to take appropriate action in response to notifications that indicate a real risk of harm. We therefore recommend that MCI/PDPC define or provide further clarification on the meaning of "significant harm."

Additionally, the draft bill's Section 26D currently requires data breach notifications to the Commission "as soon as is practicable, but in any case, no later than 3 calendar days." We suggest changing the language to "no later than 3 business days" to ensure case-by-case consistency and prevent overloading regulatory institutions with incomplete or inaccurate information before the incident has been properly analyzed. For example, in cases where the assessment happens on a Friday, the organization would only have one business day (Monday) to process information and evaluate scenarios. If the assessment happens on a Monday, the organization has three full business days (Thursday) instead.

Remove Criminal Penalties for Individual Offenses

Though we understand the intention for governments to hold individuals accountable for the mishandling of personal data as written in Section 35B, it is important to ensure meaningful enforcement by creating an enforcement framework that distinguishes between: (1) actors who willfully or due to gross negligence breach their legal obligations and cause harm to users; and (2) those who inadvertently contribute to a breach incident, or are not causing breaches intentionally. The Bill should consider actors who have invested significant resources in not only complying with legal obligations but also putting in place data management practices, technologies and security. The proposed bill could deem an individual liable to imprisonment for a term not exceeding 2 years, which risks business activity in this sector and discourages qualified candidates from accepting these roles. We suggest the MCI/PDPC remove criminal liability penalties subjecting individuals to imprisonment and instead hold the corporate entity accountable for individual offenses.

Make Clear Data Portability Obligation on User Activity Data

ITI supports MCI/PDPC for introducing data portability obligations to provide individuals with greater autonomy over their personal data. However, Section 2 includes "user activity data" in the scope of the data portability obligation. This is problematic and could adversely affect our members' products that aggregate information for legitimate security purposes such as threat analyses. Further, many companies do not organize data in a way that is tied to a particular individual. For example, some user activities are not easily sorted in a manner that a company can find all data attributable to one person. For many companies, it would be infeasible, or at least highly impracticable, to analyze all data and determine how to attribute it to an individual. We seek clarification about this requirement and recommend that "user activity data" should only apply to businesses that maintain data on individuals, rather than aggregating data of numerous individuals such that it is not attributable to any one person.

Add Information Security as an Additional Basis for "Deemed Consent"
ITI welcomes MCI/PDPC's proposal of expanding the concept of "deemed consent" under Section 15 to include contractual necessity and appropriate notification with a reasonable opt-out period. Further, we support that legitimate interests, business improvement, and research are new exceptions to consent. However, we would highlight the importance of information security and recommend MCI/PDPC add information security as an additional basis for processing or clarify that information security is within the scope of legitimate interest.

Clarify Protections for Intermediaries on Data Breach and Unsolicited Messages
ITI recommends revising Section 26C to make clear that data intermediaries do not have the obligation to monitor security breaches that are the responsibility of the main organizations. As currently proposed in the Bill, the intermediaries are required to notify the organization without undue delay where it has "reason to believe that a data breach has occurred." The intermediaries' obligations to notify organizations should apply where the intermediaries have actual knowledge or hard evidence of a breach. As currently drafted, intermediaries could be required to not only monitor their own systems but also proactively monitor the systems and content of the main organization in order to be able to comply with their obligations, which blurs responsibilities and creates a situation where the main organization may fail to implement its own appropriate security measures and monitoring systems. The proposed requirements additionally ignore the fact that intermediaries deal with security incidents daily – in some instances thousands of incidents or more – ranging from minor to significant, and they cannot and should not be expected to notify based on a guess as to what may have happened. The responsibility should remain for organizations to assess whether a data breach constitutes a "notifiable data breach" and to notify the Commission and individuals in such cases. We recommend that MCI/PDPC revise the Bill to make clear that the intermediaries should not be responsible for more than monitoring, and clarify that intermediaries are not required to notify the Commission or individuals of a "notifiable data breach."

Further, ITI supports MCI/PDPC's proposal to provide individuals with greater control over the unsolicited commercial messages they receive, including through robocalls. This will provide consumers with confidence in using communications, messaging, email, and other cloud-enabled services. However, it is also important to ensure that providers of the underlying services used to send the unsolicited messages are not inadvertently considered to have breached the new provisions the Bill would introduce. We therefore recommend Part IXA to include a provision similar to Section 36(2) to clarify that "*a telecommunications service provider who merely provides a service that enables an applicable message to be sent shall, unless the contrary is proved, be presumed not to have sent, not to have caused to be sent, and not to have authorised the sending of, the message.*"

Conclusion
ITI is pleased to respond to this public consultation. We reiterate our industry's commitment to privacy and take seriously our obligation to protect and responsibly use data. We look forward to working with MCI/PDPC to ensure globally interoperable privacy solutions in response to these challenges and opportunities in the economy.