REQUEST FOR FEEDBACK RESPONSE:

Public Consultation on the Draft Data Protection (Amendment) Bill
Singapore's Ministry of Communications and Information and the Personal Data Protection Commission

27 May 2020

I. ABOUT CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered endpoint security. Leveraging artificial intelligence (AI), the CrowdStrike Falcon® platform offers instant visibility and protection across the enterprise and prevents attacks on endpoints on or off the network. CrowdStrike Falcon deploys in minutes to deliver real-time protection and actionable threat intelligence from Day One. It seamlessly unifies next-generation AV with best-in-class endpoint detection and response, backed by 24/7 managed threat hunting. Its cloud infrastructure and single-agent architecture take away complexity and add scalability, manageability, and speed.

CrowdStrike Falcon protects customers against all cyber attack types, using sophisticated signatureless AI and Indicator-of-Attack (IoA) based threat prevention to stop known and unknown threats in real time. Powered by the CrowdStrike Threat Graph™, Falcon instantly correlates 2 trillion security events a week from across the globe to immediately prevent and detect threats.

There's much more to the story of how Falcon has redefined endpoint protection but there's only one thing to remember about CrowdStrike: We stop breaches. Learn more: www.crowdstrike.com.

II. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Privacy and public policy inquiries should be made to:

Drew Bagley (VP & Counsel, Privacy and Cyber Policy of CrowdStrike, Inc.)
policy@crowdstrike.com

III. SUMMARY

The amendments proposed will help modernize the PDPA, bringing it in-line with other data protection laws worldwide such as GDPR and CCPA. CrowdStrike recognizes the significance of the amendments in ushering in an era of holistic data protection by pragmatically expanding lawful bases for processing personal data and introducing new requirements for protecting against and responding to data breaches. However, CrowdStrike believes the amendments should also be an opportunity to further incentivize the adoption of state-of-the-art cybersecurity safeguards in line with global risk-based standards.

IV. STATEMENT OF INTEREST

In response to the Ministry of Communications and Information (MCI) and the Personal Data Protection Commission (PCPD), State of Singapore, Request for Consultation (RFC) on its draft Personal Data Protection (Amendment) Bill, including related amendments to the Spam Control Act (SCA), CrowdStrike offers the following views.

CrowdStrike approaches these questions from the standpoint of a leading cloud-native cybersecurity provider that defends globally-distributed enterprises from globally distributed threats. These comments do not seek to address every issue raised in the Public Consultation. It is limited to areas for which CrowdStrike may offer suggestions based on specific, relevant insights informed by multiple practice areas: cyber threat intelligence, proactive, incident response and managed security services, and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches.

V. COMMENTS

Strengthening accountability

Mandatory Data Breach Notification Requirement (Section 26B of the Draft Data Protection (Amendment) Bill) and Protection of Personal Data (Section 24 of the Draft Data Protection (Amendment) Bill):

Mandatory data breach reporting requirements are imperative to ensuring that organizations adopt adequate technical and organization cybersecurity practices. Considerations regarding what constitutes an adequate cybersecurity practice should consider both the actual risks and the state of the art. Accordingly, CrowdStrike believes it is necessary to go beyond the intended amendment to Section 24 of the PDPC by taking an approach similar to the GDPR requiring organizations to implement safeguards "appropriate" to the risk to protect personal data. This approach incentivizes organizations to take into account modern, rapidly-evolving data breach risks posed by cybersecurity threats from e-crime,

'hacktivist', and nation state actors using tactics such as ransomware, supply chain attacks, or malware-less intrusions.

As the MCI and PDPC stated in section 5 of their Public Consultation Paper, the number of data breaches will progressively increase. To this end, security and data protection capabilities must be robust precisely because of their (i) reliance on globally distributed infrastructure that ensures availability, resilience, and security and (ii) compliance with international standards and procedures. In order to ensure the most robust cybersecurity methods remain feasible, it is imperative that organizations have the duty to utilize state of the art measures to protect personal data against unauthorised access, collection, use, disclosure, copying, modification, disposal or similar risks. CrowdStrike applauds the impact-based approach of section 26D of the amendments to data breach notification requirements and the incentives for organizations to adopt technologies that would mitigate the impact of any such breaches.

CrowdStrike commends the recognition that various categories of data should be treated differently to protect individuals' personal data, and to spur innovation, but we caution that additional guidance and criteria for when to notify PDPC of a data breach may be necessary to avoid significant uncertainty for legal practitioners similar to that surrounding other data breach notification laws.

Offences relating to egregious mishandling of personal data (section 32 of the Public Consultation Paper) and Legitimate interest exemptions (section 40(a) of the Public Consultation Paper):

CrowdStrike applauds the recognition of the lawful basis of legitimate interest for processing personal data. As noted in the Public Consultation Paper, cybersecurity is a key part of data protection. This is why it is critical to account for the legitimate interest of necessary and proportionate data processing performed to prevent breaches, such as that performed by cybersecurity specialists, data scientists, AI engineers, and other information security professionals. Given the constantly evolving nature of the threatscape it is of utmost importance to the future of cybersecurity that those involved in the protection of data have the ability to rapidly respond. Acknowledging this lawful basis removes potential barriers to technological innovation in the ever-evolving field of cybersecurity.

Enabling meaningful consent

Enhanced Framework for collection, use, and disclosure of personal data: We commend the MCI for their efforts to expand deemed consent to include contractual necessity and consent by notification, thereby bringing them in alignment with other jurisdictions. It is vital to know that data flows are dynamic, and therefore certain exceptions are extremely important to enhancing innovation. MCI's acknowledgment of exceptions from the consent requirement for legitimate interests and business improvement provides a pragmatic assessment of data processing realities.

Greater consumer autonomy

Derived personal information exception (Paragraph 49): We again applaud the MCI's awareness that businesses need some flexibility with respect to derived personal information in order to spur innovation and advance technology. Excluding derived personal data from the data portability obligation while still providing notice obligations to individuals strikes a balance between efficiency for organizations and transparency to individuals. However, data access rights to derived personal data should take into account a balancing of interests between organizations and individuals, particularly with regard to incidentally processed personal data, like that appearing in cybersecurity or other IT telemetry data.

VI. CONCLUSION

The proposed amendments to the Personal Data Protection Bill are a thoughtful and comprehensive treatment of a complex legal and policy area. The draft reflects significant effort and represents a serious attempt to position Singapore as an innovation and consumer-friendly environment. As with most policy initiatives, the success of this effort will depend on implementation. To the extent appropriate, we recommend continued engagement with international stakeholders as the policy statement and associated legislation evolves. Although this initiative is broader than a single technology or use case, it is critical to consider implications on cybersecurity efficacy in designing Singapore's approach to data protection. Finally, because the underlying technologies evolve faster than law and policy, we recommend that the final guidance focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.