REQUEST FOR COMMENT RESPONSE

Proposed Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems

August 31, 2023

CROWDSTRIKE

CrowdStrike®, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

CONTACT

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

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy

Rob Sheldon
Director, Public Policy and Strategy

Email: policy@crowdstrike.com

SUMMARY OF MAJOR POINTS

In future iterations of the *Proposed Advisory Guidelines on the Use of Personal Data in AI Recommendation and Decision Systems* ("Guidelines"), we recommend that the Commission:

1. Make an additional exception for cybersecurity due to the risk personal data faces from cyber threat actors;
2. Avoid blanket anonymization guidelines because unique identifiers are necessary for cybersecurity in some cases;
3. And maintain the current distinction between B2C and B2B AI use cases.

I. INTRODUCTION

In response to the Personal Data Protection Commission of Singapore's ("Commission") request for feedback on the Guidelines, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, 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 and a variety of other cyber threats.

II. COMMENTS

CrowdStrike appreciates the Commission's effort to clarify how the Personal Data Protection Act (PDPA) applies in situations where the design or deployment of machine-learning AI models or systems involve the use of personal data. We recognize that the Commission has taken an important step to identify potential gaps and address additional issues or common scenarios that the proposed advisory guidelines should consider regarding the use of personal data in AI systems. CrowdStrike agrees with the Commission's approach of drafting this document as a guideline rather than regulation.

AI is introducing new capabilities in many different sectors like medicine and engineering, and disrupting normal ways of doing business. It is evolving at a rapid pace and creating benefits and risks across many sectors and aspects of life. While the public discourse around AI has grown exponentially in the last year, AI in cybersecurity

is not a new concept. CrowdStrike has deployed AI at scale across tens of millions of endpoints for prevention, dating back ten years. While we do not have feedback on every section of the Guidelines, we do want to offer several points that may be of value to the Commission as it finalizes them. Ultimately, in an era in which adversaries are now using AI to attack at scale, it is even more important to ensure that defenders can leverage the best possible technologies, including AI, to protect data, systems, and people.

PART II. USING PERSONAL DATA IN AI SYSTEM DEVELOPMENT, TESTING AND MONITORING

In the development, testing and monitoring stage of an AI system, the Commission has carved out exceptions for "Business Improvement'" and "Research" purposes in lieu of consent. Within these exceptions, organizations can use, without consent, personal data collected in accordance with the PDPA, where the use of personal data falls within the scope of these purposes. CrowdStrike recommends that an additional, specific exception be made for cybersecurity purposes. Some of the biggest risks to personal data come from cyber threat actors associated with nation states, hacktivists and eCriminals. In addition to encrypting enterprise networks to disrupt or halt operations, such threat actors increasingly threaten to publicly leak stolen data, from sensitive business information and intellectual property to internal communications and customer data, including financial or health data. This means that in addition to slowing or stopping productivity, threat actors are purposefully attempting to hold victims at heightened risk of reputational damage and adverse regulatory impacts. Therefore, to better preserve personal data, it is critical to promote policies that ensure access to security data for global operating cybersecurity teams.

As a leading cybersecurity provider, it is our view that the use of AI to detect cyber threats is an enormous advantage. As adversaries continue to evolve and find new ways to target victims,[1] organizations must increase their emphasis on cybersecurity practices that leverage the most effective technologies, including AI. AI is the best tool

[1] Cyber threat actors are constantly evolving and finding new ways to target victims, including private sector entities and government agencies involved in national security. Illustrative of this, in CrowdStrike's 2023 *Global Threat Report*, we observed a notable surge in identity-based threats, cloud exploitations, and malware-free attacks. Adversaries continued to move beyond malware to gain initial access with malware-free activity accounting for 71% of all detections in 2022 (up from 62% in 2021). A contributing factor to this shift was the rate at which new vulnerabilities were disclosed and the speed with which adversaries were able to operationalize exploits. Further, we found a 95% increase in cloud exploitation by threat actors, over 30 new adversaries, and numerous new ways that eCrime actors weaponize and exploit vulnerabilities. *CrowdStrike Global Threat Report, 2023.* https://www.crowdstrike.com/global-threat-report/

cyber defenders have to identify and prevent zero-day attacks and malware-free attacks. For AI in cybersecurity to work properly, accurate data, which may include unique identifiers, is needed to train the model. The higher the quality of the data, the less room for error in the cyber protection it offers. There should not be any broad prohibitions to AI datasets for cybersecurity purposes. Datasets used to train AI algorithms for cybersecurity should be viewed as a separate discussion from the important conversation of AI datasets for other purposes.

Access to data is critical to state-of-the-art cybersecurity. Big data allows AI to spot fainter signals that traditional antivirus tools cannot discern. Relatedly, more data is required for the development, testing and monitoring stage of an AI system because it leads to more accurate and actionable cyber threat intelligence. Without personal data, an AI system developed for cybersecurity cannot inform, predict or provide recommendations to customers when they are at risk of experiencing a cyber attack.

PART II. #7 Data Protection Considerations when using Personal Data

CrowdStrike understands that a concern with AI is the possible harm to individuals, but for AI, like for any other technology, the context in which it is used, rather than the mere fact that it is incorporated, is material. Regulating AI at the technology-level rather than its application is not the best approach to foster-innovative solutions to difficult problems. Additionally, the same principles of privacy that are already law can be applied across various uses, including AI. The context of data processing activities will decide the best ways for protection.

In Part II, items 7.1 and 7.7, the Commission encourages organizations to pseudonymise or de-identify personal data or datasets as a basic data protection control. We caution against the implementation of blanket anonymization. Anonymization is a tool used to protect data, and while anonymization may not always be the end goal, data protection is always the ultimate end goal. With this in mind, it is important to review both the positive and negative aspects associated with anonymization in effort to best prevent misconception or misunderstanding. Anonymization and pseudonymization are not always the most feasible or appropriate ways to achieve data protection. There are many examples of data processing activities in which anonymized data is not the desired state, particularly when unique identifiers are necessary for IT or cybersecurity purposes. This is another reason to add a cybersecurity exception in the development, testing and monitoring stage of an AI system.

PART IV: PROCUREMENT OF AI SYSTEMS - BEST PRACTICES FOR HOW SERVICE PROVIDERS MAY SUPPORT ORGANISATIONS IMPLEMENTING AI SOLUTIONS

We appreciate that the Commission has drawn a distinction between "business to consumer (B2C)" and "business to business (B2B)" in its guidelines. We agree with this distinction, especially when it comes to AI safeguards such as specific transparency or interpretability requirements. Consumer-facing AI applications may be more likely to involve impacts to specific users, people, or groups, or have other social implications. Enterprise (B2B) technologies that use AI may improve business processes and drive efficiency, like optimizing a maintenance schedule or reducing energy consumption. Different safeguards may be appropriate in each instance, but should relate specifically to potential risks.

III. CONCLUSION

The Commission's proposed Guidelines provide a thoughtful analysis of a complex legal and policy area. As updates to the Guidelines move forward, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any updates focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

###