PDPC'S PUBLIC CONSULTATION ON THE PROPOSED ADVISORY GUIDELINES ON USE OF PERSONAL DATA IN AI RECOMMENDATION AND DECISION SYSTEMS

KASPERSKY'S SUBMISSION (AUGUST 2023)

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly being transformed into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky technologies and we help 220,000 corporate clients protect what matters to them most. Learn more at www.kaspersky.com.

Contact Persons

For further information regarding this paper, please reach out to Genie Sugene Gan (genie.gan@kaspersky.com), Head of Government Affairs and Public Policy for Asia-Pacific, Japan, Middle East, Turkey and Africa, and Lee Heng (heng.lee@kaspersky.com), Public Affairs Manager for Asia-Pacific and Japan.

kaspersky

Introduction

Kaspersky welcomes PDPC's timely development of the Proposed Advisory Guidelines on Use of Personal Data in AI Recommendation and Decision Systems (hereinafter referred to as "the Guidelines"). Given the recent, rapid developments surrounding Generative Pre-Trained Transformer technology, and an expected rise in adoption of relevant AI and ML solutions, the Guidelines will provide clarity for how businesses should fulfill their personal data protection obligations where AI is involved.

Given Kaspersky's experiences in using AI in our work to prevent and combat cyberthreats, and in national and UN-led discussions on information and communications technologies, we would like to offer our feedback on how the Guidelines can be further enhanced to ensure the security of personal data in AI Recommendation and Decision Systems.

First Principles

It is important to understand why an additional set of guidelines is needed for personal data protection where AI is concerned – it is not because AI is harmful or dangerous by design. Rather, extra precautions are needed because the public is unfamiliar with how AI models work, or why there is a need to collect personal data for the refinement of algorithms for improvements in business processes. We believe this should be characterised as a communications exercise rather than to inadvertently lead to the impression that a new set of risks has arisen from AI, which need to be guarded against – because the risks remain traditional, in the loss of personal data and its consequent misuse. **We suggest for this to be made clear in the Guidelines' introductory chapters.**

It follows that existing law remains good law, which the Guidelines have articulated in paragraph 1.3. In that respect, we applaud the PDPC's enlightened approach of introducing the Guidelines as advisory and non-binding. This would prevent alarmism and leave space for AI innovations to grow.

On the Use of Consent and Exceptions

The problem that the Guidelines seek to address is the use of personal data in non-traditional ways, such as matching users to their needs (paragraph 5.4), and de-biasing AI systems (paragraph 5.8) – **uses which arguably have not fully entered the realm of public expectation**. It is this lack of expectation which creates the need for additional explanations during the "Deployment" and "Procurement" stages of AI system implementation. While we at Kaspersky expect such uses to be accepted over time, **we suggest that explicit consent should still be sought for the use of personal data during the "Development, testing and monitoring" stage**, at least in the interim. This is out of abundance of caution, to familiarize the public with such uses and to convince them of the utility of providing their personal data for such use cases.

We would also suggest that the PDPC **consider an opt-out system**, where a creator or owner of data is entitled to explicitly prohibit the use of their data for AI training purposes. One way to do this is to allow the addition of a hashtag to indicate that one's personal data should not be used for AI training. As the use of personal data for business improvement and research gets gradual acceptance, we expect users opting out to become the exception rather than the norm.

Finally, while we understand how the Business Improvement and Research exceptions to consent apply in the AI context, **we suggest that the Guidelines include a reminder that these exceptions should be used judiciously**. We also suggest that **the use of these exceptions be guided by a decision flowchart** so that it becomes clear to users whether the exceptions are available to them.

kaspersky

Anonymization

Kaspersky welcomes PDPC's recommendation for organizations to use anonymized datasets as far as possible instead of personal data during the "Development, testing and monitoring" stage of AI system implementation, as well as its provision of an anonymization tool. Based on Kaspersky's extensive experiences in cybersecurity and data processing, **we would also recommend the inclusion of practices such as deleting account details from transmitted URLs, obtaining hash sums of threats instead of the exact files, and obscuring user IP addresses** as additional, actionable steps that organizations can take towards anonymization. These are in line with Kaspersky's own best practices for the processing of users' data.

Accountability and Transparency

Kaspersky notes that there exists an extensive Accountability Obligation under the PDPA, which requires organizations to develop written policies and operational practices, amongst others. The Guidelines also mention (at paragraph 10.3) that organizations that make use of AI Systems should be transparent about it. Kaspersky strongly supports this, and would suggest that beyond policy statements and model cards, **organizations engaged in the development and training of AI/ML systems could be encouraged to show their transparent practices through avenues such as public demonstrations of their products**, to build trust with data subjects. This is something Kaspersky is deeply convicted in, having opened up the source code of our on-premises solutions for review by trusted partners and government agencies. We believe this is a best practice that can be promulgated throughout the industry.

That said, we recognize that transparency practices should be 'reasonable' and be accompanied by relevant precautionary measures to protect commercial secrecy, and not provide excessive information that could be used by malicious actors to disrupt the work of the AI/ML systems.

In addition, we also suggest that designers and developers of AI/ML systems should adopt such accountability mechanisms that would allow permanent self-revision and self-assessment of procedures critical for use of personal data.

Security by Design

Kaspersky further suggests that in designing and developing AI/ML systems, a 'security by design' approach should be taken. Such an approach is gaining popularity in the Internet of Things (IoT), and can ensure that any AI/ML systems would be guarded against malicious actors at the onset, thereby minimizing the risk of loss and misuse of personal data, and the resultant loss in trust.

Conclusion

In conclusion, Kaspersky reiterates its support for efforts by the Singapore government to create favorable conditions for the safe and responsible design and development of AI/ML systems, and reaffirms its readiness for further dialogue on this issue.