

Parliament No:	14
Session No:	2
Volume No:	95
Sitting No:	140
Sitting Date:	9-9-2024
Section Name:	Written Answers to Questions for Oral Answer Not Answered by End of Question Time
Title:	Measures to Ensure Protection of Biometric Data Collected by Private Entities
MPs Speaking:	Miss Rachel Ong, Mr Mark Lee, Mrs Josephine Teo

MEASURES TO ENSURE PROTECTION OF BIOMETRIC DATA COLLECTED BY PRIVATE ENTITIES

38 Miss Rachel Ong asked the Minister for Digital Development and Information (a) what measures are in place to ensure that the collection of biometric data of residents using Worldcoin Orbs is protected against the data being misused or resold; and (b) whether the collection of biometric data by private entities is or will be regulated.

39 Mr Mark Lee asked the Minister for Digital Development and Information (a) how is the Government addressing the risks of scams and fraudulent activities that can result from the misuse of biometric data by private entities; (b) what regulatory frameworks are in place or being considered to oversee and monitor the activities of such entities to ensure compliance with data protection laws and standards; and (c) what steps are being taken to educate the public about the potential risks of sharing their biometric data with these entities.

40 Mr Mark Lee asked the Minister for Digital Development and Information how is the Government collaborating with international counterparts to ensure a cohesive and robust approach to managing and mitigating the risks associated with biometric data collection technologies by private entities.

Mrs Josephine Teo: My response will also cover the matter raised in the question for oral answer by Mr Zhulkarnain Abdul Rahim which is scheduled for a subsequent Sitting. I invite the Member to seek clarifications, if need be. If the question has been addressed, it may not be necessary for him to proceed with the question for future Sitzings.

The Personal Data Protection Act (PDPA) governs the collection, use, disclosure and care of personal data by organisations in Singapore, including Worldcoin. Biometric data – which relate to the physiological, biological or behavioral characteristics of an individual – can form part of the personal data

of an individual. The Personal Data Protection Commission (PDPC) has also issued a Guide on Responsible Use of Biometric Data in Security Applications to advise on risks unique to biometric recognition technology and measures to govern and protect biometric data.

As biometric data are generally unique, they cannot be changed once compromised, unlike passwords or other tokens. Stolen biometric data can, therefore, be misused by malicious actors to spoof an individual's identity in order to access information or systems or conduct scams or other fraudulent activity. Such misuse is harder to defuse because biometric data cannot be changed.

Organisations that handle such data must ensure they put in place the necessary data protection and security arrangements to address these risks when designing and operating their systems and processes. They must also obtain consent from consumers before collecting their data by giving all necessary information in a manner that is understandable to the consumer.

PDPC has been engaging Worldcoin on their obligations under PDPA and will continue to monitor their collection, use and disclosure of personal data, including biometric data. PDPC may take enforcement action against organisations in Singapore that are found to have breached their obligations under PDPA. PDPC also monitors developments in other jurisdictions and is ready to work with international counterparts as necessary.

To support the adoption of good data protection practices, PDPC conducts educational and outreach activities through events, such as the annual Personal Data Protection Week and Privacy Awareness Week. PDPC has also worked with the Ministry of Manpower to disseminate notices to migrant workers to raise awareness about the importance of keeping their personal data safe.

Ultimately, everyone must exercise judgement and ensure they fully understand how their personal data will be used by whom before giving consent for it to be collected.
