Questions on Notice for TikTok Australia - hearing 11 July 2023
Answers received 26 July 2023

Questions unanswered as at 26 July 2023: nil

QON6
Senator Paterson: How often has Australian user data been accessed by mainland China employees?
Mr Farrell: I don't have specific numbers in front of me. I'd be happy to take that on notice.

Please find below further information in response to the committee's request:

The terms "user data" and "access" encompass an extremely broad spectrum of information and activities. In the context of large online platforms like TikTok, "Australian user data" includes (i) public information which users choose to publish on their profiles, (ii) anonymised data, (iii) business data, and (iv) aggregated data (i.e. not Australian users' personal information) which contains information relating to Australian platform users but is not confined solely to this subset of global platform users.

Similarly, "accessing" this information could include anything from looking up a user's public profile online, reviewing a spreadsheet of top trending Australian creators, aggregating data points such as the number of Community Guidelines violations in order to produce our publicly accessible transparency reports, troubleshooting a bug that has been reported by an Australian user, analysing the amount of time spent in-app across a sample of users in order to observe platform trends, or reviewing platform data in order to improve moderation accuracy - all to name but a few of the myriad ways in which platforms like TikTok interact with "user data" to ensure the platform's safety, security and effective operation.

Given the broadness of the question, and the 24/7 nature of our operations supporting a platform with more than one billion people on it, it is not possible to provide a meaningful, specific number in answer to the question as it has been put. In our previous answer, we sought to provide some parameters for the answer around sensitive user data or personal information (which we would consider information like users' email addresses and declared dates of birth), and provided an approximate frequency of access.

As we have previously outlined in evidence provided to this committee, the rules and safeguards governing employee access to TikTok user data, including Australian user data, is based on the sensitivity of that data, in adherence to the principles of least privilege.

In light of the committee's interest in this matter, it should also be noted that we are far from unique in having a global workforce, including in China, where data transfers form an essential part of our business's operations. In Australia, many major companies have operations and personnel based in China, as well as publicly available privacy policies which state that they too are able to provide access to personal information to entities within their corporate group based in China. These are common practices for global companies. The critical consideration is how that data is protected. At TikTok we are continually investing in our processes to better detect and prevent anomalous and malicious data access behaviour.

During the committee hearing we also endeavoured to provide the committee with our latest Community Guidelines Enforcement Report (covering platform activity from 1 January to 31 March

2023), which details, among other things, the covert influence operations networks identified and removed in Q1 2023. This report is available here.

Answers received 21 July 2023

The answer to the honourable Senator's question is as follows:
The rules and safeguards governing employee access to TikTok user data, including Australian user data, is based on the sensitivity of that data, in adherence to the principles of least privilege. Our engineers based around the world, including in China, will only be granted access to sensitive user data when under controls and approval protocols overseen by our US-led security team, where a valid business reason is presented. For example, this could include work to improve the relevance and accuracy of searches, recommendations, and providing troubleshooting support on technical issues. In addition, user access is periodically reviewed for appropriateness, and other controls, such as inactive permission revocation, are implemented to further restrict access when needed. Because of the size and scale of the platform, as well as the need to provide 24 by 7 support, frequency of access can vary. Consistent with the practices of other global businesses, this can be as frequent as daily, and is used to support the platform's safety, security and operation.