Administrative
Appeals Tribunal

Principal Registry

3 September 2020

Mahalingam Sutharshan
Director
Patience Immigration Lawyers
shan@ppilaw.com.au

Dear Mr Sutharshan

Re: Video Conference Hearings

I refer to your email enquiries (including your message of 11 June 2020) concerning the use of the Microsoft Teams applications for hearings. I apologise for the delay in responding.

The COVID-19 pandemic has affected the capacity of the Tribunal to conduct hearings in person and the move to hearings by video conference was made to enable it to continue to meet its objectives. The Tribunal has elected to use the Microsoft Teams application within our Microsoft Azure cloud tenancy to conduct hearings by video because it has the functionality and security to meet the Tribunal's needs and could be quickly deployed and accessed by users.

You have asked:

(a) whether the Tribunal can confirm that applicants' privacy and confidentiality will be protected

(b) whether the Tribunal has taken adequate measures to protect the privacy and confidentiality of your clients' claims and identities

(c) whether Microsoft Teams will not record or store applicants' details or the hearing or evidence of the applicant.

You provided 4 links to illustrate your concerns:

- The first link you have provided does not expressly refer to Microsoft Teams, but it does point out that, despite the best internal efforts, all electronic systems are potentially vulnerable.

- The second linked article refers to the urgent patching of a security flaw detected in Microsoft Teams in April 2020. The flaw was identified and patched before any attacks were spotted 'in the wild'.

- The third linked article concerns a scam to steal Teams credentials by tricking users into accessing cloned Microsoft Teams entry pages.

- The final linked article concerns call data potentially retained under the privacy policy of major IT players, including Microsoft, and the retention, by implied user consent of information including call length, user IDs and user IPs.

Question (a)

Under the *Privacy Act 1988* (Privacy Act) the AAT must take such steps as are reasonable in the circumstances to protect information from loss, interference, unauthorised access or disclosure (APP 11) and to include certain provisions in contracts with service providers to maintain its compliance with the Privacy Act. These provisions include notification of any data loss to enable the AAT to meet its responsibilities under the Notifiable Data Breach scheme. Further rules apply if data is held overseas.

The AAT's use of Microsoft Teams and Microsoft Azure cloud services is in accordance with a whole-of-Australian Government agreement. The agreement includes provisions in compliance with the Privacy Act. In addition, the products and services comply with existing Australian Government cyber-security standards for cloud-based services.

While the AAT cannot guarantee that information will never be subject to unauthorised access, we have taken reasonable steps to minimise the possibility. These steps include configuration of the service to ensure that all communications made during hearings with external parties are encrypted.

No person outside the AAT can participate in a hearing conducted using Microsoft Teams unless the AAT allows them to enter the virtual hearing room and only the AAT can use Microsoft Teams to record the hearing. The AAT reminds participants in hearings of the prohibition on the use of recording devices, set out in the COVID-19 Special Measures Practice Direction – Migration and Refugee Division, at the outset of the hearing and via a written notice integrated into the member's background during the hearing.

Recordings of hearings conducted by Microsoft Teams are stored in the AAT's secure cloud tenancy and can only be accessed by authorised AAT members and staff. Once downloaded by a member or staff member, recordings are held in the AAT's pre-existing internal systems.

Question (b)

See above.

Moreover, an applicant may also protect their own privacy, including by ensuring they undertake the hearing in a location where they cannot be overheard, the background does not include personal information about them, and any wifi network used to access the internet is secure.

Questions (c)

The content of the communications themselves is stored in the AAT's secure Microsoft Azure cloud tenancy and is not otherwise held by Microsoft. All metadata generated is held in Australia.

If a party or representative considers that an individual case raises security issues such that it would not be reasonable to conduct a hearing using Microsoft Teams, this should be raised with the District Registrar in the relevant State at the earliest opportunity and prior to any hearing.

I trust the above information is of assistance to you.

Yours sincerely,

SIGNED

Alison Nesbitt
a/g Executive Director Review Support