MCH Privacy Breach: Situation Update as at 10am 23 August 2019

Key points

- A digital privacy breach was notified to MCH on 22 August. Personal identification documents of some successful applicants to the Tuia 250 voyage trainee programme were available through specific Google searches. The breach was discovered when 9(2)(a) of one of the trainees contacted MCH after 9(2)(a) drivers licence was used in an 9(2)(a) 9(2)(a). It was determined that the image had originated from the Tuia 250 website. The Ministry is also confirming whether information is available through other search engines.
- We understand this information may have been available since 2 June.
- The Tuia250 website was built and is maintained by a private company, specifically for the Tuia 250 commemoration.
- All copies of personal identification documents have been removed from the Tuia 250 website.
- On the evening of 22 August, all links to pieces of personal information identified by MCH had been provided to Google. Google has removed the items from their cache.
- We have been in contact with 9(2)(a) to seek assurances that the website is now secure. We have asked the Government Chief Digital Officer (GCDO) for assistance in providing independent verification that this is the case.
- MCH will be contacting each person who may have been affected.
- MCH is treating this as a serious breach of personal information.

Background

As part of the Tuia 250 commemoration, six vessels are undertaking a voyage to 15 significant sites around New Zealand from October - December. Members of the public, 16 years and over, were invited to apply for berths on the vessels so that they could participate in different legs of the voyage.

All applicants directly uploaded their information to the Tuia 250 website (www.tuia250.nz), which included images of forms of identification (predominantly passports or drivers licences). Some scanned applications included more personal information may have also been compromised.

MCH contracted a private company as part of a competitive procurement process to build and maintain a website specifically for the Tuia 250 commemoration. As part of the website, the provider created the web forms which were used by applicants to upload their information.

Notification of a privacy breach

MCH was contacted at 9.58am on 22 August by the parent of a trainee. 9(2)(a) drivers licence had been 9(2)(a) It was determined the image of the drivers licence had originated from the Tuia250 website.

Immediately on being notified we removed the image from the website.

At 11.47am, an MCH Manager called 9(2)(a) of that trainee to apologise and advise 9(2)(a) that the image had removed been removed.

MCH staff then tested to see whether this was a wider problem with images of personal identification searchable through Google. We established that it was. The information from some successful applicants was indexed and could be accessed through a targeted Google search.

Immediate response

At 11.50am, the issue was escalated to the CIO and DCE.

The DCE established a team to respond to the breach and the following actions took place during the course of Thursday:

- Removal of all images containing personal information from the media library in the 'back end' of the website.

- The provider was contacted and asked to resolve the issue immediately. We were given a verbal assurance that the Tuia250 website content was 'secure'. We have not yet received that assurance in writing. [Further discussions are needed in relation to both this and a potential breach of contract].

- Contact was made with Google to work through the process of clearing Google's caches of these images. By Thursday evening, all links to pieces of personal information identified by MCH had been provided to Google. Google have removed the items from their cache.

- The GCPO office was contacted and the issue was escalated to the Government Chief Privacy Officer who then contacted the Director of the Digital Safety Team to seek their assistance in working with Google to expedite the process of clearing the Google cache.

- We formally notified the Office of the Privacy Commissioner around 7pm last night.

- Contact was made with the Chief Legal Adviser at DIA to ask about placing a flag on passports that may have been compromised. We are waiting for advice on what action may be needed / appropriate.
- SSC, DPMC and Arts Culture and Heritage Ministers were advised (Ministers Ardern, Robertson, Sepuloni) and the Minister responsible for Tuia 250 (Davis).

Description of the breach

- Images that provided proof of identity were uploaded by applicants to the Tuia250 website. These images were often named things like "passport" or "licence" and were filed in the media library of the website.

- Any image in the media library may have had a automatically link created for it. This is how the website works to show its content. Some images/pdfs/doc/etc files had links created, not all. We have not been able to establish a pattern yet.

- This approach is not normal practice.

- Once the folder was indexed by search engine bots, anyone who typed in a search into a search engine that was a close match for the name of the file may have received search results that included some of these images.

- The images provided on the search engine are generally not legible images, but the they linked to the original file on the Tuia website and were a larger size and legible. "eg John Smith passport".

- These files were removed as soon as we realised there was an issue. What remained available was the cached Google search engine image.

- We have checked this morning and all the linked URLS that we have supplied have been removed by Google. They may still be available through other search engines and we are taking action on this.

Scale of the breach

- We believe that 82 applicants were affected out of 324 total applicants who submitted a file to the Tuia250 website. MCH is urgently working to confirm the number of affected applicants.

- The information that was compromised includes drivers licences, passports and birth certificates and in a small number of cases information contained in the application form which includes phone numbers, addresses, medical information and criminal convictions.

Next steps

Technical assurance

- Confirm that the material has been removed from Google's caches – complete.

- Instruct provider to temporarily take the website down to ensure that any security issues are addressed – complete.

- Contact GCDO for advice on independent verification that the Tuia 250 website, and other MCH websites, are secure in relation to personal information – underway.

- Draft terms of reference with the support of the GCDO for an independent review – not started.

- Follow-up with the provider to seek further assurances that the website is secure, that no other search engine has material cached, and ascertain what steps they are taking to ensure a breach does not occur again.

Care and assistance for individuals affected

- Meet with Police in relation to those individuals whose information may have been compromised including a discussion around police cyber security and any additional actions they may be able to take – scheduled for 11am today.

- Seek advice from MSD about any particular care we need to take in relation to young people whose information may have been compromised (applications were accepted from individuals aged 16 and over) – underway.

- Confirm the list of affected trainees and contact them personally to advise what has happened and what has been done (this will not happen until further discussions with SSC). This will be done by phone for those individuals who we know have had their information compromised.

- A range of stakeholders will also be contacted at the appropriate time including the Spirit of New Zealand (one of the vessels in the Tuia flotilla) who ran a separate expressions of interest process. Their process was not affected but they may receive queries from concerned applicants.

- Investigate with DIA and NZTA whether a process could be set up for those whose information has been compromised to replace those documents easily and without charge – underway.

- Determine a process for any compromised forms of identification from other countries (eg foreign passports) and discuss any potential visa implications with Immigration NZ relevant local missions. At this stage we have identified passports from 9(2)(a) 9(2)(a) Checks are continuing – not started.

9(2)(h) [redacted]

Reactive media points

- Manatū Taonga Ministry for Culture and Heritage is investigating a digital privacy issue involving the Tuia 250 Voyage Trainee programme.

- We acknowledge this situation is unacceptable and should not have happened. We apologise unreservedly to all Trainee applicants.

- As part of the application process, applicants supplied personal information. This information was stored on the Tuia 250 website servers.

- We were notified on 22 August that personal information of a trainee was available online. We immediately took steps to ensure the personal information is removed.

- On further investigation we identified personal information from other Trainees was also available online

- All copies of personal information have been removed from the Tuia 250 website.

- We have notified our website provider and had assurance that information is now secure.
- We have identified all indexed links on Google to personal information and requested these to be removed by Google – and this has now been completed.
- We have sought advice from Government Chief Privacy Officer, State Services Commission, Department of Internal Affairs and Office of the Privacy Commissioner and New Zealand Transport Agency to ensure that we are taking all necessary steps to address this serious issue.
- All Trainees will be personally notified about this issue.