COVID app data and Intelligence Agencies within IGIS jurisdiction

16 May – 16 November 2020

First Report

Jake Blight
A/g Inspector-General of Intelligence and Security

16 November 2020

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

IGIS Report to OAIC on COVID app data – 16 May to 16 November 2020

Summary

The Office of the Inspector-General of Intelligence and Security (IGIS) has worked with agencies within IGIS jurisdiction to ensure that they are aware of their obligations under the *Privacy Act 1988* in respect of COVID app data. We have also been briefed on technical capabilities and have reviewed the policies and procedures that have been implemented by relevant intelligence agencies in the event that collection of COVID app data occurs.

As at 16 November 2020, the acting Inspector-General is satisfied that the relevant agencies have policies and procedures in place and are taking reasonable steps to avoid intentional collection of COVID app data. Incidental collection in the course of the lawful collection of other data has occurred (and is permitted by the Privacy Act); however, there is no evidence that any agency within IGIS jurisdiction has decrypted, accessed or used any COVID app data.

Inspection activities are planned in coming months to verify data deletion and to provide further assurance that no COVID app data has been accessed, used or disclosed.

Background

Under the *Inspector-General of Intelligence and Security Act 1986* (the IGIS Act) the role of the Inspector-General is to assist Ministers overseeing and reviewing the legality and propriety of the activities of six of Australia's intelligence and security agencies. This includes their compliance with Part VIIIA of the *Privacy Act 1988* (the Privacy Act). The six agencies within IGIS jurisdiction are:

- Australian Security Intelligence Organisation;
- Australian Secret Intelligence Service;
- Australian Signals Directorate;
- Australian Geospatial-Intelligence Organisation;
- Defence Intelligence Organisation; and
- Office of National Intelligence.

IGIS staff undertake regular independent inspections of the six intelligence agencies within jurisdiction and have the necessary security clearances and experience to identify and report on any non-compliance by those agencies with the various laws, directions, guidelines and policies which govern their intelligence operations.

The IGIS office also works with the internal compliance teams in each agency to foster a culture of compliance and ensure appropriate policies and procedures are in place to minimise the risk of any non-compliant activity and to ensure that, if a potentially unlawful or improper activity occurs, it is promptly reported and investigated.

The Inspector-General and the Privacy Commissioner have overlapping jurisdiction in relation to intelligence agency compliance with Part VIIIA of the Privacy Act. Shortly after Part VIIIA commenced the then Inspector-General and the Commissioner agreed that the most effective and efficient way to oversee compliance with Part VIIIA by the intelligence agencies would be for the Inspector-General to review the activities of the six agencies within IGIS jurisdiction and to provide an unclassified report to the Commissioner. The Commissioner may take that report into account when preparing her report under s 94ZB of the Privacy Act.

Identification of risks

In late-April 2020 IGIS commenced work with agencies within its jurisdiction to determine how these agencies would meet their legal obligations under the *Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements – Public Health Contact Information) Determination 2020* and later under Part VIIIA of the Privacy Act.

Not all agencies within IGIS jurisdiction have functions or technical capabilities which may enable them to collect COVID app data. For agencies where there is a risk that such data might be collected the IGIS office contacted the agencies and this led to discussions and correspondence regarding legal and technical issues around collection of COVID app data and some of the key potential measures required to comply with the Privacy Act. It was clear from these discussions that agencies were alert to their obligations under Part VIIIA of the Privacy Act and were taking active steps to ensure compliance.

Exploration of issues

The Inspector-General's staff worked with intelligence agencies to monitor their progress in ensuring compliance with Part VIIIA. This included the following activities:

- IGIS staff meeting with technical specialists in agencies to understand relevant capabilities which may give rise to the risk of COVID app data being collected.
- Where relevant, intelligence agencies sought legal advice to understand their obligations, including in the context of how specific intelligence collection systems operate. This advice was provided to the Inspector-General in full. The aspects of the advice which deal with particular intelligence capabilities is classified; however, parts of the advice simply interpret Part VIIIA. The Inspector-General facilitated declassifed versions of the advice being prepared and provided to the Privacy Commissioner in accordance with the *Legal Services Directions 2017*.
- IGIS staff obtaining advice and evidence from the agencies on steps they had or were taking to mitigate the risk of collecting COVID app data.
- Reporting to the Inspector-General on all instances where agencies had identified that they had, or had likely, collected COVID app data.
- Agencies providing IGIS staff with briefings about the difficulties which arise in identifying encrypted COVID app data amongst other lawfully collected encrypted data.
- Agencies developing procedures to apply in the event of any incidental collection of COVID app data.
- Agencies implementing procedures for deleting data reasonably believed to be COVID app data as soon as practicable.

IGIS staff are familiar with intelligence agency operations including the exercise of warrants, procedures to protect the privacy of Australians, targeting of data collection capabilities and

the very high level of security that intelligence agencies employ to protect against any unauthorised access to or disclosure of data.

Complaints

The Inspector-General can receive complaints and public interest disclosures about the activities of the six intelligence agencies within IGIS jurisdiction. No complaints or disclosures about COVID app data have been received.

Summary of findings to date

Based on the work described above the acting Inspector-General is satisfied that the intelligence agencies within IGIS jurisdiction which have the capability to incidentally collect a least some types of COVID app data:

- Are aware of their responsibilities under Part VIIIA of the Privacy Act and are taking active steps to minimise the risk that they may collect COVID app data.
- Have appropriate policies and procedures in place to respond to any incidental collection of COVID app data that they become aware of.
- Are taking steps to ensure any COVID app data is not accessed, used or disclosed.
- Are taking steps to ensure any COVID app data is deleted as soon as practicable.
- Have not decrypted any COVID app data.
- Are applying the usual security measures in place in intelligence agencies such that a 'spill' of any data, including COVID app data, is unlikely.

Next Steps

Staff from IGIS will incorporate compliance with Part VIIIA of the Privacy Act into the regular IGIS inspection program. Our next focus will be to verify that COVID app data has been deleted as soon as practicable after an agency becomes aware that it has been collected and that COVID app data has not been accessed, used or disclosed.

The Inspector-General will provide the Privacy Commissioner with a further report to inform the next report prepared by the Commissioner under s 94ZB of the Privacy Act.