



Australian Government

Office of the Australian Information Commissioner

# COVIDSafe Report May–November 2020

Report under Part VIIIA of the *Privacy Act 1988*



Angelene Falk  
Australian Information Commissioner and Privacy Commissioner  
23 November 2020

OAIC

## Contents

About this report	2
Executive summary	3
COVIDSafe guidance and advice	5
Enquiries	7
The COVIDSafe app and my privacy rights	9
Complaints	9
Investigations	10
Commissioner-initiated investigations	10
Information sharing	10
Privacy obligations regarding COVIDSafe and COVID app data	11
Data breaches	10
Assessments	12
Inspector-General of Intelligence and Security COVIDSafe report	14
Glossary	15
Attachment A: COVID app data and Intelligence Agencies within IGIS jurisdiction	17

## About this report

The Australian Government launched the voluntary COVIDSafe app (COVIDSafe) on 27 April 2020.

On 16 May 2020, the Office of the Australian Information Commissioner (OAIC) was granted additional functions and powers in relation to COVIDSafe under Part VIIIA of the *Privacy Act 1988* (Privacy Act).

The object of Part VIIIA is to assist in preventing and controlling the entry, emergence, establishment or spread of COVID-19 into Australia or any part of Australia by providing stronger privacy protections for COVID app data and COVIDSafe users in order to:

- a) encourage public acceptance and uptake of COVIDSafe, and
- b) enable faster and more effective contact tracing.

Part VIIIA expands the Commissioner's regulatory oversight role to apply to state and territory health authorities, to the extent that they deal with COVID app data.

It enhances the Commissioner's role in dealing with eligible data breaches and conducting assessments and investigations in relation to COVIDSafe and COVID app data. It enables the Commissioner to refer matters to, and share information or documents with, state or territory privacy authorities. It also imposes on state and territory health authorities the Privacy Act's rules and privacy protections and Commonwealth oversight in relation to COVID app data.







In accordance with section 94ZB, this report sets out the performance of the Commissioner's functions and the exercise of the Commissioner's powers under or in relation to Part VIIIA.

This report covers the 6-month period starting on the commencement of Part VIIIA: **16 May 2020 to 15 November 2020.**

## Executive summary

The Commissioner has an independent oversight function in relation to COVIDSafe under the Privacy Act and is actively monitoring and regulating compliance.

The Commissioner has powers to:

-  conduct assessments of an entity's or authority's compliance with the law
-  investigate complaints
-  make a declaration to ensure the conduct is not repeated and to redress any loss or damage
-  seek civil penalties against individuals and organisations that breach the law
-  refer matters to the police if the OAIC thinks a crime has been committed
-  refer matters to State and Territory privacy regulators if appropriate

### Key statistics May–November 2020

#### Enquiries received



11

#### Assessments commenced



4

During the reporting period of 16 May 2020 to 15 November 2020, the following matters were recorded under or in relation to Part VIIIA:

**Table 1 — Number of matters related to COVIDSafe and COVID app data**

Regulatory function	Number
Enquiries	11
Complaints received	0
Complaints finalised	0
Investigations	0
Commissioner-initiated investigations	0
Information sharing	0
Assessments commenced	4
Assessments finalised	0
Data breach notifications	0

## COVIDSafe guidance and advice

In March 2020 the OAIC established an internal COVID Taskforce to support the provision of advice to government and business on matters related to the pandemic and COVIDSafe.

### Government and regulator engagement

The OAIC has engaged with the Australian Government, state and territory privacy and health authorities, and international data protection regulators in providing advice and guidance on the development and implementation of COVIDSafe privacy protections.

During the development of COVIDSafe, we engaged closely with the Australian Government Department of Health (Health) in relation to its COVIDSafe Application Privacy Impact Assessment (PIA) and its implementation of the PIA recommendations.

Between May and October 2020, we also sought and received updates from Health on the implementation of the PIA recommendations.

We have provided detailed privacy advice to a range of Australian Government departments and agencies regarding:

- the draft collection and consent notices for COVIDSafe
- the draft legislation related to COVIDSafe
- bilateral agreements with state and territory health authorities on access, use and disclosure of COVID app data
- proposed enhancements to COVIDSafe
- interjurisdictional contact tracing.

We wrote to Chief Health Officers in each state and territory in May 2020 seeking further information about their contact tracing processes to inform our COVIDSafe regulatory work.

The OAIC also facilitated briefings with privacy experts and state and territory privacy Commissioners in May 2020 in relation to COVIDSafe and the draft legislation.

The National COVID-19 Privacy Team, which was convened between the OAIC and states and territories with privacy laws to respond to proposals with national implications, has been engaged and continues to be briefed on the implementation of the COVIDSafe privacy protections.

In implementing Part VIIIA, a cross-agency working group was convened in June 2020 to develop COVIDSafe guidance and referrals. Members of the working group include the OAIC, Health, Attorney-General's Department, Australian Federal Police, Department of Home Affairs, Fair Work Ombudsman and the Inspector-General of Intelligence and Security.

We also consulted the United Kingdom Information Commissioner's Office and the Personal Data Protection Commission Singapore to discuss international contact tracing approaches, including COVIDSafe.

## Guidance for regulated entities and the community

The OAIC has worked to increase awareness and understanding of privacy protections and obligations related to COVIDSafe by developing and promoting guidance for the community and regulated entities.

During the reporting period, the OAIC published 2 resources relating to the COVIDSafe app:

- [guidance for individuals](#) on the COVIDSafe app and their privacy rights, which was also made available in 10 community languages (4 June 2020)
- [guidance for regulated entities](#) on their COVIDSafe and COVID app data privacy obligations (30 June 2020).

A summary of both resources is provided later in this report.

The guidance has been promoted through the OAIC's external communications channels and directly to regulated entities and peak bodies. From the date of publication to 15 November 2020, the guidance for individuals page on the OAIC's website was visited 4,424 times, and the guidance for regulated entities page was visited 942 times.

In June 2020, we wrote to a range of peak industry bodies that represent businesses in the hospitality, real estate, hair and beauty, manufacturing, entertainment, sport and other industry sectors, to raise awareness of privacy obligations under Part VIIIA.

In July 2020, we wrote to a number of large sports and entertainment venues to raise awareness of privacy obligations under Part VIIIA.

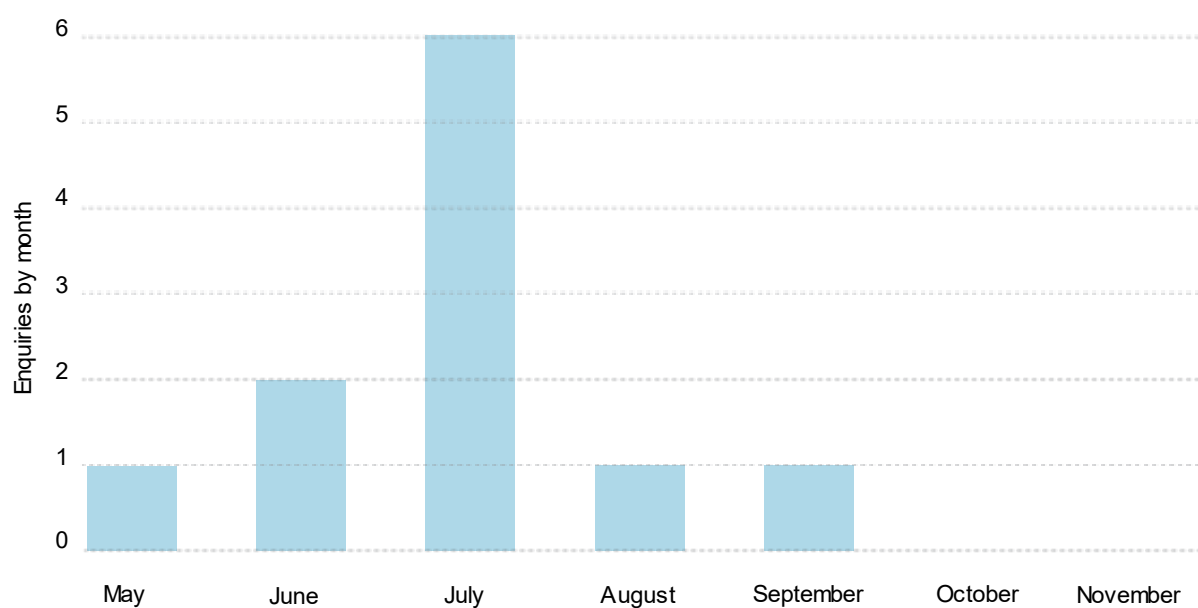
During the reporting period, the OAIC contacted two entities – a real estate agent and a sporting body – regarding acts or practices that were identified through public sources as potential contraventions of Part VIIIA, resulting in the cessation of these acts or practices.

## Enquiries

The OAIC provides a free public information service, including information about the privacy protections for COVIDSafe.

Between 16 May 2020 and 15 November 2020, the OAIC received 11 enquiries from individuals about COVIDSafe. We provided general information in response to 10 enquiries and provided assistance on how to make a complaint in response to one enquiry.

**Figure 1 — Enquiries about COVIDSafe received by month May–November 2020**





## Types of enquiries

### General enquiries or concerns about COVIDSafe

We responded to 7 enquiries raising general issues or concerns about COVIDSafe during the reporting period, including:

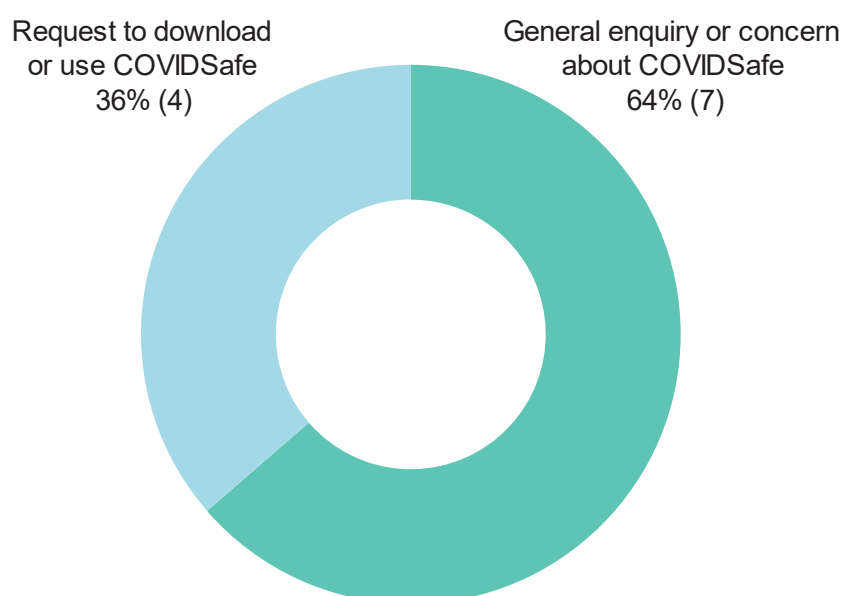
- an enquiry about the legal basis of the COVIDSafe app
- an enquiry about the number of COVIDSafe downloads.

### Request to download or use COVIDSafe

We answered 4 enquiries related to a request to download or use COVIDSafe, including:

- an enquiry about COVIDSafe installation being a condition of entry to a worksite
- an enquiry about an educational institution asking students to download COVIDSafe
- an enquiry about a sports club asking members if they had downloaded the app.

**Figure 2 — Types of enquiries about COVIDSafe received May–November 2020**



## The COVIDSafe app and my privacy rights

In May 2020, the OAIC published guidance for individuals that describes how the Privacy Act applies to COVIDSafe and addresses a range of questions about individuals' privacy rights.

The resource explains the purpose of COVIDSafe and how personal information is collected, handled and deleted in line with strict protections under the Privacy Act that are overseen by the OAIC.

The resource advises individuals that:

The app is voluntary. Whether or not you choose to download and use the app is entirely your choice. You cannot be required to download or use the app.

If the app has been installed on a device you use at your workplace, your employer should delete the app upon your request.

It is an offence under the Privacy Act for any individual, organisation or government agency to require you to download or use the app.

The resource also explains how individuals can make a privacy complaint to the OAIC in relation to COVIDSafe and COVID app data. For example, if someone requires them to download or use COVIDSafe to take part in an activity or to provide or receive a good or service.

The guidance is also available in 10 community languages: Arabic, Greek, Hindi, Italian, Punjabi, Simplified Chinese, Spanish, Thai, Traditional Chinese and Vietnamese.

The guidance is available at [www.oaic.gov.au/the-covidsafe-app-and-my-privacy-rights](https://www.oaic.gov.au/the-covidsafe-app-and-my-privacy-rights)

## Complaints

Under section 36 of the Privacy Act, an individual can complain to the Commissioner about an act or practice that may be an interference with their privacy.

During the reporting period, the OAIC did not receive any complaints related to COVIDSafe.

## Investigations

Under Part V of the Privacy Act, the Commissioner can investigate privacy complaints related to COVIDSafe and conciliate an outcome or make a determination. Under Part VIB of the Privacy Act, the Commissioner may take other enforcement action to seek civil penalties, enforceable undertakings and injunctions.

Privacy complaints may also be transferred to a state or territory privacy authority (section 94V(1) and (2)), which involves giving notice to the complainant of the transfer and providing any information or documents that relate to the complaint to the state or territory authority (section 94V(2)(b) and (c)).

If the Commissioner believes an offence relating to COVIDSafe or COVID app data may have been committed, under section 94U the Commissioner must discontinue that part of the investigation and inform the Australian Federal Police or Commonwealth Director of Public Prosecutions.

No privacy investigations were commenced during the reporting period.

## Commissioner-initiated investigations

Under section 40(2) of the Privacy Act, the Commissioner may initiate inquiries or an investigation into potential interferences with privacy. The OAIC monitors a range of information sources in considering the need to investigate certain acts or practices, including intelligence received through enquiries and complaints, media reports, domestic and international regulators, and other sources.

During the reporting period, the Commissioner did not initiate any inquiries or investigations related to COVIDSafe.

## Information sharing

Under section 94W of the Privacy Act, the Commissioner is empowered to share information with a state or territory privacy authority. The OAIC has consulted with state and territory privacy authorities to develop a protocol for the transfer of complaints and sharing of information under Part VIIIA.

During the reporting period, the Commissioner did not exercise this power.

## Data breaches

Under section 94S of the Privacy Act, a breach of a requirement under Part VIIA by the National COVIDSafe Data Store Administrator (DSA) or a state or territory health authority is considered an 'eligible data breach'. All individuals to whom the data relates are considered to be 'at risk' from the data breach and both the OAIC and affected individuals must be notified as soon as practicable about the data breach, unless the OAIC grants an exemption to the requirement to notify individuals.

During the reporting period, the Commissioner was not notified of any data breaches.

## Privacy obligations regarding COVIDSafe and COVID app data

In June 2020, the OAIC published guidance to help entities understand their privacy obligations under Part VIII A of the Privacy Act regarding COVIDSafe and COVID app data.

Among the key points in the guidance:

- No individual, organisation or government agency can require any individual to download or use the app. Criminal penalties apply for breach of these provisions.
- It is an offence for any individual, organisation or government agency to require an individual to upload their data, or cause for the data to be uploaded, from the COVIDSafe app to the National COVIDSafe Data Store (Data Store), without obtaining consent from that individual.
- COVID app data in the Data Store must be stored on a database in Australia.
- COVID app data may only be collected, used or disclosed to conduct contact tracing by a person employed or in the service of a state or territory health authority, the DSA, the OAIC, the police or the Director of Public Prosecutions.
- All parties handling COVID app data must also comply with the Australian Privacy Principles.
- The DSA must, upon the request of the individual, their parent, guardian or carer, delete that individual's registration data from the Data Store.
- A breach of any of the new COVID app-related provisions of the Privacy Act by the DSA, or by a state or territory health authority, will be considered an 'eligible data breach' under the Notifiable Data Breaches scheme.

The guidance is available at [www.oaic.gov.au/privacy-obligations-regarding-covidsafe-and-covid-app-data](https://www.oaic.gov.au/privacy-obligations-regarding-covidsafe-and-covid-app-data)

## Assessments

Under section 94T of the Privacy Act, the Commissioner is authorised to conduct an assessment of whether the acts or practices of an entity or a state or territory health authority comply with Part VIII A of the Privacy Act in relation to COVIDSafe and COVID app data.

The OAIC's COVIDSafe Assessment Program follows the 'information lifecycle' of personal information collected by the COVIDSafe app and currently includes 5 risk and compliance privacy assessments.



**Assessment 1** – Access controls applied to the Data Store by the DSA



**Assessment 2** – Access controls applied to the use of COVID app data by state or territory health authorities



**Assessment 3** – Functionality of the COVIDSafe app against specified privacy protections set out under the COVIDSafe privacy policy and collection notices, and against the requirements of Part VIII A



**Assessment 4** – Compliance of the DSA with data handling, retention and deletion requirements under Part VIII A



**Assessment 5** – Compliance of the DSA with the deletion and notification requirements in Part VIII A which relate to the end of the pandemic

### Assessment 1

The OAIC commenced Assessment 1 on 30 June 2020, focused on the Data Store and governance and protections in relation to access to the system. The Data Store is the database administered by or on behalf of the Commonwealth for the purpose of contact tracing.

The targets of the assessment are Health and the Digital Transformation Agency (DTA). Health is the policy lead for COVIDSafe and was the DSA up to 16 May 2020. The DTA was appointed the DSA under section 94Z of the Privacy Act from 16 May 2020 and currently manages the data collected by COVIDSafe.

The assessment is examining the steps taken by the DSA to comply with Australian Privacy Principle (APP) 11 to secure personal information held in the Data Store, and handling of COVID app data in accordance with Part VIII A of the Privacy Act.

The Commissioner has issued notices under section 94T(2) of the Privacy Act to the targets to give information and produce documents. The OAIC conducted fieldwork for the assessment in October and is drafting a report on the assessment.

## Assessment 2

On 7 October 2020, the OAIC commenced Assessment 2, focused on state and territory health authorities and governance and protections in relation to access to the system.

The assessment is examining the steps taken by state and territory health authorities to comply with APP 11, to secure personal information accessed from the Data Store, and the handling of COVID app data in accordance with Part VIIIA of the Privacy Act.

The targets of the assessment are the state and territory health authorities granted access to COVID app data from the Data Store for the purposes of contact tracing:

- Australian Capital Territory Department of Health
- New South Wales Department of Health
- Northern Territory Department of Health
- Queensland Department of Health
- South Australian Department of Health
- Tasmanian Department of Health
- Victorian Department of Health and Human Services
- Western Australian Department of Health.

The Commissioner has issued notices under section 94T(2) of the Privacy Act to the targets of the assessment to give information and produce documents relating to governance and access to the Data Store. The OAIC conducted fieldwork for the assessment in October and November 2020.

## Assessments 3 and 4

Assessment 3 focuses on the functionality of COVIDSafe against specified privacy protections set out under the COVIDSafe privacy policy and collection notices, and against the requirements of Part VIIIA. Assessment 4 examines the handling of COVID app data in relation to the retention and deletion requirements of Part VIIIA of the Privacy Act.

The targets of Assessment 3 are Health and the DTA. The target of Assessment 4 is the DTA.

The OAIC commenced Assessments 3 and 4 on 13 November 2020, issuing notices under section 94T(2) of the Privacy Act to the targets of these assessments.

## Inspector-General of Intelligence and Security COVIDSafe report

The Inspector-General of Intelligence and Security assists ministers in overseeing and reviewing the legality and propriety of the activities of 6 of Australia's intelligence and security agencies, including their compliance with Part VIII A of the Privacy Act. These agencies are:

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

The acting Inspector-General has reviewed the agencies' compliance with Part VIII A between 16 May 2020 and 16 November 2020 and provided an unclassified report for the Commissioner to consider in preparing a report under section 94ZB.

The *COVID app data and Intelligence Agencies within IGIS jurisdiction report* notes that:

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

IGIS advises that it plans inspection activities in coming months to verify data deletion and provide further assurance that no COVID app data has been accessed, used or disclosed.

The IGIS report is provided as Attachment A to this report and is also published on the [IGIS website](#).

# Glossary

Term	Definition
Contact tracing	<p>Section 94D(6): The process of identifying persons who have been in contact with a person who has tested positive for the coronavirus known as COVID-19, and includes:</p> <ul style="list-style-type: none"> <li>(a) notifying a person that the person has been in contact with a person who has tested positive for the coronavirus known as COVID-19; and</li> <li>(b) notifying a person who is a parent, guardian or carer of another person that the other person has been in contact with a person who has tested positive for the coronavirus known as COVID-19; and</li> <li>(c) providing information and advice to a person who: <ul style="list-style-type: none"> <li>(i) has tested positive for the coronavirus known as COVID-19; or</li> <li>(ii) is a parent, guardian or carer of another person who has tested positive for the coronavirus known as COVID-19; or</li> <li>(iii) has been in contact with a person who has tested positive for the coronavirus known as COVID-19; or</li> <li>(iv) is a parent, guardian or carer of another person who has been in contact with a person who has tested positive for the coronavirus known as COVID-19.</li> </ul> </li> </ul>
COVID app data	<p>Section 94D(5): Data relating to a person that:</p> <ul style="list-style-type: none"> <li>(b) has been collected or generated (including before the commencement of this Part) through the operation of COVIDSafe; and</li> <li>(c) either: <ul style="list-style-type: none"> <li>(i) is registration data; or</li> <li>(ii) is stored, or has been stored (including before the commencement of this Part), on a communication device.</li> </ul> </li> </ul> <p>However, it does not include:</p> <ul style="list-style-type: none"> <li>(d) information obtained, from a source other than directly from the National COVIDSafe Data Store, in the course of undertaking contact tracing by a person employed by, or in the service of, a State or Territory health authority; or</li> </ul>



- (e) de-identified statistical information about the total number of registrations through COVIDSafe that is produced by:
  - (i) an officer or employee of the data store administrator; or
  - (ii) a contracted service provider for a government contract with the data store administrator.

COVIDSafe app (COVIDSafe)	Section 6(1): An app that is made available or has been made available (including before the commencement of this Part), by or on behalf of the Commonwealth, for the purpose of facilitating contact tracing.
National COVIDSafe Data Store (Data Store)	Section 6(1): The database administered by or on behalf of the Commonwealth for the purpose of contact tracing.
National COVIDSafe Data Store Administrator (DSA)	The Digital Transformation Agency (DTA) was appointed as the DSA under the Privacy Act to manage the data collected by COVIDSafe.

## Attachment A:

### COVID app data and Intelligence Agencies within IGIS jurisdiction report



**IGIS**

INSPECTOR-GENERAL OF  
INTELLIGENCE AND SECURITY

## **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 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 declassified 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 at 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.