



Australian Government

Office of the Australian Information Commissioner

COVIDSafe Report November 2020–May 2021

Report under Part VIII A of the *Privacy Act 1988*



Angelene Falk

Australian Information Commissioner and Privacy Commissioner

17 June 2021

OAIC

Contents

About this report	2
Executive summary	3
Commissioner's powers	4
Enquiries	5
Assessments	6
COVIDSafe guidance and advice	4
Guidance for state and territory health authorities regarding COVIDSafe and COVID app data	7
Inspector-General of Intelligence and Security COVIDSafe report	8
Glossary	9
Attachment A: COVID app data and Intelligence Agencies within IGIS jurisdiction	11

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 or within 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 applies the Privacy Act's rules and privacy protections and Commonwealth oversight to state and territory health authorities in relation to COVID app data.

In accordance with section 94ZB of the Privacy Act, 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 period **16 November 2020 to 15 May 2021**.

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

During the reporting period of 16 November 2020 to 15 May 2021, the OAIC received 14 enquiries about COVIDSafe.

We also progressed the COVIDSafe Assessment Program and issued and promoted guidance in relation to the COVIDSafe system.

The Commissioner did not exercise her powers in relation to complaints, investigations, Commissioner-initiated investigations, information sharing and data breaches.

Commissioner's powers

The OAIC's [first COVIDSafe report](#) detailed the Commissioner's powers in relation to COVIDSafe and COVID app data.

During the reporting period of 16 November 2020 to 15 May 2021, the following matters were recorded in relation to Part VIIIA:

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

Regulatory function	Number
Enquiries	14
Complaints received	0
Investigations	0
Commissioner-initiated investigations	0
Information sharing	0
Assessments underway	4
Data breach notifications	0

COVIDSafe guidance and advice

During the reporting period, the OAIC developed and promoted COVIDSafe guidance to increase awareness and understanding of the system's privacy protections and entities' obligations under the Privacy Act.

The OAIC published [Guidance for state and territory health authorities regarding COVIDSafe and COVID app data](#). A summary of the guidance is provided later in this report.

We also updated our [guidance for individuals](#) on COVIDSafe to clarify that section 94H of the Privacy Act applies only to COVIDSafe and not to other contact tracing apps or QR codes.

The OAIC has continued to provide advice and guidance to the Australian Government on the development and implementation of COVIDSafe privacy protections.

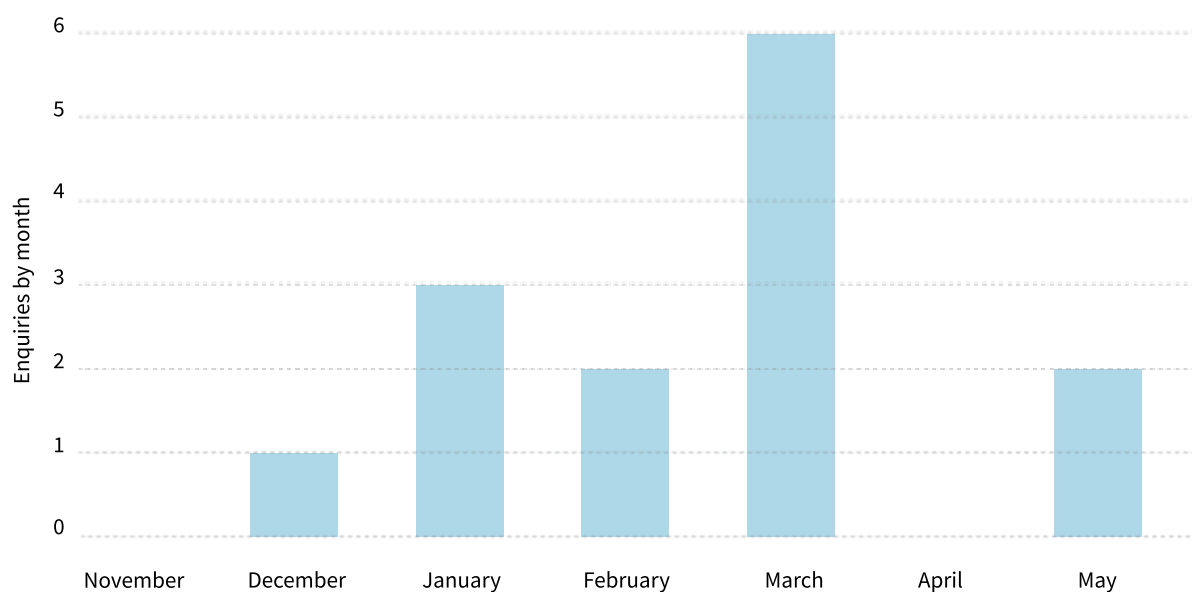
We have provided ongoing advice to the Department of Health regarding its [updated privacy impact assessment](#) for COVIDSafe and have continued to monitor implementation of the recommendations made in its [original COVIDSafe privacy impact assessment](#).

Enquiries

The OAIC received 14 enquiries about COVIDSafe during the reporting period, including 12 enquiries from individuals and 2 from businesses.

We provided general information in response to 11 enquiries and provided assistance on how to make a complaint in response to 3 enquiries.

Figure 1 — Enquiries about COVIDSafe received by month November 2020–May 2021



Types of enquiries

General enquiries or concerns about COVIDSafe

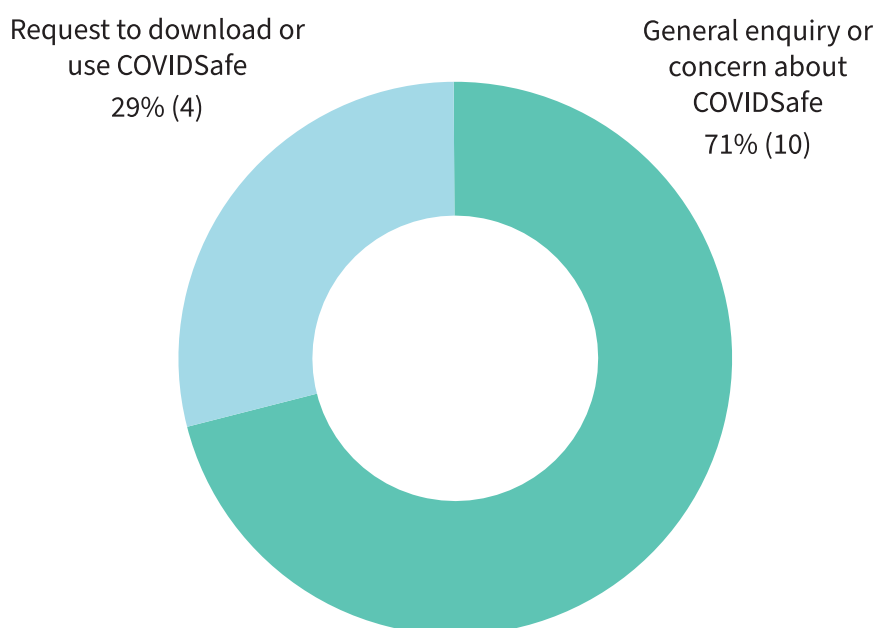
We received 10 enquiries raising general issues or concerns about COVIDSafe, including:

- an enquiry about the changes to the Privacy Act relating to COVIDSafe
- an enquiry from an individual seeking to delete data uploaded to the National COVIDSafe Data Store (Data Store).

Request to download or use COVIDSafe

We received 4 enquiries about a request to download or use COVIDSafe, including:

- an enquiry about a venue refusing an individual entry unless they used COVIDSafe or signed in using a QR code
- an enquiry about whether an employer could require an employee to download COVIDSafe.

Figure 2 — Types of enquiries about COVIDSafe received November 2020–May 2021

Assessments

Information about the OAIC's COVIDSafe Assessment Program is set out in the [first COVIDSafe report](#).

During the period covered by this report:

- The OAIC liaised with the targets of the assessments about information sharing protocols for the program.
- We reviewed documents and information provided by the targets of assessments 1 to 4.
- We planned fieldwork with the targets of assessments 2 to 4, which involved engagement with the Department of Health, the Digital Transformation Agency and all state and territory health authorities.
- We completed fieldwork for assessments 2, 3 and 4. For these assessments, the OAIC undertook a mix of in-person interviews and remote interviews via phone and video conference.
- We progressed draft reports for assessments 1 to 4.

Guidance for state and territory health authorities regarding COVIDSafe and COVID app data

In December 2020, the OAIC published guidance to help state and territory health authorities understand their privacy obligations under Part VIIIA of the Privacy Act.

Among the key points in the guidance:

- The Privacy Act, except for Australian Privacy Principle (APP) 9, applies to state and territory health authorities' handling of COVID app data. This includes APP 11, which requires organisations to take reasonable steps to protect data from misuse, interference, loss, unauthorised access, unauthorised modification and unauthorised disclosure.
- COVID app data is and remains the property of the Commonwealth, even after it has been disclosed to or used by a state or territory health authority.
- State and territory health authorities may only collect, use or disclose COVID app data for the purpose of conducting contact tracing and only to the extent required to undertake that contact tracing.
- COVIDSafe is voluntary – no individual, organisation or government agency can require any individual to download or use the app or upload their data to the Data Store.
- Consent must be obtained from an individual before uploading data about their close contacts to the Data Store.
- COVID app data must be stored on a database in Australia. This includes COVID app data that has been downloaded into a state or territory health authorities' data store.
- A breach of any of the COVID app-related provisions in Part VIIIA by a state or territory health authority will be considered an 'eligible data breach' under the Notifiable Data Breaches scheme.
- The OAIC can conduct assessments of whether the acts or practices of a state or territory health authority comply with the privacy obligations in Part VIIIA.

The guidance is available at [oaic.gov.au/guidance-for-state-and-territory-health-authorities-regarding-covidsafe-and-covid-app-data](https://www.oaic.gov.au/guidance-for-state-and-territory-health-authorities-regarding-covidsafe-and-covid-app-data).

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 Inspector-General has reviewed the agencies' compliance with Part VIII A between 16 November 2020 and 15 May 2021 and provided an unclassified report for the Commissioner to consider in preparing this report.

The report notes:

- The Inspector-General remains satisfied that the agencies have appropriate 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 has deliberately targeted, or decrypted, accessed or used any COVID app data. IGIS also found the agencies are taking reasonable steps to quarantine and delete such data as soon as practicable after becoming aware of it.
- IGIS has not received any complaints or public interest disclosures about COVID app data.

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

Glossary

Term	Definition
Australian Privacy Principles (APPs)	<p>The APPs are the cornerstone of the privacy protection framework in the Privacy Act 1988. They apply to any organisation or agency the Privacy Act covers.</p> <p>There are 13 APPs and they govern standards, rights and obligations around:</p> <ul style="list-style-type: none"> • the collection, use and disclosure of personal information • an organisation or agency's governance and accountability • integrity and correction of personal information • the rights of individuals to access their personal information.
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"> (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 (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 (c) providing information and advice to a person who: <ul style="list-style-type: none"> (i) has tested positive for the coronavirus known as COVID-19; or (ii) is a parent, guardian or carer of another person who has tested positive for the coronavirus known as COVID-19; or (iii) has been in contact with a person who has tested positive for the coronavirus known as COVID-19; or (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.
COVID app data	Section 94D(5): Data relating to a person that:

- (b) has been collected or generated (including before the commencement of this Part) through the operation of COVIDSafe; and
- (c) either:
 - (i) is registration data; or
 - (ii) is stored, or has been stored (including before the commencement of this Part), on a communication device.

However, it does not include:

- (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
- (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

COVID app data and Intelligence Agencies within IGIS jurisdiction

16 November 2020 – 15 May 2021

Second Report



The Hon Christopher Jessup QC
Inspector-General of Intelligence and Security

17 May 2021

IGIS Report to OAIC on COVID app data – 16 November 2020 to 15 May 2021

Background

This is the second report¹ by the Inspector-General of Intelligence and Security regarding intelligence agencies within jurisdiction and their compliance with Part VIIIA of the *Privacy Act 1988* (the Privacy Act). This report is provided to the Privacy Commissioner so that she may take this information into account when preparing her report under s 94ZB of the Privacy Act.

Summary of findings to date

The Inspector-General's staff have continued to work with relevant² agencies to monitor their activities in ensuring compliance with Part VIIIA of the Privacy Act. We remain satisfied that these agencies have appropriate policies and/or procedures in place and are taking reasonable steps to avoid intentional collection of COVID app data.

In addition to ongoing monitoring, IGIS staff have conducted inspections of these agencies to determine whether COVID app data that has been collected incidentally as part of agency functions has not been accessed or used, and that any COVID app data has been deleted as soon as practicable after the agency becomes aware it has been collected. The key findings from these inspections are as follows:

- Appropriate procedures remain in place and continue to be followed regarding any incidental collection of COVID app data that is identified.
- While relevant agencies have incidentally collected COVID app data, which the Privacy Act recognises may occur, IGIS has found that there is no evidence to suggest that these agencies have deliberately targeted or have decrypted, accessed or used such data.
 - Relevant agencies are also taking reasonable steps to quarantine and delete such data as soon as practicable after the agency becomes aware it has been collected.
- IGIS notes that there are ongoing discussions between relevant parties regarding the application of the prohibition against 'disclosure' as set out in s 94D of the Privacy Act.

Complaints

- No complaints or public interest disclosures about COVID app data have been received.

Next steps

- IGIS will continue to review how COVID app data is being handled by relevant agencies within IGIS jurisdiction, including the appropriateness and effectiveness of policies and procedures.

¹ For context this report should be read together with the first report available at www.igis.gov.au/what-we-do/inspections/cross-agency-matters

² Not all intelligence agencies with IGIS's jurisdiction have functions or technical capabilities which may enable them to collect COVID app data.