Australian Government

Office of the Australian Information Commissioner

COVIDSafe Report November 2021–May 2022

Report under Part VIIIA of the *Privacy Act 1988*

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

14 June 2022

OAIC

Contents

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*.

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.

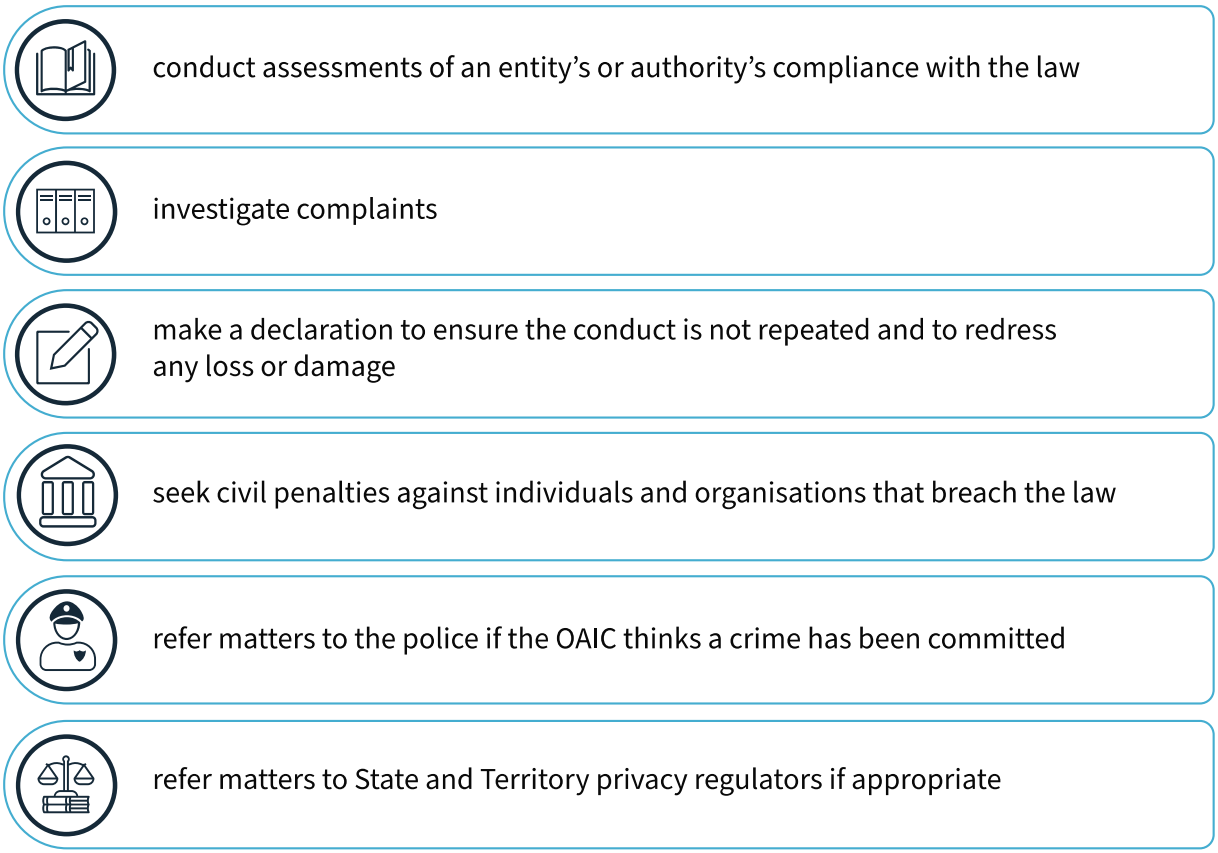
It enhances the Commissioner's role in dealing with eligible data breaches and conducting assessments and investigations in relation to COVIDSafe and COVID app data. It enables the Commissioner to refer matters to, and share information or documents with, state or territory privacy authorities. It also 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 2021 to 15 May 2022**.

Executive summary

The Commissioner has an independent oversight function for the COVIDSafe system under the Privacy Act and is actively monitoring and regulating compliance. The Commissioner has powers to:



During the reporting period 16 November 2021 to 15 May 2022, the OAIC received **no enquiries or complaints** about the COVIDSafe system.

We progressed the COVIDSafe Assessment Program, finalising **one assessment**.

The Commissioner was not required to 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 the COVIDSafe system.

During the reporting period of 16 November 2021 to 15 May 2022, the following matters were recorded in relation to Part VIIIA:

Table 1 — Number of matters related to the COVIDSafe system

Regulatory function	Number
Enquiries received	0
Complaints received	0
Investigations	0
Commissioner-initiated investigations	0
Information sharing	0
Assessments finalised	1
Assessments underway	1
Data breach notifications received	0

Assessments

We detailed our COVIDSafe Assessment Program in the first COVIDSafe report. In relation to that program, during the period covered by this report the OAIC finalised COVIDSafe Assessment 4 and progressed 8 individual reports for Assessment 2 in relation to the state and territory health authorities.

Summary of COVIDSafe Assessment 4

Assessment 4 examined the retention, destruction and deletion of COVID app data by the National COVIDSafe Data Store Administrator. The final report for Assessment 4 was published on 7 April 2022.

At the time the fieldwork for this assessment was conducted, the Digital Transformation Agency (DTA) was the sole Data Store Administrator. Between 27 September and 4 October 2021, this function transitioned to the Department of Health. From 5 October 2021, Health is the sole Data Store Administrator and the DTA no longer has access to COVID app data and information collected through COVIDSafe.

The assessment found:

- while the Data Store Administrator was taking all reasonable steps to delete registration data, it can take steps to address privacy risks for COVIDSafe users who:
  - do not reply to the text message to confirm their deletion request
  - enter an incorrect mobile number into the 'Request data deletion' webform.
- the Data Store Administrator had not implemented measures to prevent use or disclosure of registration data that cannot be immediately deleted after receiving a request for deletion, creating a privacy risk.
- the Data Store Administrator was complying with s 94N of the Privacy Act in relation to individuals who opt out of using COVIDSafe.

The OAIC made 3 recommendations and 2 suggestions to address privacy risks. The recommendations, suggestions and Data Store Administrator's responses are outlined in parts 3 and 4 of the report.

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 VIIIA 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 VIIIA between 16 November 2021 and 15 May 2022 and provided an unclassified report for the Commissioner to consider in preparing this report.

The report notes:

- There is no evidence that any agency has deliberately targeted or decrypted, accessed or used any COVID app data.
- Incidental collection in the course of the lawful collection of other data has occurred (and is permitted by the Privacy Act). IGIS found the agencies have appropriate policies and procedures in place regarding any incidental collection of COVID app data and are adhering to them. Agencies are taking reasonable steps to quarantine and delete such data as soon as practicable after becoming aware it has been collected.
- 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)	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. There are 13 APPs and they govern standards, rights and obligations around: • 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	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: (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: 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: (a) has been collected or generated (including before the commencement of this Part) through the operation of COVIDSafe; and (b) either: is registration data; or i. is stored, or has been stored (including before the commencement of this Part), on a communication device. ii. However, it does not include: (c) 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 (d) 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 (Data Store Administrator)	From 16 May 2020 to 26 September 2021, the Digital Transformation Agency (DTA) was the sole Data Store Administrator. Between 27 September and 4 October 2021, this function transitioned to the Department of Health (Health). From 5 October 2021, Health is the sole Data Store Administrator and the DTA no longer has access to COVID app data and information collected through COVIDSafe.

Attachment A: COVID app data and Intelligence Agencies within IGIS jurisdiction

IGIS
INSPECTOR-GENERAL OF INTELLIGENCE AND SECURITY

COVID app data and Intelligence Agencies within IGIS jurisdiction

16 November 2021 – 15 May 2022

Fourth Report

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

16 May 2022

IGIS Report to OAIC on COVID app data – 16 November 2021 to 15 May 2022

Background

This is the fourth six-monthly report[1] by the Inspector-General of Intelligence and Security (IGIS) 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

The Inspector-General's staff have continued to work with relevant[2] agencies to monitor their activities in ensuring compliance with Part VIIIA of the Privacy Act. IGIS staff have also conducted inspections of these agencies to determine whether COVID app data that has been collected incidentally[3] has not been accessed or used, and is deleted as soon as practicable after the agency becomes aware it has been collected.

The key findings from these inspections are as follows:

- There is no evidence to suggest agencies have deliberately targeted or have decrypted, accessed or used COVID app data.
- Relevant agencies continue to take reasonable steps to quarantine and delete COVID app data.
    - This office will continue to work with those agencies to ensure that processes and procedures ensure that deletion occurs as soon as practicable.
- Appropriate policies and procedures remain in place and are being adhered to regarding any incidental collection of COVID app data that is identified.

Prohibition against 'disclosure'

The proposed discussions between relevant agencies and the OAIC regarding the application of the prohibition against disclosure as set out in s 94D of the Privacy Act, identified in the November 2021 report have begun, but have not yet concluded. The Inspector-General continues to request the relevant intelligence agencies to progress these discussions with the OAIC as a matter of priority.

Complaints

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

Next steps

- IGIS will continue to engage with the Office of the Australian Information Commissioner to ensure our oversight activities, as they relate to the COVID app data, remain useful and valuable. .
- IGIS will continue to review how COVID app data is being handled by relevant agencies within IGIS jurisdiction, including reviewing the appropriateness and effectiveness of policies and procedures.

---

[1] The first three reports are 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.

[3] The Privacy Act recognises that incidental collection of COVID app data may occur as part of agency functions.