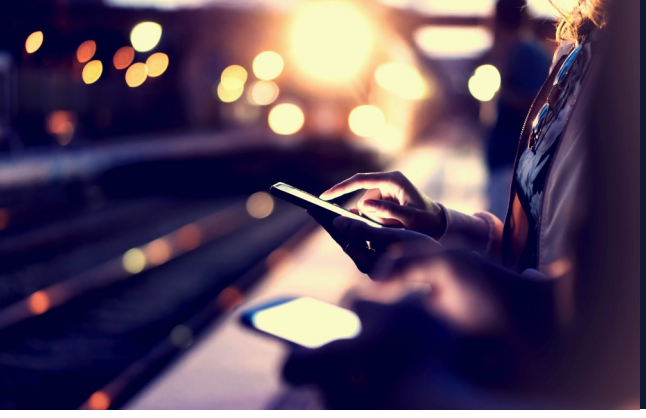

The COVIDSafe app – Recent changes to the law and your privacy

Author: Royce Tout

Privacy concerns have plagued the introduction of the COVIDSafe app (**App**). In response, strict privacy protections for users of the App have now been enshrined in law via *The Privacy Amendment (Public Health Contract Information) Act* 2020 (**the Act**) which introduces Part VIIIA into the *Privacy Act* 1988 (Cth) (**Privacy Act**). In line with community expectations, the Act imposes strong privacy protections and strict requirements on the collection, use and disclosure of App data.

What is COVID App data?

Given App data is what the Act is designed to protect, it is important to firstly delineate what constitutes App data. Under the Act, App data is data relating to a person that has been:

1. collected or generated via the App; and
2. that is stored on a mobile telecommunication device.

Overview of regulatory protections

The Act provides that:

- Data uploaded through the App which is stored in the Data Store must be used for the principal purpose of facilitating COVID–19 contact tracing activities by State and Territory heath authorities. Collecting, using or disclosing App data for a purpose that is not related to contact tracing is a criminal offence. The misuse of App data, such as decrypting App data stored on a communication device is also a criminal offence. Data held in the data store must be retained in Australia, and not be disclosed to a person outside of Australia (except for the purposes of contact tracing by a State or Territory Government health official).
- A breach of any of the above principles attracts a maximum penalty of 5 years imprisonment or a $63,000.00 fine.
- Any data relating to an individual is classified as 'personal information' under the Privacy Act.
- The Office of the Australian Information Commissioner (**AIC**) has the power to investigate complaints about breaches of the Act. The AIC has the ability to require State and Territory Authorities to co-operate with investigations, and to refer matters where appropriate to the Commissioner of Police or the Director of Public Prosecutions (**DPP**) to investigate criminal offences. The AIC also has the power to refer matters to, and share information with State and Territory privacy regulators as appropriate. The scope of the AIC's powers in relation to State and Territory authorities is strictly limited to COVID App data.
- The Act requires State and Territory Health Officials to notify the AIC about data breaches involving App data that are likely to cause serious harm. Once notified of a potential breach, the Commissioner can then require the notifying entity/individual to prepare a statement, and take reasonable steps to provide that statement to individuals to whom the App data relates.
- The Act operates in place of any inconsistencies with other laws, including less strict requirements about personal information under the Privacy Act.

Your rights

There are important measures within the Act that users and potential users should be aware of:

- The use of the App is voluntary and your informed consent is required to allow the App to collect and upload data to the Data Store.
- Users may request the deletion of data uploaded from your device. When the Data Store receives a user's request, they must take all reasonable steps to delete the data.
- The Act also includes a requirement to delete App data received in error and imposes an obligation to delete App data from the National Store at the end of the data period. This will likely occur once the threat of COVID-19 passes, but will ultimately be determined by the Health Minister.

Our analysis

The Act offers a significant amount of privacy protection for App users. The powers afforded to the AIC under the Act also provide a rigorous oversight regime.

There are however some important issues that need to be highlighted and ultimately require further guidance:

1. Data breach notifications are not required in cases that may interfere with a police investigation into an offence committed under the Act. Further, the Commissioner has discretion to grant an exemption, or a time-limited exemption from the notification requirement on public interest grounds. Although this ensures that, for example, the Police may execute their powers efficiently, it does fly in the face of the purpose of the Act, which is to ensure transparency and protection with regard to a user's personal information;
2. While the App does not collect personal or location data, this does not mean that these details cannot be inferred from the data that is collected. This leads to the further question of whether data that is derived from App data will be subject to the protections of the Act; and
3. Only data collected from mobile telecommunications is protected by the Act. There remains conjecture as to whether SIM-less devices, such as IPad's and tablets fall under the definition of mobile telecommunications devices. Clearly, this is an issue if users choose to use these devices when downloading and using the app.

Generally the Act adequately addresses several privacy concerns by providing a significant level of protection for App users. Although we are yet to see an offender prosecuted under the Act, the threat of 5 years imprisonment or a $63,000.00 fine is a significant deterrence to the misuse of App data. Further, the wide powers of the AIC establish a strong enforcement and oversight regime. However, some issues remain unresolved, leaving room for privacy concerns to arise.

If you are having difficulty with ascertaining your rights under the Act, or have privacy concerns with regarding the App, please contact Jimmy Gill on 02 8235 1239 or your usual ClarkeKann contact.

61 2 8235 1222
Level 4 , 9 Castlereagh Street, Sydney
NSW 2000
www.clarkekann.com.au/