Rachel Stephen-Smith MLA
Minister for Health
Minister for Families and Community Services
Minister for Aboriginal and Torres Strait Islander Affairs

Member for Kurrajong

Mr Jeremy Hanson MLA
Chair
Standing Committee on Justice and Community Safety (Legislative Scrutiny Role)
ACT Legislative Assembly
CANBERRA ACT 2601

Dear Chair

I write in relation to the Standing Committee on Justice and Community Safety's (Legislative Scrutiny Role) comments on the COVID-19 Emergency Response (Check In Information) Amendment Bill 2021 (the Bill) in Scrutiny Report 8 of 24 August 2021 .

I note the Bill is scheduled for debate on 16 September 2021 and apologise for the delay in responding to the Committee.

The objective of the Bill is to displace the power of a Territory or Court or Tribunal to impose an order requiring production of documents, records or information collected by the Check in CBR app (the App). The Bill also seeks to limit the use of 'check in information' to contact tracing or associated purposes. There is no suggestion that this has occurred in the ACT however these amendments to the *COVID-19 Emergency Response Act 2020* (the Act) will entrench in primary legislation that personal information collected about individuals by the App:

a. is provided directly to, and stored by, ACT Health; and
b. is stored for 28 days and is then deleted (unless the person is subject to an investigation or prosecution for failing to comply with the Public Health Emergency (Check In Requirements) Direction or gives false or misleading information about contact tracing); and
c. can only be used for contact tracing and contact tracing compliance purposes.

Legislative provisions contained in the Bill are unique to the COVID-19 public health emergency and our efforts to minimise transmission of this disease. These provisions are only necessary during the public health emergency. As such, the *COVID-19 Emergency Response Act 2020* is the most

ACT Legislative Assembly London Circuit, GPO Box 1020, Canberra ACT 2601
+61 2 6205 2661 stephen-smith@act.gov.au
@RachelSS_MLA rachelSSMLA rachelss_mla

appropriate Act for the amendments, both because of its stated purpose of providing emergency measures in response to the COVID-19 emergency, and because it contains provisions designed to offer community assurance, specifically in relation to parliamentary oversight through section 3 of the Act. Furthermore, the entire Act is to expire "at the end of a 12-month period during which no COVID-19 declaration has been in force".

As the Committee will be aware, contact tracing is a vital component of the public health response to COVID-19 in the ACT and is a mandatory requirement under the ACT's Public Health (Check In Requirements) Emergency Direction 2021 (the Direction), which sets out the requirements for checking in. The App ensures that personal data collected at check in is provided directly to ACT Health and not through a third party. Personal data can only be accessed by ACT Health (if necessary) for contact tracing, which would be if there is a suspected or confirmed positive case of COVID-19.

The ACT Government has been very clear that personal data collected by the App can only be accessed or used for contact tracing purposes and is deleted after 28 days in accordance with the privacy policy for the App. These amendments will further strengthen the privacy provisions by establishing this in primary legislation. As 'checking in' is mandatory in certain businesses and settings as established in the Direction, it is necessary that a provision be included to enable investigation and prosecution of a breach of the Direction, similar to Western Australia's check in requirements legislation.

I note that the Committee's comments centre around whether the Bill protects other information from misuse, which would have been collected in any case for a purpose other than contact tracing, but is then disclosed for contact tracing purposes.

The Committee has outlined that Part 2C of the Bill defines check-in information as:

(a) information about the presence of a person at a place in the ACT, collected for the purpose of contact tracing; but

(b) does not include—

i. information collected in the ordinary course of carrying on a business, activity or undertaking if the information would have been collected in any case for a purpose other than contact tracing.

The Committee is concerned that to exclude (b)(i) above (hereafter 'ordinary business records') from the definition of 'check-in information' would mean that this information would not be afforded the same protection under the Bill as check-in information.

The protections that are afforded under the amendments made by this Bill operate to limit:

1. the collection of check in information to the App, or in a way permitted under the public health direction (2D); and

2. the use of check in information to an authorised person for a purpose related to and including contact tracing (2E).

The Bill is not intended to capture information which a business would have ordinarily captured in the absence of a Public Health Emergency, such as staff attendance records or booking records, even where that information may be used to assist in contact tracing.

There would likely be a number of unintended consequences of including ordinary business records in the definition of check-in information, including requiring a business to destroy its ordinary business records, which it might have otherwise been required to retain under a number of legislative requirements, including the *Fair Work Act 2009* or for tax purposes.

Separately, ACT Health's obligations in relation to handling of various information is already regulated under the *Information Privacy Act 2014* and the *Health Records (Privacy and Access) Act 1997*. The objects of the Information Privacy Act include promoting responsible and transparent handling of personal information by public sector agencies and contracted service providers.

Given the protections already in place and the potential unintended consequences outlined above, the Bill does not seek to displace obligations that remain with the business who collected ordinary business records under existing legislation, as well as the Territory's obligations under various privacy legislation.

The Bill is not intended to capture information which it obtains for contact tracing through other methods outside of the App, as the collection, use and disclosure of such information is already subject to robust legislative protections. As such, I am content that the definitions in the Bill are appropriate and support the objectives of the Bill.

I also note that the Bill has been prepared during a public health emergency and is responsive to the concerns of the ACT Human Rights Commissioner about the adequacy of the existing privacy protections that apply to personal information specifically collected by the App.

I acknowledge that the nature of check-in information collected through the App is more intrusive on the privacy of an individual, providing a detailed window of where individuals have been in the ACT, however this has been a vital and significant tool to assist ACT Health in its contact tracing efforts. The community use and compliance has been invaluable in ACT Health's efforts to respond to this unique public health emergency and the Bill is unique in addressing the need to secure personal information collected in the context of the emergency requiring the use of the App in various settings.

The Committee also queried "how the limitations on use by authorised persons of check-in information is intended to be enforced". ACT Health understands this to be a query into how the Bill would protect misuse of check-in information by an authorised person (as defined by the *Public Health Act 1997*).

ACT Health considers there to be existing legislative protections which protect the misuse of information by a public servant. Those protections include the *Public Sector Management Act 1994*, which requires a public servant to comply with and actively demonstrate the ACT Public Service (ACTPS) Values and Signature Behaviours.

A public servant must comply with laws applying in the Territory in connection with their job. This includes a requirement that public servants follow the privacy principles contained within the *Information Privacy Act 2014* and comply with the *Health Records (Privacy and Access) Act 1997*.

If a public servant is found to have acted in a way that is inconsistent with the ACTPS Values and Signature Behaviours, it may result in a finding that the public servant has engaged in misconduct. There are a range of sanctions which may be applied to a person found to have engaged in misconduct with one of the most serious sanctions being termination of employment.

Additionally, section 153 of the *Crimes Act 1900* makes it an offence for a public employee to publish or communicate, to an unauthorised individual, information which is gained through the public servant's job and where there is a duty not to disclose that information.

I trust that the Bill will introduce additional safeguards for personal information collected through the App and provide additional confidence to the community that personal information collected through this novel way is protected from disclosure and limited to the purpose for which it was intended being contact tracing to prevent the spread of COVID-19 in our community.

I trust that this information assists in addressing the Committee's comments.

Yours sincerely

Rachel Stephen-Smith MLA