28 May 2020

Parliamentary Joint Committee on Human Rights
PO Box 6100,
Parliament House
Canberra ACT 2600

By Email: human.rights@aph.gov.au

Dear Committee Secretariat,

RE: COVID-19 LEGISLATIVE SCRUTINY

We appreciate this opportunity to make submissions in relation to the COVID-19 Legislative Scrutiny.

EFA's submission is contained in the following pages; however, at the outset, it is imperative to appreciate that Australia (unlike any other Western democratic nations) does not have an enforceable federal human rights framework nor does our law recognise a tort for serious invasions of privacy. These fundamental regimes are integral to ensuring that legislation made today is not capable of abuse in the future.

We are agreeable to this submission being published publicly.

Established in January 1994, EFA is a national, membership-based non-profit organisation representing Internet users concerned with digital freedoms and rights. EFA is independent of government and commerce, and is funded by membership subscriptions and donations from individuals and organisations with an altruistic interest in promoting civil liberties in the digital context.

EFA members and supporters come from all parts of Australia and from diverse backgrounds. Our major objectives are to protect and promote the civil liberties of users of digital communications systems (such as the Internet) and of those affected by their use and to educate the community at large about the social, political and civil liberties issues involved in the use of digital communications systems.

Yours sincerely,

Angus Murray
Chair of the Policy Committee
Electronic Frontiers Australia

Submission

1. We are grateful for the Committee's resolution to engage in ongoing monitoring of legislative reform in response to the COVID-19 pandemic and we note that approximately 165 Bills have passed since 21 January 2020.

2. It is trite that these are testing times and that the COVID-19 pandemic has been a historic moment and the world has forever changed as a consequence. In our view, there is also the potential for the rapid response to the pandemic to be a momentous detriment to the fundamental rights that ought to be enjoyed by future generations.

The Human Rights Framework

3. Firstly, we appreciate that the committee recognises that the federal bills and instruments being made in response to this COVID-19 pandemic may have significant human rights implications.

4. It has been our longstanding position that a significant issue with respect to legislative reform that engages human rights issues in Australia is the lack of an enforceable human rights framework at a federal level and the introduction of a statutory tort for serious invasion of privacy[1].

5. In this context, and with regard to the Committee's Human Rights Scrutiny Report (Report 6 of 2020) and its Human Rights Scrutiny Report of COVID-19 Legislation (Report 5 of 2020), we agree that there is a need for a response to the pandemic; however, it ought to be considered abhorrent to good governance for the legislature to fail to provide human rights implication and privacy impact assessments alongside legislation, even in circumstances where such assessments are not expressly required (although should be produced).

6. In this context, and whilst we have serious concerns about privacy impact assessments being issued at the same time as a Bill, we do appreciate that legislation passed in response to the COVID pandemic was necessarily passed quickly. However, it is equally important that legislation is repealed quickly and that this situation is used to appropriately and holistically consider Australians' human rights.

[1] It is relevant to note that the Human Rights Commissioner has also recommended the introduction of a tort for serious invasion of privacy in his recent Human Rights and Technology Discussion Paper and that this right has also been recommended by the Australian Law Reform Commission and the Productivity Commission, see: https://humanrights.gov.au/about/news/human-rights-and-technology-discussion-paper-launches

The "COVIDSafe" app

7. In our view, the COVIDSafe App warrants a great degree of scrutiny particularly in terms of the procurement of the app, the operation of the app, the messaging around the app and the normative shift as consequence of the app.
8. Firstly, we are concern to ensure that the Committee focuses on the Government's messaging around the app with members of government expressing that the app is "like sunscreen"[2] and abusively bargaining that downloading the assertedly voluntary app would allow government to give Australians back pubs and sports[3]. These statements are abusive, unfair and manipulative and ought to be deeply criticised. If the government was acting in a responsible and representative manner focused on the preservation of human rights it would have focused on educating people about the operation and risks associated with the app and placed greater weight and focus on safe hygiene rather than coercion into downloading an app facilitated by a foreign, profit driven, company.

9. It is our concern that the COVIDSafe App was produced in a secretive manner by the Department of Home Affairs and information regarding the app was only made available after significant public pressure was placed upon the Federal government.

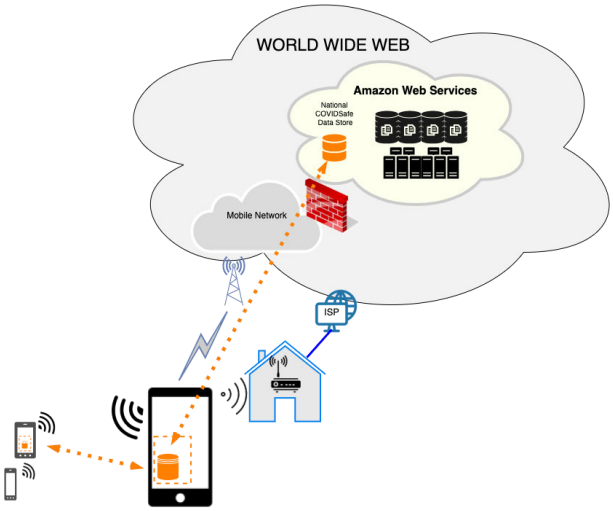
10. We note that the source code has not yet been made clearly available for scrutiny (which would be best achieved by making the source code available as open source). This causes concern regarding the transparent function of the app as well as ensuring that the app is subject to robust testing to ensure that it is truly "safe" (and we explain this concept below).

11. The Federal Government has a woeful track record of tech and data privacy disasters including My Health Record, Census Fail, Robodebt, the Data Retention scheme and My Gov crashing just when Australians needed it most.

12. We are also deeply concerned that the government's role in relation to the COVIDSafe App has been to procure a private and foreign entity[4] to develop an application that deeply affects Australians' data. Specifically, our concern is that Amazon (indeed any company but particularly foreign companies) has a different mandate to that of a democratic nation. Namely, the company is beholden to its shareholders whose interest lie with commercial profit whereas the sovereign citizens' interest lines with the preservation of autonomy and human dignity - the fundamental premises of human rights. The alienation of the sovereign in this process ought to be the subject of deep and forceful review as this is a precedent that must be unwound and critiqued to the fullest extent.

[2] https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant.
[3] https://7news.com.au/lifestyle/health-wellbeing/download-app-for-pubs-to-reopen-morrison-c-1012475.
[4] ITNews - 'Government Services Minister Insists COVID Tracing App Data Safe on AWS'. n.d. ITnews. Accessed 17 May 2020. https://www.itnews.com.au/news/government-services-minister-insists-covid-tracing-app-data-safe-on-aws-547185.

13. As we understand, the COVIDSafe App could be graphically depicted as follows:



14. The COVIDSafe application utilises many technical aspects to achieve its goal. From the end users' smartphone where the application is executed, bluetooth technology to enable contact tracking, and the data stored on the phone, to the way that data travels to the National COVIDSafe datastore which is then housed on servers hosted by Amazon Web Services[5].

15. Smartphones (indeed all IoT devices) are notoriously difficult to secure and Bluetooth technology is known for its extreme complexity and difficulty in securing compared to other wireless technology.

16. Bluetooth technology and related devices are vulnerable[6] to common wireless networking threats:

    - denial of service (DoS) attacks
    - eavesdropping
    - message modification
    - man-in-the-middle (MITM) attacks
    - message modification
    - resource misappropriation
    - unauthorised access to Bluetooth device
    - unauthorised entry point to via Bluetooth devices to key systems and networks.
    - vulnerabilities in implementation

[5] 'Dutton Opens Door to New Surveillance of Journalists via Foreign Orders'. 2020. Crikey. 15 May 2020. https://www.crikey.com.au/2020/05/15/dutton-surveillance-journalist-foreign-orders/.
[6] See: Padgette, John, John Bahr, Mayank Batra, Marcel Holtmann, Rhonda Smithbey, Lily Chen, and Karen Scarfone. 2017. 'Guide to Bluetooth Security'. NIST SP 800-121r2. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-121r2.

17. There are also Specific Bluetooth-related attacks such as the below which ought to be understood as a serious risk to Australians' privacy and security including:

    - bluesnarfing.
    - bluejacking
    - bluebugging
    - fuzzing attacks
    - secure Simple Pairing Attacks

18. When the data leaves the User's phone, the means and responsibility of securing and safeguarding citizens economically valuable datasets rest in the hands of the Australian government and an American multinational corporation to ensure that privacy rights are not violated, and that these personal datasets do not make its way into the surveillance capitalism, of which Amazon is completely invested in.

19. There is also the important issue as to whether the data will be accessible by the United States due to the Cloud Act as the data is stored in the cloud on Amazon Web Services who are a US-incorporated business subject to the US Cloud Act. The Cloud Act requires cloud services to produce data held by them regardless of where internationally that data is stored if required to do so by subpoena.

20. Whilst the COVIDSafe App has been cased in the context of a legislative framework that speaks strongly of privacy protection (and this should be a precedent for all future legislation regarding government use of technology), it is not yet clear whether the United States is technically able to access Australian information. If there is any possibility of foreign access to Australian data, the system should be immediately shut down as Australia does not control the legislative direction of foreign governments who may later see value in the technical ability to access Australians' personal information.

21. In relation to the domestic legislative intent, we are concerned to ensure that the Committee understands the COVID-19 legislation during its scrutiny in the context of a much wider surveillance regime including mandatory data retention, whistleblower legislation, assistance and access amendments made to telecommunications and criminal law in 2018 and the seemingly endless assumption of power by the Home Affairs portfolio.

22. Simply stated - the COVID19 legislation cannot be looked at in isolation against the rapid increase of surveillance focused legislation in Australia and the significant disparity that has arisen between the State's law enforcement tools and the citizens' fundamental human rights.

23. We trust that this submission is of assistance to the Committee and please do not hesitate to contact Mr Angus Murray, Chair of the Policy Committee - Electronic Frontiers Australia should you require any further assistance or information.