Submission to the PJCIS

on the proposed

Australian Security Intelligence Organisation Amendment Bill 2020

Digital Rights Watch

Overview

We welcome the opportunity to submit comments to the Parliamentary Joint Committee on Intelligence and Security (PJCIS) concerning the Department of Home Affairs' proposed *Australian Security Intelligence Organisation Amendment Bill 2020* amending the *Australian Intelligence Organisation Act 1979.*[1]

While our comments below are limited to the technical aspects over the Bill which most fall under our mandate, we are concerned about the scope of powers prescribed in the draft text and we would like to iterate our support of the Human Rights Law Center effort to raise the age of criminal responsibility.[2]

Due to the topical overlap of this Bill with the Assistance and Access Act (TOLA) we would also like to draw the Committee's attention to our submissions regarding the Act's impact on human rights and freedoms:

- INSLM review of the Assistance and Access Act https://digitalrightswatch.org.au/2019/09/13/inslm-review-of-the-assistance-access-act/
- PJCIS review of the Assistance and Access Act https://digitalrightswatch.org.au/2019/07/10/submission-to-pjcis-on-the-review-of-the-telecommunications-and-other-legislation-amendment-assistance-and-access-act-2018/

Digital Rights Watch

Digital Rights Watch is a charity organisation founded in 2016 whose mission is to ensure that people in Australia are equipped, empowered and enabled to uphold their digital rights. We stand for Privacy, Democracy, Fairness & Freedom in a digital age. We believe that digital rights are human rights which see their expression online. We educate, campaign, lobby and advocate for a digital environment where individuals have the power to maintain their human rights.

General remarks

On 15 May 2020, the Department of Home Affairs released the draft *Australian Security Intelligence Organisation Amendment Bill 2020 ("the Bill")* amending the *Australian Intelligence Organisation Act 1979.* While the protection of the Australian community is obviously important, it is incumbent on the Government to ensure that this is achieved in a

[1] The full text of the Bill: https://www.homeaffairs.gov.au/nat-security/files/asio-amendment-bill-2020.pdf

[2] "All Australian Governments should raise the age of criminal responsibility because it is the right thing to do, because it is evidence-based, and because the recommendations of the NT Royal Commission present a rare opportunity to embrace this change." More at: https://www.hrlc.org.au/factsheets/2018/2/8/explainer-raising-the-age

manner which is necessary and proportionate to human rights guaranteed under international law.[3]

The Bill builds on TOLA's overbroad powers -- which are still under PJCIS as well as INSLM review and subject to change -- with no additional oversight and without a substantive justification beyond convenience for the agency. Given the evolving status of TOLA and the ongoing debate in the PJCIS over necessity and proportionality of infringing upon individual's privacy by appropriating private technologies as tools for law enforcement and intelligence, we recommend that consideration of the Bill be suspended until TOLA has been adequately amended.

We are extremely concerned about the changes proposed to the definition of 'tracking device.' While physical surveillance or the installation of devices can be cumbersome, it is by its physical nature subject to safeguards and protections which are too easily brushed aside when dealing with mobile devices and remote tracking. The perception of an activity when carried out in the physical world provides something of a sanity check which remote tracking lacks -- often resulting in abuse and overuse of such powers.[4] It generates an important (though insufficient) practical barrier to the endless expansion of mass surveillance, which can be so easily operationalised in the digital age.

As with TOLA, Home Affairs is seeking to use privately owned devices as an extension of the government's power, constituting a gross violation of an individual's privacy and sense of self-determination. Furthermore, remotely operating tracking malware on an individual's device can have unforeseen impacts on the security and integrity of their device, ultimately putting all of their communications, potentially with their legal representation, minors or other protected groups, in jeopardy. The existence, let alone the exercise of such powers can also undermine trust generally, generating a broad disincentive to update software within the community. This too has an impact on our digital security at a societal level.

The explanatory memorandum provided with the Bill asserts that it is "reasonable, necessary and proportionate" to track individuals by deploying remote tracking devices and using 'modern capabilities.'[5] While the possibilities of mobile devices to track and surveill the population are seductive to security agencies, our devices collect and subsequently derive a trove of personal data about individuals not comparable to anything in the analog world. In the INSLM public hearings regarding TOLA, Dr. James Renwick had several exchanges with experts about the nature of data collected by such devices and how a mobile phone poses insight into an individual's life well beyond anything foreseen by our current legislative system. So while the ambition of the Bill to "obtain information using as little intrusion… as possible" is commendable, it is not a realistically deliverable guarantee for individual's privacy in such a volatile environment.

---

[3] See more at: https://necessaryandproportionate.org/principles
[4] Such cases are well documented in the United States: https://theintercept.com/2019/10/10/fbi-nsa-mass-surveillance-abuse/
[5] The explanatory memorandum is available here: https://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r6554_ems_a0b798e8-7f5a-4714-a80a-9e826e90e280/upload_pdf/737484.pdf;fileType=application%2Fpdf

We recommend that members of the Australian Parliament suspend this Bill until the independent (INSLM) as well as committee (PJCIS) review of TOLA is completed and its text has been adequately amended to protect individual's rights.

Furthermore, we have several serious concerns regarding the Bill, namely that it:

1. Introduces an overbroad definition of "tracking device" essentially commandeering any/every mobile device for the purpose of remote tracking;
2. Makes lawful activities which are not in certain states and territories and erodes the need for warrants;
3. Normalises remote surveillance and tracking of individuals without their knowledge or a right to legal representation; and
4. Does not provide satisfactory independent oversight for such intrusive activity.

Recommendations

- Given the context of the ongoing review of TOLA, we recommend that the consideration of the bill be suspended until the independent (INSLM) and parliamentary (PJCIS) review of TOLA is completed and the bill has been amended to protect individual's rights and freedoms.
- We recommend the PJCIS to reject the overbroad definition for a tracking device as proposed under Schedule 2. The definition provided stating that, "*[tracking device] means any device capable of being used (whether alone or in conjunction with any other device) to track a person or an object*," is far too broad, erodes the integrity of existing definitions in other texts and poses a serious threat to the privacy of individuals and the integrity of any such devices.
- The internal authorisation (introduced under 26G and 26K) does not constitute a satisfactory substitute for a warrant obtained from a court, or even (as a less preferable, second option) the Attorney-General. A warrant must be required in all instances and a further independent review (outside of Home Affairs) whether it be a court or an institution like the Administrative Appeals Tribunal (ATT). Such an independent review should regularly review the scope and justification of approved warrants.
- Under schedule 2, we recommend that a warrant remains necessary in instances where it is currently required. An internal authorisation is an insufficient replacement in any instance when we are dealing with such a gross interference with individual privacy. All activities that are viewed as unlawful in certain states and territories must remain that way.
- While we appreciate the need to align the definitions across the ASIO Act, and between the ASIO Act and the Surveillance Devices Act 2004, this should not come at the expense of the lowest common denominator. We recommend keeping the categories of devices explicitly listed under the new definition.