Human Rights Law Centre

Submission to the Parliamentary Joint Committee on Intelligence and Security on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020

18 February 2021

Human Rights Law Centre

Contact

Daniel Webb
Legal Director
Human Rights Law Centre
Level 17, 461 Bourke Street
Melbourne VIC 3000

T: + 61 3 8636 4450
F: + 61 3 8636 4455
E: [redacted]
W: www.hrlc.org.au

Kieran Pender
Senior Lawyer
Human Rights Law Centre
Level 17, 461 Bourke Street
Melbourne VIC 3000

T: + 61 3 8636 4450
F: + 61 3 8636 4455
E: [redacted]
W: www.hrlc.org.au

Human Rights Law Centre

The Human Rights Law Centre uses a strategic combination of legal action, advocacy, research, education and UN engagement to protect and promote human rights in Australia and in Australian activities overseas. It is an independent and not-for-profit organisation and donations are tax-deductible.

The Human Rights Law Centre acknowledges the people of the Kulin and Eora Nations, the traditional owners of the unceded land on which our offices sit, and the ongoing work of Aboriginal and Torres Strait Islander peoples, communities and organisations to unravel the injustices imposed on First Nations people since colonisation and demand justice for First Nations peoples.

Contents

1. Introduction

The Human Rights Law Centre is a national not-for-profit legal centre which promotes and protects human rights in Australia. We welcome the opportunity to provide input to the Parliamentary Joint Committee on Intelligence and Security on the Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020 (**the Bill**).

The main purpose of the Bill is to amend the *Surveillance Devices Act 2004* (Cth) (***Surveillance Devices Act***) and *Crimes Act 1914* (Cth) (***Crimes Act***) to give officers of the Australian Federal Police (**AFP**) and Australian Criminal Intelligence Commission (**ACIC**) access to three new types of surveillance warrant:

- a **Data Disruption Warrant**, which enables the AFP and the ACIC to access data on one or more computers and perform disruption activities;[1]
- a **Network Activity Warrant**, which enables the AFP and the ACIC to collect intelligence on online activities; [2] and
- an **Account Takeover Warrant**, which enables the AFP and the ACIC to take over a person's online account (collectively, **the Warrants**).[3]

The Human Rights Law Centre is concerned about the disproportionate scope of these powers and the lack of evidence justifying the need for warrants of this nature beyond those already available to the AFP and ACIC. Australia lacks a robust human rights framework that would provide adequate protection against the abuse of the powers contained in this Bill. In the absence of those safeguards, the Human Rights Law Centre cannot endorse the expansion of the already-considerable powers possessed by the AFP and ACIC to intrude on the privacy of Australians.

In the past decade, transformative technological innovation has enabled the development of surveillance capabilities on an unprecedented scale. These capabilities have been deployed in a range of forms and in a range of jurisdictions, including in Australia. The increasing surveillance capacity of the Australian Government erodes individual privacy, has a chilling effect on the exercise of political rights and has a disproportionate impact on vulnerable communities. The Australian Government has failed to ensure robust safeguards to minimise the adverse impact of these new powers.

The Human Rights Law Centre echoes the broader concerns expressed in relation to the Bill by fellow civil society organisations, including in the submission by the New

[1] See Bill sch 1.
[2] See Bill sch 2.
[3] See Bill sch 3.

South Wales Council for Civil Liberties and the joint submission by the Queensland Council for Civil Liberties, Liberty Victoria, Electronic Frontiers Australia and the Australian Privacy Foundation. For present purposes, the Human Rights Law Centre will limit its particularised submissions to technical concerns.

2. Recommendations

1. The Bill be amended to increase the maximum term of imprisonment specified in the definition of relevant offence, to ensure that the Warrants are only available where their use would be proportionate to the severity of the alleged offence.

2. The Bill's definitions in relation to the Network Activity Warrants be substantially redrafted to prevent their application to individuals that have no involvement in the commission or facilitation of a relevant offence.

3. The Bill be amended so that, in circumstances where an alternative means exists of preventing the offence or obtaining the evidence sought, the decision-maker should be obliged to deny the application unless reasonably satisfied that the alternative means would be more intrusive on the targeted individual's privacy, or materially less effective in frustrating the offence or obtaining the evidence sought.

4. The Bill be amended to ensure adequate safeguards for the freedom against self-incrimination.

3. Narrow Scope of Warrants

The Warrants enable the AFP and the ACIC to undertake significant invasions of privacy in the investigation of suspected criminal activity. This is particularly so with the Network Activity Warrant, which gives law enforcement the ability to access and monitor a range of devices with a potential connection to criminal activity, and the Account Takeover Warrant, which grants law enforcement the power to alter and remove individuals' access to their online accounts.

The Bill's Explanatory Memorandum justifies this interference by claiming that the warrants "*can only be applied for on the basis of a link to serious offending. They target* ***activity of the most serious nature****, including terrorism, child exploitation, drug trafficking and firearms trafficking.*"[4]

However, the range of offences for which the Warrants may be sought is much broader than "activity of the most serious nature". A Data Disruption Warrant and a Network Activity Warrant may be issued in relation to any "relevant offence", as that term is defined in the *Surveillance Devices Act*. This includes:[5]

- any Commonwealth offence punishable by a maximum term of imprisonment of 3 years or more; and
- any State offence with a federal aspect punishable by a maximum term of imprisonment of 3 years or more.

Similarly, the Account Takeover Warrant may be issued in relation to:

- any Commonwealth offence punishable by imprisonment for 3 years or more that involves a wide-ranging list of matters, from violence and theft to tax evasion, bankruptcy violations and misuse of a computer; and
- any State offence that has a federal aspect and that would be a serious Commonwealth offence if it were a Commonwealth offence.[6]

The breadth of these definitions means that the Warrants can be used to target relatively minor criminal activities, such as theft, as well as the activities of individuals acting in the public interest, such as whistleblowers. For example, under the current definitions a warrant can be deployed where:

- a person posts content on social media that is deemed menacing, harassing or offensive;[7]

[4] Explanatory Memorandum, *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020*,
[5] We have extracted the two most relevant elements of the definition, albeit the Bill also provides for other, more-specific offences to be covered.
[6] Crimes Act, section 15GE.
[7] *Criminal Code Act 1995* (Cth), section 474.17.

- a person dishonestly takes, conceals or tampers with post;[8]
- a person dishonestly obtains cheaper internet;[9]
- a person marries two other people;[10]
- a person alters a registered trade mark without permission;[11]
- a person owns a whale or dolphin that has been unlawfully imported;[12]
- a person organises a protest activity involving breaking into a farm;[13]
- a whistleblower communicates information obtained under a surveillance warrant in a way that prejudices an investigation;[14]
- a whistleblower discloses information relating to the "assistance and access" regime in the *Telecommunications Act*;[15] and
- a lawyer or journalist assists a government whistleblower to uncover wrongdoing, in a manner deemed to constitute "incitement".[16]

The definitions also capture a range of offences that are wholly unrelated to the purpose of the Bill stated in the Explanatory Memorandum;[17] in such circumstances, the use of these warrants is unlikely to be proportionate.

Recommendation 1: The Human Rights Law Centre recommends that the Bill be amended to increase the maximum term of imprisonment specified in the definition of relevant offence, to ensure that the Warrants are only available where their use would be proportionate to the severity of the alleged offence.

[8] *Criminal Code Act 1995* (Cth), section 471.3, 471.7.
[9] *Criminal Code Act 1995* (Cth), section 474.2(1).
[10] *Marriage Act 1961* (Cth), section 94.
[11] *Trade Marks Act 1995* (Cth), section 145.
[12] *Environment Protection and Biodiversity Conservation Act 1999* (Cth), section 230.
[13] *Criminal Code Act 1995* (Cth), section 474.47.
[14] Surveillance Devices Act, section 45(2).
[15] *Telecommunications Act 1997* (Cth) (**Telecommunications Act**), section 317ZF.
[16] *Criminal Code Act 1995* (Cth), section 11.4.
[17] For example, the definition of "relevant offence" includes offences under the *Financial Transaction Reports Act 1988, Fisheries Management Act 1991* and *Torres Strait Fisheries Act 1984*.

4. Limit Application of Network Activity Warrants

The Bill provides that the chief officer of the AFP or ACIC can apply for the issue of a Network Activity Warrant against any person in a group of individuals considered a "criminal network of individuals".[18] A criminal network of individuals is defined as an electronically linked group of individuals, where one or more individuals in the group:

(a) have engaged, are engaging, or are likely to engage, in conduct that constitutes a relevant offence; or

(b) have facilitated, are facilitating, or are likely to facilitate, the engagement, by another person (whether or not an individual in the group), in conduct that constitutes a relevant offence.[19]

An "electronically linked group of individuals" simply means any 2 or more people who use the same electronic service (including a website)[20] or communicate with other individuals in the group electronically.[21]

On a broad, but not unreasonable, interpretation of these definitions, the effect is that a person who visits the same website as a person engaging in conduct facilitating or constituting a relevant offence is in a "criminal network of individuals". This is regardless of whether the website or communication bears any relation to the offence, or whether the individuals have any knowledge of, involvement in or connection to the offence.

For instance, if someone commits a relevant offence using WhatApp, then:

- every user of WhatsApp worldwide would be a member of that "criminal network of individuals", because they use the same electronic service as an individual engaging in a relevant offence;
- every person who has communicated with that individual via any form of electronic communication (not limited to WhatsApp) would be a member of that "criminal network of individuals", because they have communicated with an individual engaging in a relevant offence; and
- every person who uses a mobile device with the same operating system (such as Android, iOS, or Windows) as the person would be a member of that "criminal network of individuals", because they use the same electronic service (the operating system) as an individual engaging in a relevant offence.

This is absurdly broad. It effectively means that, where a person engages in a relevant offence, every other user of any website they access or app that is installed on their phone could potentially have their data accessed, changed or deleted, without their knowledge, consent or opportunity to object.

Not only does this seriously impact the privacy and freedom of expression of individuals with little or no connection to the offending conduct or target individual,

[18] Bill, sch 2 item 9.
[19] Bill, sch 2 item 8.
[20] *Telecommunications Act*, section 317D.
[21] Bill, sch 2 item 3.

it opens up vast swathes of online activity to monitoring by law enforcement without sufficient safeguards to prevent abuse.

Even on a narrower interpretation, these provisions still offer expansive scope. To provide a practical example: say the AFP thought that a prominent journalist with a history of reporting on information arising from whistleblowers was 'likely to' incite an intelligence officer to blow the whistle and provide them with information. The AFP could seek a Network Activity Warrant to monitor online activity of the journalist. If the journalist was part of WhatsApp group with colleagues, the AFP could potentially seek a Network Activity Warrant to monitor the online activities of these other journalists. And so on.

At minimum, the definition of "criminal network of individuals" should require that each individual in the group be engaged in or facilitating conduct that constitutes a relevant offence (whether knowingly or not). This would help protect the privacy of individuals who have no involvement in the criminal activity, while ensuring that law enforcement can target individuals or groups that inadvertently facilitate criminal activity, such as website administrators and app developers. This reflects the intent and purpose of the warrant, as stated in the Explanatory Memorandum:

> *"There is no requirement that every individual who is part of the criminal network is himself or herself committing, or intending to commit, a relevant offence. The word 'facilitating' is used to capture those individuals who are, knowingly or unknowingly, facilitating engagement by another person in conduct constituting a relevant offence as defined in section 6 of the SD Act.*
>
> *For example, a criminal network of individuals may include an individual who owns an IT platform that is, without the knowledge of that person, being exploited by a criminal organisation for illegal purposes. It will sometimes be necessary for agencies to collect intelligence on the devices used by unwitting or incidental participants in the criminal network in order to determine the full scope of offending and the identities of offenders. However,* ***this does not include accessing the devices of third parties who are not connected to the criminal network in any way****."*[22]

Recommendation 2: The Human Rights Law Centre recommends that the definitions underlying the Network Activity Warrants be substantially redrafted to prevent their application to individuals that have no involvement in the commission or facilitation of a relevant offence.

[22] Explanatory Memorandum, paragraphs 318-319.

5. Preference Alternative Means

In determining whether any of the Warrants should be issued, the decision-maker (either a Judge, magistrate or AAT member, as appropriate) must have regard to the existence of any alternative means of frustrating the offence or obtaining the evidence sought.[23] However, a Warrant may be issued regardless of any such alternative means. Given the intrusive nature of the Warrants, it is vital that where law enforcement can obtain the information required with less invasion of privacy, that opportunity should be taken.

Recommendation 3: The Human Rights Law Centre recommends that the Bill be amended so that, in circumstances where an alternative means exists of preventing the offence or obtaining the evidence sought, the decision-maker should be obliged to deny the application unless reasonably satisfied that the alternative means would be more intrusive on the targeted individual's privacy, or materially less effective in frustrating the offence or obtaining the evidence sought.

[23] Bill, sch 1 item 13; sch 2 item 9; sch 3 item 4.

6. Protect Freedom Against Self-Incrimination

Accompanying each of the warrants is an additional power for law enforcement officers to obtain an Assistance Order, which requires a specified person to provide any reasonably necessary information or assistance to allow the officer to carry out the warrant.[24]

A "specified person" can be the person suspected of committing the offence, but can also include a range of other persons, including the owner or lessee of a relevant computer or account, an employee of the owner or lessee of that computer or account, any person who uses or has used that computer or account, or a person who is or was a system administrator for the system including the computer or the electronic service to which the account relates. The person must have relevant knowledge of the computer or account or measures applied to protect data held in the computer or account.

It is a criminal offence to fail or refuse to comply with an Assistance Order, punishable by up to 10 years' imprisonment and/or 600 penalty units.

The ability for law enforcement to compel individuals to answer questions or provide assistance that could expose them to legal ramifications contradicts the right to freedom from self-incrimination, a longstanding legal doctrine that has been recognised in both common law[25] and international human rights law.[26] The right allows a person to refuse to answer questions or produce documents or other things if doing so could expose them to criminal or civil liability, and reflects both the presumption of innocence and the prosecution's burden of proving guilt.[27] While the application of the privilege "may be affected by a statute expressed clearly or in words of necessary intendment", the principle is essential in preserving the balance between the powers of the state to prosecute and the rights and interests of the accused.[28]

The Bill's Explanatory Memorandum suggests that requiring someone to comply with an Assistance Order does not breach the right to freedom from self-incrimination because "*they do not compel individuals to provide evidence against their legal interest.* ***Assistance orders only compel individuals to provide***

[24] Bill, sch 1 item 47; sch 2 items 30-31; sch 3 item 4.
[25] See *Pyneboard Pty Ltd v Trade Practices Commission* (1983) 152 CLR 328; *Environment Protection Authority v Caltex Refining Co Pty Ltd* (1993) 178 CLR 477, 498–499 (Mason CJ and Toohey J), 512–514 (Brennan J), 544–545 (McHugh J); *Sorby v Commonwealth* (1983) 152 CLR 281.
[26] *International Covenant on Civil and Political Rights*, article 14.3(g): "In the determination of any criminal charge against him, everyone shall be entitled to the following minimum guarantees, in full equality… Not to be compelled to testify against himself or to confess guilt."
[27] *Cornwell v R* (2007) 231 CLR 260, [176]; *Lee v The Queen* [2014] HCA 20 (21 May 2014) [32]–[33].
[28] *Lee v The Queen* [2014] HCA 20 (21 May 2014) [32]–[33].

access to computers or devices to assist in disruption*, in the same manner as a search warrant compels individuals to provide access to a premises to assist in a search*."[29]

This statement contradicts the wording of the proposed power, which states that an Assistance Order may compel an individual to provide *any information or assistance that is reasonable and necessary* to allow an officer to carry out the warrant, not merely access to computers or devices.[30] There is a significant gap between what the Bill provides and the interpretation offered by the Explanatory Memorandum.

Moreover, one of the considerations that the Judge, magistrate or AAT member must take into account when granting an Assistance Order is whether the disruption or account takeover is necessary "for the purpose of enabling evidence to be obtained of the commission of the alleged relevant offence".[31] It therefore appears that an Assistance Order could compel an individual to assist law enforcement to obtain evidence which is against their legal interest.

A more narrowly worded provision might limit an Assistance Order to *only* information or assistance that is *strictly* necessary for the execution of the underlying Warrant.

As currently drafted, an Assistance Order could also be used to punish people for not cooperating with police investigations in violation of their right to freedom from self-incrimination. For example, if a person suspected of committing a relevant offence refuses to provide their account credentials to law enforcement, and subsequent investigations reveal that the suspect in fact did **not** commit the offence, the person could be acquitted of that offence but nevertheless imprisoned for 10 years for failing to do comply with the Assistance Order. This concern is heightened given the availability of Assistance Orders in relation to third parties; a third party who is not guilty of any underlying offence could face 10 years' imprisonment for failing to assist law enforcement, when that failure was motivated by a desire to not self-incriminate in relation to, say, an unrelated, minor offence.

Recommendation 4: The Human Rights Law Centre recommends that the Bill be amended to ensure adequate safeguards for the freedom against self-incrimination.

[29] Explanatory Memorandum, paragraphs 254 and 985.
[30] Bill, sch 1 item 47; sch 2 items 30-31; sch 3 item 4.
[31] Ibid.