Submission to:

Mr Joshua Lickiss **&** **Panel Members**

Director, Governance & Engagement,
Electronic Surveillance Reform
Branch,
Department of Home Affairs

Electronic Surveillance and Law
Enforcement Policy Division,
Department of Home Affairs

Presented by: **Cameron Russell**

Submission on: Proposed expansion of powers for State and Territory corrective services agencies allowing them to access telecommunications data

Date: **29 June 2022**

SLIDE 1 (Title)
Good afternoon, Mr Lickiss and panel members.
(My name is Cameron Russell)
Thanks very much for the opportunity to make this submission.

SLIDE 2 (Big Brother)
This presentation shall recommend that the powers of corrective agencies not be permitted to directly access telecommunications data because: (a) mobile phones and Internet access are already disallowed in the prisons in most jurisdictions, leaving only telephone calls with approved people; (b) corrective agencies can source data through the police when needed; (c) corrective services were excluded from the list of 20 'criminal law-enforcement agencies' that could access telecommunications data when the *TIA Act* was amended in 2015; (d) for offenders under orders in the community, there is even less justification for Corrective Services data access because the police and NIC are in a better position for surveillance, investigation and intelligence roles than Corrective Services; (e) where released offenders are being monitored by Corrective Services, fundamental freedoms of association, movement and expression are curtailed; and (f) supervision orders to override these rights tend to compromise the rule of law and separation of powers, resulting in 'lawful illegality.'

SLIDE 3 (Yard)
The rights of prisoners are often disregarded for reasons of security, smooth operations, political expediency or punishment, creating an 'us versus them' dynamic. However, as the success of Norwegian prisons demonstrates, trusting prisoners and allowing them social interaction and privacy can be restorative. A study of CCTV in Queensland prisons interviewed prison managers who said the gym, workshops and program rooms had no cameras because people went there for the right reasons. Cameras were also absent in exercise yards so prisoners could (in their words) 'have a bit of a chat' and be given 'a degree of privacy.' Enlightened decisions such as these strike the right balance between security and privacy.

SLIDE 4 (Peanuts)
As the Court of Appeal explained in *Nigro against Secretary to the Department of Justice,* 'some level of risk is acceptable in a democratic society that values the rights of an individual to freedom and privacy.' A study by Mann and colleagues found individual privacy rights tend to give way to collective security rights, especially when surveillance powers are extended or threats exaggerated. We should therefore favour privacy and human rights, or at least reduce the intrusiveness of surveillance.

SLIDE 5 (Metropolis)
Recommendation 78 of the *Richardson Review* (with which the Government agreed) is as follows:

'As part of the development of a new electronic surveillance Act, corrective services authorities should be granted the power to access telecommunications data, if the relevant state or territory government considers it… necessary'

SLIDE 6 (Vague)

This recommendation is very vague. It raises such questions as:

- What is the process by which State or Territory Government conveys to Federal Government that it considers the powers necessary?;
- What is the process by which the Federal Government grants the expanded power?; and
- Does the State/Territory government need to prove necessity, and if so, on what basis? For example, a government wishing to win an election could conceivably argue that data access is necessary to be tough on crime.

The *TIA Amendment (Data Retention) Bill 2014* as originally introduced would have required State and Territory governments to prove a 'demonstrated need' to access the data, which seems wise.

SLIDE 7 (Substantive necessity)

As Michael Kirby stated, 'Citizen surveillance is only justified in very limited circumstances.' In the same vein, the demonstrated need for data access should be substantive, only justified in such limited circumstances as preserving national security or human life (and not for political gain, suppression or PR damage control).

SLIDE 8 (Truman)

Kirby said that the breadth of earlier NIC surveillance on him and its unjustifiability demonstrated the need for effective controls to avoid the dangers. These 'effective controls' would require major reforms for the Parliamentary Joint Committee on Intelligence and Security. De Zwart and colleagues argue for independent oversight of coercive or invasive data collection by engaging a jurist to review the collection of big data; which would be constructive.

SLIDE 9 (Kirby's effective controls)

It is not recommended, however, that the PJCIS be replaced with a body independent of the three branches of Government because then any findings would be mere recommendations to the Legislature. A balanced mix of Senators and Representatives, and of both major parties, with greater input from the cross-benches, is necessary, together with greater power and wider scope to hold the NIC and Executive to account.

SLIDE 10 (Definition)

'Telecommunications data' is not defined in the current legislation, but it is understood to be metadata such as date, time, duration, type of communication, telephone numbers, IP addresses, URLs and location information. 'Telecommunications data' does not include the content of the communication, although data may be more revealing than content because of the wider range of data collected.

It is recommended that 'telecommunications data' be defined in the new *Electronic Surveillance Act* to avoid uncertainty and loopholes, but in such a way that legislation remains technology-neutral to avoid frequent amendments.

SLIDE 11 (Govt response)

The Government response to the *Richardson Review* merely stated that they agreed. The Government discussion paper, however, gave insight into conditions for being granted the additional powers. The electronic surveillance powers must be needed for corrective services to perform their functions and they must provide the Federal Government with a 'clear and compelling case' to receive the powers.

SLIDE 12 (Minority Report)

Rival Alameddine and Hamzy crime family members have been limited to one mobile phone and restricted from using encrypted messaging apps or speaking with known associates and rivals under parole conditions, bail conditions, serious crime prevention orders and non-association orders. The latter two orders limit the telecommunications of free people, but the High Court of Australia held that SCPOs are lawful and constitutional. With non-association orders, freedom of association is not expressly protected in the Australian Constitution and there is no free-standing right to association implied in the Constitution. Freedom of movement is protected by s92 of the Constitution, except in the public interest where there are conflicting rights or clear legislative intent to restrict movement. However, these restrictions contravene most rule of law principles including equality before the law, accountability to the law, fairness and proportionality in the law's application, separation of powers, legal certainty, presumption of innocence and procedural and legal transparency. These Minority-Report'-style 'PreCrime' measures are examples of Austin's 'lawful illegality' and are an injustice for free people who are innocent or reformed. It is recommended that State and Territory laws that allow these orders be repealed, instead sanctioning people if they actually break the law.

SLIDE 13 (Electronic ankle bracelets)

Bagaric and colleagues identify three main areas that technology may be used as alternatives to incarceration, all involving telecommunications: (a) wearing electronic ankle bracelets that remotely monitor location; (b) wearing sensors so that unlawful or suspicious activity can be monitored remotely; and (c) wearing a conducted energy device (or CED) to remotely immobilize prisoners who attempt to escape their area of confinement or commit other crimes.

It's recommended that the CED option not proceed in Australia because it is brutal, perilous, subject to abuse and sets a dangerous precedent, as well as unnecessary since the police could be called out instead. Wearing ankle bracelets and sensors may be suitable as an alternative to ineffective incarceration (for example, in Domestic Violence Electronic Monitoring programs), but it would need to be governed by stringent regulations to

mitigate dangers such as data from the sensors being interpreted wrongly; or technology being expanded with privacy implications. For example, in the US, some ankle bracelets can listen in on conversations, measure heart beats, and issue warnings to wearers.
There may also need to be consent to bracelets and sensors due to current telecommunications laws.

SLIDE 14 (Village of the damned)
'Lawful illegality' is again relevant in two Victorian complexes that house 85 released sex offenders still considered an unacceptable risk of re-offending. These complexes outside Ararat require the residents to wear ankle bracelets. It is recommended that the only way to restore the rule of law would be to repeal the *Serious Offenders Act 2018 (Vic),* which would tend to increase sentences for serious sexual and violent crimes while retaining the non-parole period. Telecommunications devices could then more properly be dealt with as parole conditions to which prisoners agree.

SLIDE 15 (Camera)
If the expansion of corrective agency powers is to proceed, it is recommended that model Federal legislation be developed with input from the States and Territories, preferably within the new Act, with each State or Territory passing their own same or similar legislation. Such harmonization of laws has been successfully used to establish the National Construction Code; the model Work Health and Safety laws; harmonised payroll tax legislation; and recently, the Legal Profession Uniform Law scheme.

SLIDE 16 (Plans A & B)
Since the expansion of corrective services into policing, national security and intelligence roles is a significant shift, it is recommended that corrective services need to apply for access to data. If, however, corrective services powers are expanded, important safeguards will need to be incorporated in the new Act including:

(a) For each corrective agency to be listed under s.101A of the TIA Act or the new Act, if their respective government considers it necessary, having regard to the effectiveness of any existing arrangements; and
(b) Only after the State or Territory government proves a 'demonstrated need' to access the data; and
(c) The 'demonstrated need' is substantive, with the relevant State/Territory government making a 'clear and compelling case'; and
(d) Before each use of electronic surveillance powers by a corrective agency, they demonstrate it is needed to perform their functions. This could be ensured with warrants and/or strong oversight.

SLIDE 17 (Peacock)
Thanks very much for listening to this submission.