Australian Prison Reform Journal

No to expanded powers-1

Australian Prison Reform Journal

Volume 2, Issue 2, Article 1, 2022

Cameron I Russell

View ORCID profile

URL: www.aprj.com.au/articles/APRJ-2(2)-1-No-to-expanded-powers-1.pdf

A. Abstract

The Australian Government has committed to far-reaching reforms of its electronic surveillance legal framework following reviews finding the laws wholly inadequate for modern conditions and technology, and overly complex following piecemeal legislation over the four decades since the last major review of security and intelligence legislation. This research report focuses on a recommendation that the power of corrective services authorities be expanded to access telecommunications data under certain conditions. This report examines those conditions and possible ways in which the electronic surveillance power for corrective services could expand, with discussion centred on the NSW jurisdiction. Issues addressed include whether the expanded powers of Corrective Services NSW [CSNSW] are needed to perform its functions; and how any dangers may be averted and governance frameworks strengthened.

B. Introduction

The rights of prisoners and ex-prisoners are often disregarded for reasons of security, smooth operations, political expediency or punishment (Vinson 1981:1; Rosa 2000; Willis 2004:31,41-45,104). The interception and recording of prisoner communications is an example. There may be good reasons for the surveillance, but it affects the mind, emotions and rehabilitative prospects of prisoners, creating an 'us versus them' dynamic. There are always reasons for utilitarian methods, but little thought is given to possible alternatives that achieve security while preserving prisoner privacy, dignity, health and human rights (Bernal 2016:244,252-261). This is because, as Professor Eileen Baldry observed, there are no votes in rehabilitative investment in prisoners and ex-prisoners (Baldry and Homel 2021).

As the success of Norwegian prisons demonstrates (Johnsen et al. 2011; Benko 2015; Hoidal 2018; Midtlyng 2022:6-9), trusting prisoners and allowing them social interaction and privacy can be restorative, whereas observing inmates at all times and locations makes them adversarial, recidivistic and creative in avoiding surveillance. A study on CCTV in four Queensland prisons notes that, 'CCTV schemes have been criticised as they are frequently implemented based on the presumed benefits that result from camera surveillance rather than being based on any clearly articulated objectives' (Allard et al. 2006:5). The four prisons studied, however, did not select the default blanket CCTV surveillance. Rather, they were consistent in locations not watched (Allard et al. 2006:11). Interviewed managers said that the gym, hall, education/program rooms and industries/workshops had no cameras because people went there for the right reasons and were engaged. Regarding exercise yards, one manager said staff had a good view anyway and another said there were 'some issues in exercise yards' but that the absence of cameras enabled prisoners to 'have a bit of a chat' and gave them 'a degree of privacy' (Allard et al. 2006:15). Enlightened decisions may be risky for brave decisionmakers, but they strike the right balance between safety, security, prevention, operability on one hand and privacy, dignity, freedom and health on the other. Finding this optimal balance applies equally to prison design, the extent of CCTV in vulnerable locations, and the surveillance powers of law enforcement, security and intelligence agencies.

C. Background and context

With L'Estrange and Merchant's 2017 *Independent Intelligence Review* and Dennis Richardson's 2018 *Comprehensive Review of the Legal Framework of the National Intelligence Community* [the *Richardson Review*], Australia has undergone the most comprehensive inquiry into national security and intelligence agencies and their governing legislation since the 1974 and 1983 Hope Royal Commissions (L'Estrange and Merchant 2017; Richardson 2020a; ASIO n.d.). Hope's reforms reconstructed the intelligence system (ASIO n.d.) and dissolved public mistrust (Edwards 2020a), despite ASIO's lack of cooperation (Kirby 2021:2; Veness 2008). Forty years later, further comprehensive reform was required to address accelerating technological change; increasing cybercrime; cyber-

espionage, election interference and other attacks on governments, corporations and public; pervasive digital surveillance; National Terrorism Threat Level of 'Probable'; and rising international tensions (L'Estrange and Merchant 2017:5-6; Kirby 2021:11; Burgess 2020, 2022; Australian National Security 2022). Richardson's *Review* again sought to integrate the intelligence agencies for effective and accountable service, and to defend both national security and civil liberties (L'Estrange and Merchant 2017:5-9; Edwards 2017). Michael Kirby regretted that Richardson was, as a former head of ASIO particularly, a non-independent 'insider' rather than a fellow past or present jurist and outsider (2021:5-7) and was dissatisfied with the limited public consultation. However, Kirby credited Richardson with unquestioned experience, knowledge, integrity and professionalism (2021:5,12). Richardson (like Hope, L'Estrange and Merchant before him) had a strong commitment to replacing 'complex, inconsistent, outdated and inflexible' laws with a 'single, streamlined and technology-neutral Act' (DHA 2021b:3; DHA 2021c:2-4); and preservation of privacy and civil liberties (Edwards 2021; Richardson 2020:104-162). Overall, Kirby considered that the security agencies achieved "substantial success" in having their submissions incorporated in the *Richardson Review* despite Richardson's sharp rejection of some of them, but both Kirby and Richardson admirer, Professor Edwards, agree that the next review should be a Royal Commission (Kirby 2021:13; Edwards 2021).

The focus of this research report is the *Richardson Review* which reviewed the legal frameworks governing the functions, powers and oversight of the National Intelligence Community (NIC) (Richardson 2020a:32). The Federal Government agreed (or agreed in principle) with all but four of Richardson's 190 unclassified recommendations (a further 13 were classified) (2020a:166-374; Attorney-General's Department 2020:4-52).

This report shall examine Recommendation 78 of the *Review* (with which the Government agreed) that would permit corrective services authorities to access telecommunications data if the relevant State or Territory government considers it necessary (Richardson 2020b:279). A Government discussion paper for the reform of Australia's electronic surveillance framework was released in 2021 (DHA 2021b). Public submissions closed in February 2022 and the Department of Home Affairs is now considering them.

This research report examines possible ways in which the electronic surveillance power for corrective services could expand, with discussion centred on the NSW jurisdiction. Issues addressed include whether the expanded powers of Corrective Services NSW [CSNSW] are needed to perform its functions; and how any dangers may be averted and governance frameworks strengthened.

D. Overview of existing and proposed laws and powers

Although there are some federal, military, immigration detention centres and holding cells, correctional services are primarily the responsibility of the States and Territories. This research shall mainly focus on the jurisdiction with the highest prison population, that of New South Wales (with 13,126 prisoners or over 30% of the Australian prison population– ABS 2021:Table 40). For clarity, the overview shall be numbered for cross-reference.

1 Recommendation 78 of the *Richardson Review* 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' (2020a:70; 2020b:279).

'Telecommunications data' is not defined in the *Telecommunications (Interception and Access) Act 1979* (Cth) *[TIA Act], Surveillance Devices Act 2004* (Cth) or *Telecommunications Act 1997* (Cth), but it is understood to be metadata such as date, time, duration and type of communication; telephone numbers or IP addresses of the parties; and location information or URLs (unless they reveal the content). It may be noted that 'telecommunications data' does not include the content of the communication (DHA 2022; Brew 2012; Explanatory Memorandum to the *TIA Amendment Bill 2007* (Cth)), where communications are defined in the *TIA Act* as including text, conversation, messages, images, animations, data, music and sounds (s.5). 'Telecommunications data' may, however, be far more revealing than content because of the wider range of data that tends to be collected (Westby 2019). The Australian Law Reform Commission believes it is advantageous not to define 'telecommunications data' so the legislation remains technology-neutral as technology advances (ALRC 2010:73.33).

The Government response to the *Richardson Review* did not elaborate on the Recommendation, merely stating they agreed (Attorney-General's Department 2020a:24). Whilst the present *National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021* (Cth) does not provide this additional power for corrective authorities, Recommendation 78 is referred to in the discussion paper for the new framework (DHA 2021b:17). The Government states that '[a]gencies will only be able to use electronic surveillance powers where those powers are needed to perform their functions' and that the Government may add to an agency's electronic surveillance powers where it makes a 'clear and compelling case' (2021b:17).

Recommendation 15 of the Review of the Mandatory Data Retention Regime by the Parliamentary Joint Committee on Intelligence and Security [PJCIS] (2020:xix-xx) includes that Government legislates to ensure:

> 'only ASIO and the agencies listed in section 110A of the *Telecommunications (Interception and Access) Act 1979*… be permitted to authorise the disclosure of telecommunications data'
>
> And only through Part 4–1 of the *TIA Act*.

CSNSW is not listed under s110A of the *TIA Act* as a 'criminal law-enforcement agency' although the Corrective Services Administrators' Council has been lobbying Parliament for correctional services to be given criminal law-enforcement agency status (CSAC 2020).

2 If corrective powers are expanded, each agency will need to be listed in s.110A of the *TIA Act,* but relevant State and Territory legislation will also need to be amended to allow these powers.

3 Prior to outlining Recommendation 78 in volume 1, the *Richardson Review* commented, 'We have made detailed recommendations about how we believe a new Act should be developed… Of particular note, we recommend that several agencies be granted additional powers' (2020a:45)… State and territory corrective services agencies should be permitted to access telecommunications data, should their respective governments request it' (2020a:45).

The use of the phrase 'Of particular note' gives some prominence to Recommendation 78 in helping to form the new Act. Reasons for this are provided in comments in the next point.

4 Further comments on Recommendation 78, in volume 2 (2020b:277-279), are selectively summarized below:

27.41 A number of State or Territory governments requested that their corrective agencies be permitted to access telecommunications data. These agencies play a frontline role in managing prisoners and contributing to the detection or prevention of serious or organised crime.

27.42 Prior to 2014, corrective agencies were permitted to access telecommunications data as 'enforcement agencies' (but then the Government limited access to telecommunications data to a smaller range of 'criminal law-enforcement agencies')…

27.46 The *Review* sought views from States and Territories about whether corrective agencies should be able to access telecommunications data. Some supported this, noting the increasing role of corrective agencies in national security, and that if it is accepted there are good reasons for corrective agencies to access telecommunications data, the power should be applied to all states and territories consistently.

27.47 Several police authorities questioned whether it was necessary to for corrective services authorities to access telecommunications data in their own right since it could already be sought from police authorities.

27.48 The evidence was not sufficiently strong to recommend that all corrective agencies be permitted access to telecommunications data at that time.

27.49 The evidence from several states indicated well-managed, cooperative and joint investigative arrangements between police forces, integrity bodies and corrective agencies could investigate criminal activity in prisons effectively.

27.50 The *Review* supported enabling corrective services agencies with a demonstrated need to access telecommunications data in a new Act. The statistics of Corrective Services NSW and Corrections Victoria's use of telecommunications data from 2010-2015 indicated the power was heavily relied on in criminal investigations.

27.51 Corrective authorities should be granted the power to access telecommunications data, if their respective State or Territory government considered it necessary, having regard to the effectiveness of any existing arrangements in place.

5 Regarding interception of telephone *content* within prison*,* CSNSW already does this. Unless authorized, it is an offence to intercept or permit someone to intercept telecommunications (s.7 *TIA Act).* However, telephone conversations may be recorded with the consent of both parties. At the start of each conversation, both parties hear a recorded message that the conversation will be recorded and that the call will be terminated if there

is inappropriate conversation (*Crimes (Administration of Sentences) Regulation 2008* (NSW) s110(4)-(6)). Conversations may be listened to by correctional officers except for calls to legal representatives or an exempt body or person – CSNSW n.d.-b).

6 With respect to offenders living or working in the community under CSNSW supervision (for example, home detention, conditional release orders or work release) who have been released from prison yet remain under CSNSW supervision, the offender or ex-prisoner may have certain parole, community-based Intensive Corrections Order (ICO), Community Corrections Order (CCO), or other supervision or community service work conditions that have a bearing on telecommunications. For example, standard parole conditions or non-association orders could require a person not to associate with specified people (including in telecommunications) and they would need to comply with directions for monitoring compliance with the orders (State Parole Authority n.d.; Chain 2022). Additional parole conditions could be to submit to electronic monitoring (State Parole Authority n.d.). Community Corrections, a division of CSNSW, is mainly responsible for managing offenders with court orders in the community (CSNSW), with serious breaches of conditions referred to the State Parole Authority (SCNSW 2020).

E. Analysis of existing and proposed governance frameworks

1 The recommendation that corrective authorities should be granted the power to access telecommunications data if the relevant State or Territory government considers it necessary (2020a:70; 2020b:279) is vague with regard to the condition that the State or Territory government considers it necessary. It raises the question of whether the State or Territory government needs to prove necessity, and if so, on what basis. For example, a government wishing to win an election could argue that data access is necessary to be tough on crime. The level of discretion afforded the State or Territory Government requires definition and appropriate limits.

2 With the exception of State and Territory police forces, the agencies currently listed in s.110A of the *TIA Act* are national bodies. The addition of CSNSW to s.110A would also necessitate State and Territory legislation being amended.

3 The comment with regard to the State or Territory government 'requesting' the data access is again vague. How the power may be requested would need to be established by the new Act. It could be on the basis of any past request, such as those made to the Richardson Review (2020b:27.41) or prior to 2014 - 2020b:27.42); or official application procedures could be established by the new Act; or there could be a listing of the agency in s.110A of the *TIA Act;* or model Federal legislation could be established and each State or Territory could pass their own same or similar legislation.

4 The *Richardson Review* implied that State and Territory governments would be inclined to request that their corrective agencies be granted access to data for crime prevention (202b:27.41;27.44), especially in Victoria and NSW which applied to access data for criminal investigations 926 and 387 times respectively from 2010-2015 (2020b:27.44). In 2020-21, Victoria Police alone made 109,381 authorisations to access existing telecommunications data for the enforcement of criminal law and NSW Police made 103,051 (DHA 2021:55-56).

There may be some safety, security, prevention and operability risks associated with excluding corrective agencies from telecommunications data access, but as the Court of Appeal explained in *Nigro v 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.' We have been proceeding adequately with CSNSW applying for data access or working with police to access it, and the administrative burden and low level of risk must be balanced against the value society places on privacy, dignity, freedom and health. A study by Mann et al. found individual privacy rights tend to give way to collective security rights, especially when surveillance powers are extended or when threats are exaggerated to gather that power (2018:373-379). If anything, we should therefore favour privacy and human rights when balancing the two (Mann and Murray 2021:46-50), or at least reduce the intrusiveness of surveillance and seek complementarity (Hong 2017). As Kirby stated, 'Citizen surveillance is only justified in very limited circumstances. The discovery of the breadth of earlier NIC surveillance and its unjustifiability demonstrates the need for effective controls lest the enthusiasm for collection outweighs the legitimacy of officials' monitoring citizens and the dangers that can arise in consequence' (2021:9). Kirby's 'effective controls' would require major reforms for the PJCIS. De Zwart et al. argue for independent oversight of coercive or invasive data collection powers by engaging a member of the judiciary to review the collection of big data (2014:747), which would be constructive. It is not recommended, however, that the PJCIS be replaced with a body completely 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 (Grayson 2018).

5 Mobile phones, SIM cards and phone chargers are prohibited items in NSW prisons (*Crimes (Administration of Sentences) Regulation 2008* (NSW) s113) because they may be harder to intercept and used for unsupervised conversations (*Crimes (Administration of Sentences) Regulation 2008* (NSW) s110(1)-(3)). Instead, prisoners are allowed to register a limited number of people with whom they wish to converse, and these people need approval by the prison intelligence section. Prisons therefore have access to not only recorded conversations, but also basic metadata for all people a prisoner calls.

6 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 [SCPOs] and non-association orders (Young 2022; Hunter 2021; Chain 2022). It could be argued that the latter two orders are unlawful because they limit the telecommunications of free people who have done their time, but the High Court of Australia held that SCPOs are lawful and constitutional (Gregoire and Nedim 2019). 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 (ALRC 2014:35). 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 (ALRC 2014:41-46).

Such considerations will have increasing significance when technological alternatives to incarceration gain ground. Bagaric et al. identify three main areas that technology will be used, 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 [CED] to remotely immobilize prisoners who attempt to escape their area of confinement or commit other crimes (2018:98-110).

F. Recommendations of existing and proposed governance frameworks

1 It may be argued that States and Territories should not be required to prove they consider it necessary to access data because (a) the need to do so would cause unnecessary expense and delays; and (b) allowing States and Territories to opt into a national scheme (rather than have to fight for it) is good policy because a national approach reduces the costs and complexity of dealing with cross-border communications. However, the *TIA Amendment (Data Retention) Bill 2014* (Cth) as originally introduced would have required State and Territory governments to prove a 'demonstrated need' to access the data (2020b:27.42-27.43), although this was amended to remove the Government's ability to declare additional agencies following a PJCIS recommendation (2020b:27.43). Since the expansion of corrective services into policing, national security and intelligence roles is a significant shift, it is recommended that Recommendation 15 of the Review of the Mandatory Data Retention Regime be followed (PJCIS 2020:xix-xx) with corrective services needing to apply for access to data. If, however, the power of corrective services is to be expanded, it is recommended that requirements specifically for corrective services be included in the new Act regarding procedures, reporting, human rights, transparency, accountability and oversight (see point 4 below). Important safeguards would include:

(a) Recommendation 15 of the PJCIS Review (2020:xix-xx) still being followed so that each State or Territory government must apply for listing under s.101A of the *TIA Act*
(b) To be listed under s.101A, the State or Territory government must first prove a 'demonstrated need' to access the data
(c) The 'demonstrated need' is to be substantive (e.g. not a demonstrated desire for political gain). The relevant State or Territory government must make a 'clear and compelling case'
(d) A requirement that every use of electronic surveillance powers by the corrective agency is needed to perform its functions. This could be ensured with warrants or strong oversight.

2 Legislation such as the *Surveillance Devices Act 2007* (NSW) and *Surveillance Devices Regulation 2014* (NSW) have been amended to allow NSW police surveillance and the same will be required for CSNSW if added to the s.110A list of the *TIA Act*. CSNSW may also

possibly be exempted under s.27 of the *Privacy and Personal Information Protection Act 1998* (NSW) as happened for the NSW Police.

3 Although it is not recommended that corrective services be permitted to access telecommunications data, if the expansion of corrective agency powers were to proceed, retrospective requests from the States and Territories to access data would lack certainty, particularly because governments have since changed. An official application procedure would be more certain, but it should be linked with listing of each successful agency in s.110A *TIA Act*.

4 If the expansion of corrective agency powers is to proceed, it is not recommended that all States and Territories receive the expanded powers at once because of Recommendation 1 above and finding 27.48 in the Richardson Review regarding insufficient evidence to justify this. However, if all State and Territory governments are to receive such powers at once, it is recommended that model Federal legislation be developed with input from the States and Territories, preferably within the new legislative scheme. The reason is that corrective services are very different from the largely national bodies currently listed in s.110 *TIA Act,* and even different from the State and Territory Police Forces listed there in terms of roles played in the justice system. It is recommended that model Federal legislation for Federal prisons and detention centres be passed, with each State and Territory passing their own same or similar legislation. This method has been successfully used to establish the National Construction Code and model Work Health and Safety laws.

5 Metadata kept by corrective services could technically be regarded as outside the current powers of corrective agencies, although it would be argued by the prison that consent by the prisoner has allowed the metadata to be stored. It is recommended, however, that because the consent was provided for the purpose of being connected with family and friends, the use by corrective services of the metadata for intelligence or other purposes should be illegal, and there must also be safe recordkeeping to prevent unauthorized access.

6 Discussions about, and issuing of, SCPOs and non-association orders have to date mainly revolved around the 'usual suspects' of bikie gangs, organised criminal gangs and

terrorist organisations (whether individual members are innocent or guilty being another matter). The first danger is that groups that invoke public fear are used to further policy-making objectives. The second danger is that once policies have been adopted to contain 'scary' groups, it is easy for the restrictions to be expanded to contain new groups where there is less and less likelihood for crime, starting with people who have been charged with child sex offences, completed their sentences, satisfied psychologists that they are no longer a risk and perhaps even voluntarily been chemically or physically castrated (NSW is one of three States that can mandate chemical castration for 'dangerous sex offenders' on release from prison, which may reduce public fear, but goes against the rule of law and basic human rights – Hall 2014). Even with gangs, applying telecommunications and other restrictions on the basis of their criminal record and family contravenes most rule of law principles including equality before the law, accountability to the law, fairness and proportionality in the application of the law, separation of powers, legal certainty, avoidance of arbitrariness, presumption of innocence and procedural and legal transparency. Although found 'lawful' by the courts, these orders are examples of 'lawful illegality' (Austin 2015:295) and are an injustice for people who may be reformed. It is recommended that State or Territory laws that allow these orders be repealed, instead sanctioning people if they actually break the law.

With regard to wearing electronic ankle bracelets, wearing sensors and wearing a CED, it is 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 is suitable for avoiding incarceration and reoffending (for example, in the NSW Domestic Violence Electronic Monitoring program – CSNSW 2021), but it would need to be governed by stringent regulations to mitigate dangers. For example, data from the sensors could be interpreted wrongly, whether by humans or computers, so review and rapid appeal process are required. There may also arguably need to be consent to bracelets and sensors because (a) it can be stigmatizing to wear them in public; (b) current telecommunications law may not allow the communications without consent; and (c) it sets a dangerous precedent for government control of citizens. It is recommended as an absolute minimum that all

offenders be granted the right to opt out of the electronic monitoring condition imposed by courts, receiving time in prison or an alternative measure instead. Connected with this recommendation, it is further recommended that at least one change of mind be allowed so that the offender can again come out of prison under electronic monitoring or other available measure (too many changes of mind would be an unreasonable administrative burden).

Although not a solution, wearing of ankle bracelets and sensors could be a public relations assistance and safeguard for some sexual offenders who have been released from prison. It is extremely difficult to house these offenders in the general community due to public opposition. For example, two Victorian complexes house 85 released former sex offenders who are still considered an unacceptable risk of re-offending. These complexes on the outskirts of Ararat are officially called 'Corella Place' but named the 'Village of the Damned' by locals. These men can use mobile phones and travel to Ararat for shopping under guarded supervision. The residents need not have consented to wearing ankle bracelets, a strict curfew and inability to leave without guards, because they are there on a supervision order under one of: repealed *Serious Sex Offenders Monitoring Act 2005* (Vic); repealed *Serious Sex Offenders (Detention and Supervision) Act 2009* (Vic); or current *Serious Offenders Act 2018 (Vic),* the latter managing serious violent offenders as well as serious sex offenders.

A number of residents, however, have escaped, presumably tracked down by ankle bracelet, although one resident cut off his ankle bracelet with a pair of scissors (ACA 2016; News.com.au/AAP 2017; Palin 2016). Given that the residents housed at Ararat are considered a continuing unacceptable risk and that they are released people locked in by supervision order, this is another example of lawful illegality. 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 even though the non-parole period could remain the same. Telecommunications devices such as ankle bracelets and sensors could then more properly be dealt with as parole conditions and prisoners could consent to them or have the option of remaining in prison or being the subject of an alternative order until the sentence is served.

G. Conclusion

It is recommended that the powers of corrective agencies not be extended to permit access to telecommunications data because: (a) mobile phones, SIM cards, phone chargers, computers and Internet access are already generally disallowed and technologically blocked in prisons, leaving only telephone calls with approved people, the content of which is recorded (and with that comes the basic metadata); (b) although there has been some administrative burden in making applications to access data for criminal investigations (particularly for Victoria and NSW), as the police noted in the *Richardson Review,* corrective agencies can source data through the police when needed; (c) for offenders under orders in the community, there is even less justification for CSNSW data access because the police and NIC are in a better position for surveillance, data access, investigation and intelligence roles than CSNSW; (d) corrective services were excluded from the list of 20 'criminal law-enforcement agencies' (DHA 2021d:54) that could access telecommunications data when amendments were introduced in 2015 to the *TIA Act* establishing the mandatory data retention; (e) where released former offenders are being monitored by CSNSW (through their Community Corrections division) fundamental human rights and freedoms of association, movement and expression are curtailed as we proceed towards 'Minority-Report'-style 'PreCrime' measures (Spielberg 2002); and (f) supervision orders to override these rights tend to make separation of powers a little more murky; and the rule of law compromised, resulting in 'lawful illegality' (Austin 2015:297).

If, however, corrective agencies are to be permitted access to data, it is recommended that each State and Territory individually be required to prove with a 'clear and compelling case' a 'demonstrated need' to access the data before being listed under s.101A *TIA Act* (or new Act); and that every use of electronic surveillance powers by the corrective agency be shown to be needed to perform its functions (whether with warrants, strong oversight or both).

It is not recommended that all States and Territories receive the expanded powers at once but if that is to happen, it is recommended that model Federal legislation be developed with

input from the States and Territories, preferably within the new Act, and that each State or Territory pass its own same or similar legislation.

Despite some safety, security, prevention and operability risks associated with continuing to exclude corrective agencies from telecommunications data access, 'some level of risk is acceptable in a democratic society that values the rights of an individual to freedom and privacy' *(Nigro v Secretary to the Department of Justice).*

References

ABS (Australian Bureau of Statistics) (2021) 'Prisoners in Australia', accessed 22 March 2022.

ACA (A Current Affair) (3 August 2016) 'Ararat residents call for stricter security at residential complex for released sex offenders', *9 News,* accessed 6 May 2022.

ACMA (Australian Communications and Media Authority) (2021) 'Devices we prohibit', Australian Government, Canberra.

Allard T, Wortley R and Stewart A (2006) 'The purposes of CCTV in prison', *Security Journal,* 19(1):58-70, Palgrave Journals, https://doi.org/10.1057/Palgrave.sj.8350009

ALRC (Australian Law Reform Commission) (2010) 'Communications and 'telecommunications data'', *ALRC Report 108,* Australian Law Reform Commission.

—(2014) 'Traditional rights and freedoms – encroachments by Commonwealth laws', *ALRC Issues Paper 46,* Australian Law Reform Commission.

ASIO (Australian Security Intelligence Organisation) (n.d.) 'The Hope Royal Commissions', Australian Government, Canberra, accessed 29 April 2022.

Attorney-General's Department (2020a) 'Commonwealth Government response to the Comprehensive Review of the Legal Framework of the National Intelligence Community', Australian Government, Canberra.

—(2020b) 'Comprehensive Review of the Legal Framework of the National Intelligence Community', Australian Government, Canberra.

Austin LM (2015) 'Surveillance and the rule of law', *Surveillance & Society, 13*(2):295-299.

Australian National Security (2022) 'Current National Terrorism Threat Level', Australian Government, Canberra, accessed 2 May 2022.

Bagaric M, Hunter D, and Wolf G (2018) 'Technological incarceration and the end of the prison crisis', *Journal of Criminal Law and Criminology,* 108(1):73-135.

Baldry E and Homel R (2021) 'Tony Vinson Memorial Lecture' (delivered at the University of Wollongong on 9 September 2021).

Benko J (26 March 2015) 'The radical humaneness of Norway's Halden Prison', *The New York Times Magazine.*

Bernal P (2016) 'Data gathering, surveillance and human rights: Recasting the debate', *Journal of Cyber Policy,* 1(2): 243-264.

Brew N (2012) 'Telecommunications data retention – an overview', Department of Parliamentary Services, Australian Government, Canberra.

Burgess M (2020) 'Director-General's Annual Threat Assessment', ASIO, Australian Government, Canberra, accessed 29 April 2022.

—(10 February 2022) 'ASIO director-general Mike Brugess' annual threat assessment - 2022', ASIO, Australian Government, Canberra, accessed 29 April 2022.

Chain B (30 January 2022) 'Exclusive: A rare glimpse inside the workings of Sydney's biggest gang war: How the Alameddines have 'picked off the Hamzys like flies' - and why they 'keep coming out on top' in bloody battle', *Daily Mail Australia,* , accessed 5 May 2022.

CSAS (Corrective Services Administrators' Council (2020) 'Submission to Parliamentary Joint Committee on Security and Intelligence Review of the mandatory data retention regime prescribed by Part 5-1A of the Telecommunications (Interception and Access) Act 1979 (Cth)', accessed 25 March 2022.

CSNSW (Corrective Services NSW) (n.d.-a) 'Community corrections policy and procedures manual', NSW Government, Sydney.

—(n.d.-b) 'Custodial Operations Policy and Procedures: Inmate telephones', NSW Government, Sydney.

—(n.d.-c) 'Managing offenders in the community', NSW Government, Sydney.

—(2020) 'Community corrections', NSW Government, Sydney.

—(2021) 'Domestic Violence Electronic Monitoring (DVEM) program', NSW Government, Sydney.

DHA (Department of Home Affairs) (2021a) 'Explanatory Memorandum: *National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021* (Cth)', Australian Government, Canberra.

—(2021b) 'Reform of Australia's electronic surveillance framework discussion paper', Australian Government, Canberra.

—(2021c) 'Surveillance Devices Act 2004 Annual Report 2020-21', Australian Government, Canberra.

—(2021d) 'Telecommunications (Interception and Access) Act 1979 Annual Report 2020-21', Australian Government, Canberra.

—(2022) 'Lawful access to telecommunications: Telecommunications interception and surveillance', Australian Government, Canberra.

de Zwart M, Humphreys S and van Dissel B (2014) 'Surveillance, big data and democracy: Lessons for Australia from the US and UK', *UNSW Law Journal,* 37(2):713-747.

Edwards P (2017) 'The intelligence review: our Hope for years to come', *The Strategist* (26 July 2017), Australian Strategic Policy Institute (ASPI), accessed 12 March 2022.

—(2020a) 'Keeping Australians and their civil liberties safe: The origins of the Hope model', *The Strategist* (23 April 2020), Australian Strategic Policy Institute (ASPI), accessed 12 March 2022.

—(2020b) 'Keeping Australians and their civil liberties safe: Who was Robert Marsden Hope?', *The Strategist* (28 April 2020), Australian Strategic Policy Institute (ASPI), accessed 12 March 2022.

—(2021) 'Richardson intelligence review much more than an 'inside job'', *The Strategist* (5 March 2021), Australian Strategic Policy Institute (ASPI), accessed 12 March 2022.

Grayson K (2018) 'Intelligence committee: 'powerful', or toothless tiger?', *The Strategist* (11 July 2018), Australian Strategic Policy Institute (ASPI), accessed 4 May 2022.

Gregoire P and Nedim U (2019) 'NSW serious crime prevention orders are lawful, High Court rules', Sydney Criminal Lawyers, accessed 5 May 2022.

Hall M (2014) 'Treatment or punishment? Chemical castration of child sex offenders', *The Conversation,* accessed 6 May 2022.

Hoidal A (2018) 'Normality behind the walls; Examples from Halden Prison', *Federal Sentencing Reporter* 31(1):58-66.

Hong S-H (2017) 'Criticising Surveillance and Surveillance Critique: Why privacy and humanism are necessary but insufficient', *Surveillance & Society,* 15(2):187-202.

Hunter F (24 February 2021) 'Hamzy brother arrested for alleged breach of crime prevention order', *Sydney Morning Herald,* access 5 May 2022.

Johnsen B, Granheim PK and Helgesen J (2011) 'Exceptional prison conditions and the quality of prison life: Prison size and prison culture in Norwegian closed prisons', *European Journal of Criminology* 8(6):515-529, doi: 10.1177/1477370811413819

Judicial College of Victoria (2019) 'Serious Offenders Act 2018', Guide, Melbourne.

Kirby M (2021) 'The changing legal framework of the Australian intelligence community: From Hope to Richardson', *Australian Law Journal,* 95(1):1-14.

L'Estrange M and Merchant S (2017) 'Report of the 2017 Independent Intelligence Review', Australian Government, Canberra.

Mann M, Daly A, Wilson M and Suzor N (2018) 'The limits of (digital) constitutionalism: Exploring the privacy-security (im)balance in Australia', *International Communication Gazette,* 80(4):369-384.

Mann M and Murray A (2021) 'Striking a balance: Legislative expansions for electronic communications surveillance', *Precedent.* 166:44-51.

Meares M (2018) 'Mass surveillance and data retention in Australia: Balancing rights and freedoms', *Journal of Internet Law,* 21(10):3-6.

Midtlyng G (2022) 'Safety rules in a Norwegian high-security prison: The impact of social interaction between prisoners and officers', *Safety Science*, 149(May 2022):1-10

Murray A and Mann M (2022) 'Submission: Reform of Australia's electronic surveillance framework discussion paper', Queensland Council for Civil Liberties, Australian Privacy Foundation and Liberty Victoria.

News.com.au/AAP (2017) 'Victorian government will open second Village of the Damned to house evil paedophiles', *News.com.au,* accessed 6 May 2022.

Palin M (2016) 'Village of the Damned': Inside Victoria's most notorious paedophile prison', , *News.com.au,* accessed 6 May 2022.

PJCIS (Parliamentary Joint Committee on Intelligence and Security) (2020) 'Review of the mandatory data retention regime of the *Telecommunications (Interception and Access) Act 1979* (Cth)', Australian Government, Canberra.

Richards K, Death J and McCartan K (2020) 'Community-based approaches to sexual offender reintegration', Research Report (Issue 07), Australia's National Research Organisation for Women's Safety (ANROWS), Sydney, accessed 11 March 2022.

Richardson D (2020a) 'Volume 1 Recommendations and Executive Summary; Foundations and Principles; Control, Coordination and Cooperation', in Comprehensive Review of the Legal Framework of the National Intelligence Community, Australian Government, Canberra.

—(2020b) 'Volume 2 Authorisations, Immunities and Electronic Surveillance', in Comprehensive Review of the Legal Framework of the National Intelligence Community, Australian Government, Canberra.

—(2020c) 'Volume 3 Information, Technology, Powers and Oversight', in Comprehensive Review of the Legal Framework of the National Intelligence Community, Australian Government, Canberra.

—(2020d) 'Volume 4 Accountability and Transparency; Annexes', in Comprehensive Review of the Legal Framework of the National Intelligence Community, Australian Government, Canberra.

Rosa S (2000) *Prisoners rights handbook,* Redfern Legal Centre Publishing, Redfern NSW.

Spielberg *S (director)* (2002) *Minority Report* [motion picture], 20th Century Fox/DreamWorks Pictures, Los Angeles.

State Parole Authority (n.d.) 'Parole conditions', NSW Government.

Veness P (27 May 2008) 'Hope spy inquiry distrusted ASIO', *The Sydney Morning Herald*, accessed 20 March 2022.

Vinson T (1981) 'Prisons: Facts and fantasies', Corrective Services Commission NSW.

Westby J (2019) ''The Great Hack': Cambridge Analytica is just the tip of the iceberg', Amnesty International, accessed 29 May 2022.

Willis M (2004) 'Ex-prisoners, SAAP, housing and homelessness in Australia: Final report to the national SAAP Coordination and Development Committee', Australian Institute of Criminology.

Young R (11 April 2022) 'Mohamad Alameddine's bid to change bail conditions rejected', Perth Now, accessed 5 May 2022.

Legislation and Bills

Main Acts to be repealed

Telecommunications (Interception and Access) Act 1979 (Cth)

Surveillance Devices Act 2004 (Cth)

(Parts of) *Australian Security Intelligence Organisation Act 1979* (Cth)

Recent Acts and Bills contributing to new electronic surveillance framework

Assistance and Access Act 2018 (Cth)

National Security Legislation Amendment (Comprehensive Review and Other Measures No. 1) Bill 2021 (Cth)

Surveillance Legislation Amendment (Identify and Disrupt) Act 2021 (Cth)

Telecommunications Legislation Amendment (International Production Orders) Bill 2020 (Cth)

Other legislation referred to in this Research Report

Crimes (Administration of Sentences) Regulation 2008 (NSW)

Privacy and Personal Information Protection Act 1998 (NSW)

Radiocommunications Act 1992 (Cth):

- *Radiocommunications (Prohibition of PMTS Jamming Devices) Declaration 2011* (Cth)
- *Radiocommunications (Prohibited Device) (RNSS Jamming Devices) Declaration 2014* (Cth)

Serious Offenders Act 2018 (Vic)

Serious Sex Offenders (Detention and Supervision) Act 2009 (Vic) [now repealed]

Serious Sex Offenders Monitoring Act 2005 (Vic) [now repealed]

Surveillance Devices Act 2007 (NSW)

Surveillance Devices Regulation 2014 (NSW)

Telecommunications Act 1997 (Cth)

Telecommunications (Interception and Access) Amendment Bill 2007 (Cth) [referred to Explanatory Memorandum]

Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 (Cth)

Video may be viewed at:

https://youtu.be/T8Y0tcdeslk

Duration: 10min 55 sec