

Table of Contents

Introduction.....	1
The Objectives of the Bill.....	3
Cyber Currency.....	3
Social Media.....	3
Anonymising Services.....	4
Dark Net.....	4
Crimes of Foreign Origin.....	4
Child Recovery.....	4
Search and Seizure in the Cyber Realm.....	5
Emergency Powers.....	6
Accountability - Checks/Balances and Oversight.....	7
Provision for Destruction of Copies of Restricted Records.....	7
Framework.....	7
Issuing of Warrants & Assistance Notices.....	8
Access to Service Provider Networks.....	8
Custody of Warrant Data.....	8
Custody of Service Provider Confidential Information.....	8
An Alternative - A Centralised Warrant/Notice Clearing House.....	9
Specific Provisions.....	10
50 After subsection 28(1).....	10
59 After subsection 32(2).....	11
50(1)(g), (h) and (I).....	12
64A.....	12
37 Subsection 6(1).....	13
317ZS Annual reports.....	13
3F(2)(2a)(b).....	13
3F(2)(2a)(c) - Confidential.....	14
3F(2)(2C).....	14
6A At the end of section 3K 6 (vii).....	14
9 Paragraphs 201A(1)(a), and (c).....	15
13 At the end of paragraph 201A(2)(b).....	15
21A Voluntary assistance provided to the Organisation.....	15
34AAA 1(b).....	16
34AAA 2a(v).....	16

Re: The Assistance and Access Bill 2018

Author: Paul Wilkins

Date: 8 September 2018

Introduction

It's been said before that there are two things the public should never see, the making of legislation, and the making of sausages. With regards The Assistance and Access Bill 2018, it is perhaps more

curate's egg than sausage, or perhaps a curate's sausage. It bears all the hall marks of an ambit claim by law enforcement agencies, with little consideration given to either the rights of the public to protection of their privacy and their right to control dissemination of their private information. But less regard still given to the needs of service providers on whom the costs and legal onus of compliance with directions that will be issued by law enforcement. Conspicuous in its absence is adequate protection for service operators against arbitrary, high handed, ill prepared and/or ill considered actions by Law Enforcement causing disruption to their business in overriding established business practices for risk management, security, and change control procedures of the IT systems that form their core business.

This submission, discussing the objectives and provisions of The Assistance and Access Bill 2018, is divided into 3 parts, where is discussed:

1 - The Bill's objectives. The author is sympathetic to the argument that it is necessary to extend judicial writ from the physical realm to the cyber domain, however the provisions under the bill go beyond this. There is absent the checks and balances needed to protect the interests of service operators from either unlawful intrusion, or from undue interference and disruption. Accountability for the exercise of these new powers also appears lacking or inadequate in the provisions, where there is the bearest of reporting, predominantly upstream, and not such as would provide for democratic oversight.

2 - The framework under which the bill will be administered. The bill envisages a regime for data retrieval that parallels the existing warrant regime for search and seizure of the physical domain and of physical assets. This fails to reflect the complexity and business processes of service providers, who under the bill, have little scope to protect their interests or the interests of their customers, should law enforcement exceed their remit. There ought to be scope for a negotiated framework for the exercise of Assistance Notices that allows for service providers to comply in a manner consistent with established risk management, security, and change management processes. The author suggests an alternative framework that would better meet the needs of service providers, and reduce the possibility of adverse consequences for service providers arising as a consequence of their forced compliance under the bill.

The problem being where a diversity of agencies all have power to authorise and execute Assistance/Capability Notices. This should instead be managed through a single agency, that serves as the interface for the purposes of the bill, between law enforcement, and service providers. This is the only way to ensure a standard capability for intelligence gathering across agencies, smooth administration of justice and execution of Assistance/Capability Notices, and mitigates the vulnerability that arises from over a dozen different agencies and their agents all with access to service provider networks and services. This one agency should work as a clearing house for

Assistance/Capability Notices, for disseminating gleaned data to client agencies, and for ensuring the protection of warrant data and service provider confidential information.

3 - An examination of those provisions of the bill that struck the author as of salient interest.

The Objectives of the Bill

It is fair to say that technological developments have outdistanced legislation. As a consequence, the “three Cs” - Criminals, Terrorist Conspirators, and Child Molesters, find that while subject to the peril of the rule of law within the jurisdiction of physical space, their activities enjoy comparative immunity within the cyber realm, arising from difficulties in detection of their activities, establishing identity, and evidentiary difficulties in producing proof sufficient to support a prosecution. The present situation is unsupportable, and if not addressed through extending judicial writ to the cyber domain, will get worse, as encryption and anonymising technology moves from geek concept to main stream.

On the other hand, moves to extend these powers to Law Enforcement, not subject to the protections, checks and balances consistent with liberal democracy, not subject to judicial oversight, and not subject to democratic accountability, are to be resisted as overreach and prejudicial to the interests of liberal democracy.

Cyber Currency

If there is one competitive advantage enjoyed by cyber currencies over conventional currency, it is the supply of anonymity as a service. Consequently, in order for law enforcement to police money laundering and criminal transactions, they require access to cyber exchanges that would allow the identity of account holders to be identified. Consequently judicial writ ought to have scope for data collection of evidence of suspected criminal activity.

Social Media

Users of social media need to be subject to the rule of law, no less than other activities in the public domain. Consequently judicial writ ought to have scope for data collection of evidence of suspected criminal activity.

Anonymising Services

The purposes of the bill will be very much in opposition to providers of anonymising services, whose business model is predicated on providing strong anonymity. At the same time, there is a certain winking relationship between providers of anonymity as a service, and those using their services for criminal ends. The author anticipates a vocal response from hard line “privacy advocates” some of which will be motivated from criminal profit, or from the proceeds of criminal profit. Judicial writ ought to have scope for data collection of evidence of the use of anonymising services for suspected criminal activity.

Dark Net

Dark Net site operators can be expected to not cooperate with Law Enforcement. The Dark Net sites of interest to Law Enforcement will be operated by criminals, well aware that evidence of their activities will send them to prison, consequently, the application of the Bill to investigation of their operations is extremely limited. The effect of Assistance Notices will likely not extend beyond creating evidence of non compliance with an Assistance Notice.

Crimes of Foreign Origin

Where the Bill calls for cooperation with foreign law enforcement, it raises pregnant possibilities for unhappy outcomes, where Australian Law Enforcement may be compelled to remove the veil of anonymity for users who have broken no Australian law. Such would be the case where a user is pursued by foreign law enforcement for activities that would be lawful within Australia, but in foreign jurisdictions might meet the legal standard for adultery, blasphemy, sedition etc. Australian Law enforcement will then find themselves culpable in particular cases for having identified individuals then pursued by foreign law enforcement for capital crimes, albeit classed as lawful activity within Australia. It is beyond question that the interests of justice will not be served with such outcomes.

Child Recovery

Where technology can be used to assist in Child Recovery, this seems perfectly amenable to public expectations for the protection of democracy and privacy consistent with the rule of law. That said, as a non expert in child recovery, it would surprise the author if the great majority of target perpetrators were not aggrieved parents, consequently not the same profile as criminal collaborators, and therefore unlikely to use any degree of sophistication in their use of technology. Though Recovery Orders are included within the remit of the bill, they do not seem germane to the proposed data recovery regime. As a consequence, the cooperation required of service providers for the execution of Recovery Orders will be different in kind to that for detection, identification, and

prosecution of criminal collaborators. The author does not envisage that Law Enforcement activities for the execution of Child Recovery Orders under the Bill will greatly inconvenience service providers.

Search and Seizure in the Cyber Realm

"Privacy laws must prevent arbitrary or unlawful interference, but privacy is not absolute. It is an established principle that appropriate government authorities should be able to seek access to otherwise private information when a court or independent authority has authorized such access based on established legal standards. The same principles have long permitted government authorities to search homes, vehicles, and personal effects with valid legal authority. "

Five Country Ministerial 2018

Now it's possible to have sympathy for the intent to ensure judicial writ extends to the cyber domain, while at the same time holding grave concerns that search and seizure of information assets can be so easily conflated with physical search and seizure. It betrays a lack of comprehension of the technical hurdles and complexities of extending judicial reach to IT systems. Without a framework which is specifically designed to cater for judicial reach extending to IT systems, there will be more light than heat, and a great number of unhappy outcomes. Most of this will be to the detriment of the service providers and the right to privacy.

The Crown needs to rethink the approach which presume Law Enforcement should be able to summarily issue Assistance Notices, to be given instant access to data centres. Otherwise there will be inevitable disruption to the businesses of service providers. There will be embarrassment and confusion where law enforcement front data centres with a valid writ, to be refused entry by data centre security officers, for reasons of ignorance of the application of these new powers, or from difficulty in establishing the credentials of law enforcement agents seeking entry, and confusion will ensue. There is the real prospect of security officers being criminalised for simply doing their job, which is to protect the security of the data centre. Law enforcement needs to create a framework that would allow managed entry to data centres, that would include such things as a prior identification of LEA officers with data centre security, and having the design and implementation of systems and processes needed for data extraction in place well before the issuance of Assistance Notices.

Powers of search and seizure within the cyber realm granted under the bill extend beyond judicial writ. Authority for actions by the state to invade privacy properly belongs with the judiciary. It's not acceptable to have authority for exercise of these powers to lie with law enforcement. The bill as drafted affords ample latitude for the abuse of these powers by law enforcement agencies, particularly given the framework for accountability and oversight (or lack of it). The bill goes as far

as to obscure the actions of law enforcement, where the bill empowers law enforcement to gag service providers as to the existence and terms of Assistance/Compliance Notices.

Emergency Powers

It's not clear that service providers may raise objections at any stage of the proceedings. Indeed, consideration of the interests of service providers is abundantly absent in the provisions of the Bill. Particularly in the case where emergency authorisations would circumvent judicial oversight, the legal jeopardy in which service providers find themselves where they would be chancing their arm and more, should they object to an Assistance Notice or equivalent, on grounds of infeasibility, technological, security, or business risk, lack of notice given, the form of the capability notice where there is absent detail, or lack of technical competence evident in the Notice.

Given the 10 year custodial sentence that attaches to non compliance with Emergency Assistance Notices (64A(8)), in all likelihood service providers will attempt to comply with whatever's in the order. There is the real likelihood of precipitating unhappy outcomes and considerable disruption to a service provider's business, attributable to a combination of cavalier belligerence and lack of preparedness on the part of law enforcement. Indeed, the bill encourages cavalier belligerence, signified where in the bill there is no consideration of a service provider's business management processes, of the necessity to comply with change controls, to manage security and risk, these are no defense for non compliance. Nor is there any requirement on law enforcement for technical competence in the framing of Assistance Notices, which will necessarily see non expert law enforcement officers issuing directions to technical experts who understand the risks and consequences, but have no latitude whatsoever, no avenue to express objections, and no choice but to act as directed, even to the peril of the service provider's business and the interests of their customers.

The situation is entirely unacceptable where Law Enforcement are to be afforded a 48 hour window for directions to be issued without being subject to any judicial oversight, during such time the power to issue Assistance Notices (and verbal Assistance Notices) would make the Law Enforcement a law unto themselves within the service provider's data centre, and one can anticipate volatile scenes where a Strike Force team can see no further than the narrow focus of the imminent apprehension (and career credit) of a wanted suspect. This is no idol consideration, where the Bill ensures that even should the direction by law enforcement be unlawful, the data collected regardless will be admissible. One need not be a cynic to see where ambition could trump scruples, to create a crisis in which an emergency 48 window ensues, and the threat of a 10 year custodial sentence might be used to either secure unlawful data access, or to put service providers in an impossible situation where they must comply with directions to the detriment of their business.

Accountability - Checks/Balances and Oversight

It's not acceptable that accounting for exercise of these powers to government and the public constitute no more than a rubber stamp metric annual reporting of the number of Assistance/Capability notices issued. There needs to be detail as to the kind of criminal activity being investigated, the seriousness of the crime, and percentages of Assistance Notices issued that led to successful prosecutions. There needs to be a separate metric for the number of Capability / Assistance notices issued, where non disclosure formed part of the terms of the notice.

Provision for Destruction of Copies of Restricted Records

The provisions for destruction of restricted records under the Telecommunications (Interception and Access) Act 1979 do not extend to copies of restricted records, (by virtue of the definition of restricted record Part 1-2(5) Interpretation. Given the ease of reproduction of copies of digital records, the Crown ought to make proper provision to control both restricted records, and any copies, and ensure that where a restricted record is to be destroyed, so too should be all copies.

This process would be significantly more secure if the author's suggestion were adopted, where a unique SSL certificate is assigned to each warrant, and warrant data encrypted such that subsequent access to the record in the usual line of business required authorised use of the SSL certificate's private key.

Framework

The bill anticipates a new regime for search and seizure, where Capability and Assistance Notices facilitate the examination and extraction of data under Data Warrants and Computer Warrants. The Bill appears to have been drafted on a presumption that this new regime would overlay the existing warrant regime for search and seizure of physical property and physical assets. This does a grave disservice to the interests of service providers, where the commercial value of processes for risk management, security, and change management are given scant consideration, the possible impacts to the technical environment is gravely misrepresented, and where service providers can be put in a position of having little or no time to plan, test, stage and deploy changes within complex environments, with possibly gravely adverse consequences to their services, their customers, and their business. Quite possibly they may be compelled to silence, other than "something broke", for which they will simply have to wear the reputational damage.

Issuing of Warrants & Assistance Notices

The Bill empowers a swathe of law enforcement to issue Data/Computer Warrants and Assistance Notices. It goes further to extend this power to Senior Officers, which at the end of the day is probably several thousand individuals entrusted to exercise these powers in the interests of Law Enforcement, while balancing their actions against the interests of service providers, their customers, and democratic rights to privacy and free speech.

Access to Service Provider Networks

The Bill envisages a swathe of agencies that potentially will either have access, or be empowered to compel access, to service providers' computer networks and data centres. This presents obstacles and considerable cost and risk for service providers to establish the credentials and authority every time an officer seeks to serve a warrant/notice.

If the access is to be provisioned as a permanent connection between the service provider and the agency, this will require them to reproduce the effort for every agency requesting access.

Custody of Warrant Data

The Bill envisages that warrant data will be in the custody of the agency (and officers) who issued the warrant/notice. Consequently custody of warrant data will be spread widely across a swathe of agencies. The replication multiplies the number of targets for would be hackers, and consequently multiplies the risk of warrant data leaking.

Custody of Service Provider Confidential Information

One can easily anticipate that in the process of preparing Capability Notices, a great deal of a service provider's intellectual property, internal process and security documentation, and other confidential information will gravitate towards a multiplicity of agencies. There is nothing specific within the Bill as to ensure the protection of such information. Presumably the Privacy Act 1988 would apply, but the bill provides little in the way of incentive or compulsion for agencies to go to take pains to protect this information. Custody of this information across multiple agencies multiplies the risk of this confidential information leaking.

The author had anticipated that the exercise of the far reaching powers granted under the Bill would lie only in the hands of at least Deputy Commissioners of Police (or equivalent). However we find that in fact these powers will extend to anyone of “authorising officer” rank as defined under the Surveillance Devices Act 2004, to include the following:

- 5(c) - a senior executive AFP employee the chief officer authorises under subsection (5)10(c)
- 10c - a staff member of ACLEI who is an SES employee the chief officer authorises under subsection (5)5(c)
- 15(b) - an executive level member of the staff of the ACC the chief officer authorises under subsection (5)
- 5(c) a state or territory police Superintendent or a person holding equivalent rank 10(d)
- 10(d) an executive level officer of ICAC whom the chief officer authorises under subsection (5)15(b)
- 15(b) - an executive level member of the Staff of the NSW Crime Commission the chief officer authorises under subsection (5)20
- 20 - executive level member of staff of the LECC NSW (within the meaning of that Act),
- 22(d) - an executive level sworn IBAC Officer (within the meaning of that Act) the chief officer authorises under subsection (5)
- 25 - a CCCQ senior executive officer (within the meaning of that Act)
- 35 - an ICAC SA executive level member of the staff of the Commissioner the chief officer authorises under subsection (5)

Surveillance Devices Act 2004 - Authorising Officers - 6A

An Alternative - A Centralised Warrant/Notice Clearing House

The author suggests an alternative where a single law enforcement agency is entrusted to manage the warrant/notice regime, with a mandate to create the processes and systems needed to support the regime, and entrusted with the responsibility to protect the custody of both warrant information and service provider confidential information.

This agency could act as a clearing house for warrants/notices, and for the dissemination of warrant data to client agencies. It would need to be resourced to support the processes and systems facilitating access to service provider networks and data centres.

This approach is clearly preferable from a system’s architecture perspective. By consolidating all the functions within a single agency, there are cost savings in eliminating the multiplication of effort, but more importantly, the multiplication of security risks across agencies is eliminated. By

investing this agency with a mission to protect warrant data and service provider data, ensures that there is both accountability and resourcing for these such as would meet the public's expectation of government for protection of privacy.

Centralisation of data gathering with a single agency would greatly improve the effectiveness of the warrant/notices regime, where establishing and maintaining information capability with service providers was core business, and where establishing secure mechanisms and processes for information sharing across agencies was also core business.

Further, this would provide the opportunity to create information systems specifically designed for the protection and dissemination of warrant information across agencies. One example serves to illustrate the possibilities: it is the case that the SSL certificate has a field that allows for the certificate to be identified with a particular purpose, the Alternative Name field, where it supports an Object ID. Where a warrant was issued an Object ID, a unique SSL certificate could be allocated to a specific warrant/notice. All data subsequently collected within the purview of that warrant could be encrypted with the SSL's private key, providing a security layer that would encapsulate all data pertaining to the warrant. Service provider confidential information could be similarly protected, with a unique SSL certificate issued for each service provider. These certificates would be issued by the agency acting as a Certificate Authority. Service providers on uploading warrant data would need look no further than the certificate used for uploading the warrant data to ascertain the validity of the warrant. Client agencies would access the data through the same SSL certificate. One might hope that where separation of warrant data gathered under different warrants was cryptographically maintained would create more confidence with the public and service providers that the government was treating with private rights and privacy with the consideration they deserve.

Specific Provisions

50 After subsection 28(1)

Insert:

(1A) A law enforcement officer may apply to an appropriate authorising officer for an emergency authorisation for access to data held in a computer (the target computer) if, in the course of an investigation of a relevant offence, the law enforcement officer reasonably

suspects that:

- (a) an imminent risk of serious violence to a person or substantial damage to property exists; and
- (b) access to data held in the target computer is immediately necessary for the purpose of dealing with that risk; and

(c) the circumstances are so serious and the matter is of such urgency that access to data held in the target computer is warranted; and

(d) it is not practicable in the circumstances to apply for a computer access warrant.

59 After subsection 32(2)

(2A) An emergency authorisation for access to data held in a computer may authorise anything that a computer access warrant may authorise.

One might expect the breath taking reach of this emergency power to lie in the hands of at least Deputy Commissioners of Police. However the Bill extends this power (unacceptably in the author's opinion) to the following:

- 5(c) - a senior executive AFP employee the chief officer authorises undersubsection (5)10(c)
- 10c - a staff member of ACLEI who is an SES employee the chief officer authorises undersubsection (5)5(c)
- 15(b) - an executive level member of the staff of the ACC the chief officer authorises under subsection (5)
- 5(c) a state or territory police Superintendent or a person holding equivalent rank 10(d)
- 10(d) an executive level officer of ICAC whom the chief officer authorises undersubsection (5)15(b)
- 15(b) - an executive level member of the Staff of the NSW Crime Commission the chief officer authorises undersubsection (5)20
- 20 - executive level member of staff of the LECC NSW (within the meaning of that Act),
- 22(d) - an executive level sworn IBAC Officer (within the meaning of that Act) the chief officer authorises under subsection (5)
- 25 - a CCCQ senior executive officer (within the meaning of that Act)
- 35 - an ICAC SA executive level member of the staff of the Commissioner the chief officer authorises under subsection (5)

Surveillance Devices Act 2004 - Authorising Officers - 6A

This is wholly unacceptable to the author, where a police task force have a 48 hour remit to act as a law unto themselves, to compel compliance with their directions in the interests of the mission of the task force, potentially trumping and riding rough shod over established business practices for risk, security, and change management, regardless of the technical risks to the service provider's business, technical ignorance, and the lack of preparedness and planning on behalf of Law Enforcement agencies. One would hope that technical ignorance could be confined to the ranks of Deputy Commissioner or above.

50(1)(g), (h) and (l)

Nothing in these paragraphs reflects the severity of the crimes committed, nor reflects their nature - money laundering, drug trafficking, child exploitation, etc. The public have a right to know not only the number of arrests and prosecutions, but to what ends these law enforcement actions were exercised. There ought also to be specific quantitative disclosure of prosecutions within the realm of free speech prosecuted as terrorism, hate speech, harassment, child exploitation etc. and also quantitative reporting of the prosecution of journalists. There should also be provision for quantitative reporting of custodial sentences delivered, both number and length of custodial sentence.

64A

Provisions do not extend to securing cooperation in gaining physical access to computers, such as might be required to secure a physical connection to target computers. The author suspects this betrays ignorance on the part of the bill's authors of some of the methods that could be employed by law enforcement in the execution of data warrants. Or perhaps they didn't think it necessary, as covered under warrants for physical access. Though probably best to clarify, because if there's a gap at the interface, between physical access, and computer access, this may be grounds for defence council to challenge the legality of the subsequent evidentiary chain.

This would also be relevant where non cooperative service providers may have deliberately restricted administrative access according to the location of computer terminals, or made provision to restrict access to those with local knowledge or unique cryptographic devices, in an attempt to impede the execution of warrants.

Another consideration is where terminal access is controlled by a systems administrator or network administrator other than the system administrator who administers the target computer.

Another consideration is where systems other than the target computer control authorisation and access to the target computer.

37 Subsection 6(1)

data held in a computer includes:

- (b) data held in a data storage device on a computer network of which the computer forms a part.

It's an open question to what extent this definition can be legally enforced. This could be read as an overreaching attempt to provide for search of the data of any computer connected to the internet, as all the data on all these computers meet the standard of "data held in a data storage device on a computer network of which the computer forms a part". There is the same problem at organisational and corporate boundaries, and within government departments. This is an extremal definition.

A minimalist definition would be to restrict the scope of any computer network to one within the computer network's "immediate circle" (as defined by the Telecommunications Act 1997).

The jurisdiction of writs/notices ought to lie somewhere between the 2 positions, recognising that cloud and virtual file systems means that a computer's data storage may lie beyond the computer's "immediate circle", but to employ a definition where all the internet is within the purview of a single writ/notice is overreach, and the courts would be well within their right to take a prejudicial view. One unanticipated consequence would be where an Emergency Assistance Notice is used to effect the discovery of a proxy chain, and the 48 hour suspension of judicial oversight used to follow the proxy chain wherever it leads, hoping to arrive at the ultimate destination within the 48 hour interval. If on the other hand, this particular drafting is intentional, it should not be allowed to stand.

317ZS Annual reports

A private citizen will only ever see the number of Capability/Assistance Notices issued. Which is meaningless. There needs to be correlation to investigations and prosecutions, and their type and seriousness. There needs to be further provision for specific reporting of the number of Assistance Notices issued where non disclosure formed a part of the notice.

3F(2)(2a)(b)

if necessary to achieve the purpose mentioned in paragraph (a)—to add, copy, delete or alter other data in the computer or device mentioned in subparagraph (a)(i); and

There will be circumstances where the data that needs to be added/copied/deleted/changed to secure access resides on a different computer (hypervisor/virtual machine/firewall/proxy/cryptographic vault). Indeed, the Bill creates this eventuality where such measures are employed to frustrate such access. A chain of virtual machines across data centres and jurisdictions, being one possibility. It's not even clear that if a virtual machine's sole purpose is to provide secure access to a computer which is used for criminal purposes, whether the Bill will service to afford jurisdiction.

3F(2)(2a)(c) - Confidential

See separate submission.

3F(2)(2C)

Subsections (2A) and (2B) do not authorise the addition, deletion or alteration of data, or the doing of any thing, that is likely to:

(a) materially interfere with, interrupt or obstruct:

(i) a communication in transit; or

(ii) the lawful use by other persons of a computer; unless the addition, deletion or alteration, or the doing of the thing, is necessary to do one or more of the things specified in the warrant; or

(b) cause any other material loss or damage to other persons lawfully using a computer.

The phraseology is problematic and at cross purposes. On the one hand, (b) disallows material loss. Where (a) (ii) permits material interference in the prosecution of the warrant.

1 - (b) should extend to disallow material loss for the service provider

2 - (a)(ii) Fails to recognise that "lawful use by other persons" may number hundreds or thousands, and that it may be quite impossible for law enforcement to even know of the importance to their interests of reliability of service, or of the consequences of an interruption of that service.

6A At the end of section 3K 6 (vii)

(vii) a deceased person who, before the person's death, used the relevant computer;

Probably “used, or is reasonably suspected of having used or had in their possession, the relevant computer” may be preferable, on the grounds that a deceased person may be a result of unlawful death, and the computer may furnish evidence of their unlawful death.

9 Paragraphs 201A(1)(a), and (c)

(a) access data held in, or accessible from, a computer or data storage device that:

(i) is on warrant premises; or

...

(c) convert into documentary form or another form intelligible to an executing officer:

(i) data held in, or accessible from, a computer, or data storage device, described in paragraph (a); or

Which extend to any computer reachable via the internet. All under the jurisdiction of a premises warrant. This has every appearance of being an ambit claim and can only make for bad law. Similar to concerns of 37 Subsection 6(1), there ought to be a limitation to judicial reach of a writ somewhat beyond immediate circle, but less than the global internet.

13 At the end of paragraph 201A(2)(b)

(vi) a person who is or was a system administrator for the system including the computer or device; and

Arguably those who maintain network devices (network administrators) are beyond the purview of this clause. Not only because they’re arguably not system administrators, but more importantly, they do not administer the computer, but rather control network access to the computer. Similar considerations apply to security devices, which may require modification to non target systems to enable access to the computer.

21A Voluntary assistance provided to the Organisation

1(d) the conduct does not involve the person or body committing an offence against a law of the Commonwealth, a State or a Territory; and

Possibly directly contradicts the Privacy Act 1988.

34AAA 1(b)

(b) copy data held in, or accessible from, a computer, or data storage device, described in paragraph

Here, the issue of the overreach of the global internet raised against 37 Subsection 6(1), does not apply. Given the combined gravity of the Director General's and the Attorney General's imprimatur, across heads of government, jurisdictional reach within the purview of the order in this instance is perfectly appropriate.

However, note that in 37 Subsection 6(1) and elsewhere, the combined Director General's and Attorney General's authorisation is not required, and so this provision serves to undermine the justification for the judicial reach of 37 Subsection 6(1).

34AAA 2a(v)

2a(v) access by the Organisation to data held in, or accessible from, the computer or data storage device will be for the purpose of obtaining foreign intelligence relating to a matter specified in the relevant notice under subsection 27A(1); and

Again the problem of overreach, regardless of the imprimatur of the Attorney General's authorisation, the authorisation does not span heads of government. Consequently the warrant can issue entirely from within the government. The extension of judicial warrant to the global internet is overreach. If a 27A warrant applies, a request should come from the Director General, as provided for under 34AAA 1.