Submission to the Parliamentary Joint Committee on Intelligence and Security

Telecommunications Legislation Amendment (International Production Orders) Bill 2020

Contents

Summary

i. This submission examines the operation and effect of the Telecommunications Legislation Amendment (International Production Orders) Bill 2020 ('the Bill'). It is particularly focussed on how the new powers proposed under the Bill will interact with the growing powers of multinational telecommunications carriers in respect of personal data.

ii. The surveillance powers in the Bill are not simply a replication or an extension of the existing regime. There are features of the Bill that will significantly extend and alter the surveillance capability of the Australian Government, by leveraging the massive commercial exploitation of personal data by multinational companies and their associates.

iii. The key concern of this submission is that the main area of the Bill's operation will be outside of Government control – either because commercial data collection operates outside Australian jurisdiction, or because the powers in the Bill leverage the unconscious and unwitting exposure to extensive surveillance by the general population. This is a marked departure from existing regimes such as the *Surveillance Devices Act 2004*, which not only recognises that Government interference with personal privacy should be closely watched and carefully controlled, but also does this effectively through regulation.

iv. No Australian legislation should legalise the use of information as evidence if it has been unlawfully acquired. The Bill should be amended to ensure that it cannot have this effect.

v. There is a growing gap in privacy regulation within Australia and a lack of genuine engagement by the Australian Government in the regulation of personal data use within the digital environment. The push for more access to data for security purposes has been at the cost of investment in commensurate privacy protections. Previous inquiries have highlighted this problem, perhaps none more so than the recently completed ACCC Digital Platforms Inquiry in 2019.

vi. The Bill should not be passed at least until the following occur:

- the amendments to the *Privacy Act 1988* which were announced in March 2019, together with the Government's formalisation of the agreed code for social media and online platforms which trade in personal information online, and
- telecommunications privacy rights are legislated under a stand-alone Act, under a Minister whose responsibility under the Act is the protection of Australians' online privacy and digital rights.

vii. Given the existence of processes under the *Mutual Assistance in Criminal Matters Act 1987* which can support Australian agencies in the short term (and indeed are relied upon by other countries) there is no practical reason why this staged approach cannot be adopted.

List of Recommendations

Recommendation 1

The Bill should include protections against the collection and use of data which has been obtained or used by private industry in contravention of Australian privacy principles.

Recommendation 2

The passage of the Bill should be contingent on the amendments to the Privacy Act which were announced in March 2019, together with the Government's formalisation of the agreed code for social media and online platforms which trade in personal information online.

The Bill should not be passed unless and until the privacy gaps in current law (being those referred to by the Attorney-General and the Minister for Communication and the Arts in March 2019) have been rectified.

Recommendation 3

The Committee should examine the Government's response to Recommendation 1 of the *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* to ensure that those reforms are being progressed, so that the IPO framework does not exacerbate systemic weaknesses in the outdated regime.

Recommendation 4

The short title of the *Telecommunications (Interception and Access) Act 1979* should be changed to the *Telecommunications and Internet Data Interception Act 2020*.

The long title of the *Telecommunications (Interception and Access) Act 1979* should be changed from:

An Act to prohibit the interception of, and other access to, telecommunications except where authorised in special circumstances or for the purpose of tracing the location of callers in emergencies, and for related purposes.

To:

An Act to regulate law enforcement and national security interception of telecommunications and internet data, to regulate telecommunications industry assistance with such interception, and for related purposes.

Recommendation 5

The objectives of the TIA Act should no longer include the prohibition of telecommunications interception and privacy protection. It should only regulate interception and access. The privacy objectives should instead be dealt with in separate privacy-based legislation administered outside of the Home Affairs portfolio.

Recommendation 6

The definition of 'stored communication' in the Bill should be the same as that used in the *Telecommunications (Interception and Access) Act 1979.*

Recommendation 7

The applicant for a stored communications IPO under clause 39 of the Bill should be required to specify the stored communications sought under the order (e.g. by type and date range) and justify why obtaining that specific set of data would be likely to assist in the investigation of the serious offence.

Recommendation 8

An IPO for stored communications issued under clause 40 of the Bill should specify what stored communications are to be provided by the designed communications provider under the order (e.g. by type and date range).

Recommendation 9

An IPO for stored communications issued under clause 40 of the Bill should include the ability of the issuing authority to impose restrictions on the scope of the order.

Recommendation 10

The term 'serious category 1 offence' should be replaced with the term 'category 1 offence' throughout the Bill.

Recommendation 11

The matters to which an Issuing Authority must be satisfied of before issuing an IPO should include whether the data being sought was acquired or retained in accordance with the foreign country's domestic laws.

Recommendation 12

The word 'designated' should be removed from the defined term '*designated communications provider'* throughout the Bill.

Recommendation 13

As a precondition for issuing an IPO, the Issuing Authority should be satisfied that the communications provider subject of the IPO has a lawful right of access to, or the retention of, the type of data sought under that foreign country's laws, including in respect of applicable privacy laws and protections.

Recommendation 14

Every IPO application should be required to state that the order sought will comply with the terms of the relevant *designated international agreement* under which it will be executed. The Issuing Authority should be independently satisfied the IPO complies with the *designated international agreement* before the IPO is issued.

Recommendation 15

The powers in Part 3 of the Bill should be limited to only interception orders and should only permit the interception of communications which are made while a Control Order or a succeeding Control Order is in force.

Introduction

1. The modern communications environment has seen increasing use of large-scale, internationally operated digital communications services. In turn, the private telecommunications companies who provide those services have dispersed their data collection and storage operations across the world. These changes present particular problems for law enforcement agencies when seeking to use their legislative powers to obtain digital evidence of crime. Jurisdictional boundaries mean that Australian law enforcement and security agencies may have no domestic ability to access communications data stored outside national borders in criminal and national security investigations.

2. The conventional method by which evidence from foreign countries is collected by Australian agencies is through Mutual Legal Assistance Treaties ('MLAT') and the *Mutual Assistance in Legal Matters Act 1987.* These conventional methods are reported to be slow, and they have proved increasingly inadequate to deal with the higher volumes of digital communication information relevant to domestic investigations now held offshore.[1]

3. The Telecommunications Legislation Amendment (International Production Orders) Bill 2020 ('the Bill') will create a new cross-border framework ('the IPO framework') for direct access to the data and interception capabilities of offshore telecommunications providers. This framework will sit within the *Telecommunications (Interception and Access) Act 1979* ('the TIA Act') and models key parts of this existing legislation.

4. The creation of a domestic IPO framework is an essential precondition for Australia to enter a proposed bilateral "executive agreement" with the United States, pursuant to the Clarifying the Lawful Overseas Use of Data Act ('the CLOUD Act').[2] Currently the UK has such an agreement with the US,[3] with Australia potentially being the second country to enter such an agreement.

[1] Explanatory Memorandum to the Telecommunications Legislation Amendment (International Production Orders) Bill 2020, paragraph 5. See also comments about the mutual assistance system in the US Department of Justice *White Paper on the purpose and impact of the CLOUD Act* at https://www.justice.gov/opa/press-release/file/1153446/download

[2] For an explanation of the US process, see Stephen P. Mulligan Legislative Attorney, *Cross-Border Data Sharing Under the CLOUD Act* April 23, 20 https://fas.org/sgp/crs/misc/R45173.pdf

[3] See the US Department of Justice announcement at https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists

5. The CLOUD Act enjoys the support of the UK and the USA governments, and large technology companies such as Microsoft.[4]

6. The IPO framework permits independently-authorised International Production Orders ('IPOs') to be issued directly to *designated communications providers* in foreign countries with which Australia has a *designated international agreement*. It further provides for reciprocal arrangements for the receipt of such orders between countries that have an agreement with Australia, and in that regard, lifts certain domestic legislative protections that would otherwise operate to prevent this disclosure.

7. The Bill contains three types of IPO:
    - an IPO for interception (including B-Party interception),
    - an IPO for stored communications, and
    - an IPO for telecommunications data.

8. An *interception agency*, *control order IPO agency*, and the Australian Security Intelligence Organisation (the Organisation) may apply for an IPO directing a *designated communications provider* to intercept communications carried by the individual carriage service during a specified period.

9. A *criminal law enforcement agency, control order IPO agency* and the Organisation may apply for an IPO directing a *designated communications provider* to obtain *stored communications*. An *enforcement agency*, *control order IPO agency*, and the Organisation may also apply for an IPO directing a *designated communications provider* to obtain *telecommunications data* for a specific period.

10. The issuing authorities for an IPO are an eligible judge or nominated Administrative Appeals Tribunal member.

Privacy Implications

11. The primary justification for the IPO framework is that the MLAT process is no longer adequate to deal with the volume of offshore information being sought to support domestic law enforcement and national security investigations.[5] The changes in the telecommunications industry are also leading to changing patterns of criminal activity. Collectively they make the investigation and prosecution process more difficult.[6]

12. Although not disputed in this submission, the justification pre-supposes that interference with privacy involved in digital surveillance and data-collection by law enforcement and national security agencies is necessary. Despite widespread concerns with government electronic surveillance,[7] that is the position under Australian law. It is consistent with long-standing

---

[4] See Microsoft's media release (Brad Smith) at https://blogs.microsoft.com/on-the-issues/2018/04/03/the-cloud-act-is-an-important-step-forward-but-now-more-steps-need-to-follow/

[5] US Department of Justice *White Paper on the purpose and impact of the CLOUD Act,* page 3.

[6] Squire, Peter *Why Cross-Border Government Requests for Data Will Keep Becoming More Important,* May 23 2017, available at https://www.lawfareblog.com/why-cross-border-government-requests-data-will-keep-becoming-more-important

[7] Electronic Frontiers Foundation article titled: *CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data* available at **https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data**

exemptions in the *Privacy Act 1988* which make certain covert exchanges of personal information, which would otherwise require notification or consent, lawful.

13. The same information sought by law enforcement is, in many cases, already collected and used by private companies for their own commercial purposes, including commercial political purposes.[8] It follows that the same information should also be available to law enforcement agencies, who act in the pursuance of legitimate public objectives through their use of statutory powers.

14. Further, because that same information would be obtainable from domestic sources if it were collected domestically, where the data is held offshore there is justification for law enforcement agencies having access to that material in the same manner as domestic warrants currently work.

15. These propositions are not disputed in this submission.

16. What then, is different about this Bill and what new privacy risks does it present?

Privacy Risk 1: Insufficient accountability and oversight

17. The most significant privacy risk in the Bill lies in the IPO framework's reliance on the offshore collection and storage of Australians' personal data by private multinational companies. Those massive companies are not subject to Australian laws, nor Australian oversight and control. There are obvious and well documented privacy risks with the accumulated powers of the social media giants and other technology companies, which translate into clear risks of Australians' private data being used and exploited outside Australia.

18. In March 2019, the Commonwealth Attorney-General and the Minister for Communication and the Arts acknowledged the veracity of these concerns when they jointly stated:

> *Existing protections and penalties for misuse of Australians' personal information under the Privacy Act fall short of community expectations, particularly as a result of the explosion in major social media and online platforms that trade in personal information over the past decade.*[9]

19. The activities involved in telecommunications interception, and the collection and storage of telecommunications data, are activities which are so inherently prejudicial to the privacy of Australian citizens that they should only be carried out in circumstances that are directly amenable to Australian jurisdiction and control.

    - This is evidenced by a comparison between the operation of the Bill and of the surveillance powers under the *Surveillance Devices Act 2004* (Cth). Part 6 of that Act (including s. 49 - report on each warrant or authorisation) show how seriously the surveillance of the activities of individuals was viewed by previous Parliaments.

[8] The *Cambridge Analytica* scandal provides a well-known example.
[9] Media release Attorney-General, The Hon Christian Porter MP Minister for Communications, Minister for Arts Senator The Hon Mitch Fifield, titled *Tougher penalties to keep Australians safe online* dated 24 March 2019. Available at https://www.attorneygeneral.gov.au/media/media-releases/tougher-penalties-keep-australians-safe-online-24-march-2019

- Another example is s.77 of the TIA Act, which prohibits the use of illegally obtained telephone interceptions as evidence. This is a significantly higher threshold than applies to other types of evidence, and recognises the gravity of privacy issues at stake in intercepting communications.[10]

20. A lack of effective Australian control over such data acquisition and use ultimately subverts the orthodox model under which the surveillance powers of a democratic State have a high degree of accountability to Government and to Parliament.

21. Where such collection and interception activities are carried out by an offshore carrier that is responding to an Australian IPO, the entirety of that activity should be understood as an exercise of the Executive powers of Government. Those offshore communications providers are carrying out work traditionally reserved to the Executive when they collect or provide the personal data of Australians sought under an IPO.

22. At its highest, this analysis suggests the proposed IPO framework conflicts with the extent and exercise of the Executive power under s. 61 of the constitution. At the least, it raises the issue of public trust and knowledge of the activities of Government. As Dawson, Toohey and Gaudron JJ noted in *Re Residential Tenancies Tribunal of NSW v Henderson; Ex parte Defence Housing Authority* [1997] HCA 36:

> *Indeed it is of the very nature of executive power in a system of responsible government that it is susceptible to control by the exercise of legislative power by Parliament.*

23. This quotation references the High Court's unanimous decision in *Lange v Australian Broadcasting Corporation ("Political Free Speech case")* [1997] HCA 25, where the High Court made the following observations about the nature of executive power:

> *In his Notes on Australian Federation: Its Nature and Probable Effects*http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCA/1997/25.html - fn37*, Sir Samuel Griffith pointed out that the effect of responsible government "*is that the actual government of the State is conducted by officers who enjoy the confidence of the people".
>
> …
>
> *Moreover, the conduct of the executive branch is not confined to Ministers and the public service. It includes the affairs of statutory authorities and public utilities which are obliged to report to the legislature or to a Minister who is responsible to the legislature. In* British Steel v Granada Televisionhttp://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/cth/HCA/1997/25.html - fn47*, Lord Wilberforce said that it was by these reports that effect was given to "*[t]he legitimate interest of the public*" in knowing about the affairs of such bodies.*

24. A key question arising from this Bill is whether Australian Government agencies and Government regulatory authorities should be permitted to obtain the benefits of surveillance and data capture processes that occur offshore and in the absence of Australian government (indeed perhaps any government's) effective supervision.

---

[10] For an example of these aspects of the TIA framework in operation see *R v Scarpantoni* (No 2) [2013] SADC 70 (22 May 2013)

Comparison with the MLAT process

25. The proposed IPO framework is closely modelled on Australia's domestic telecommunications interception regime under the TIA Act. The existing MLAT process already provides a mechanism for relevant enforcement agencies to obtain access to data and capabilities of offshore carriers. Because of those similarities between the current TIA Act and MLAT arrangements and the proposed IPO model, it might be argued that the accountability concerns raised in this submission are misplaced - that a lack of accountability under Australian law is simply a feature of the modern telecommunications environment which must be accepted, no matter the cost to civil rights.

26. The issue with relying on a "status quo" argument is that the privacy protections within the current TIA Act and MLAT regimes are already inadequate to deal with the problem that the IPO framework is said to address – being the offshore location of Australian's telecommunication data. The IPO framework represents a logistical solution to this problem, but does not deal with its broader ramifications, including for user's privacy.

27. A comprehensive PJCIS review in 2013 found that the TIA Act regime needs significant reform,[11] and the MLAT process is clearly not coping with the increased use of offshore carriers and services by Australian consumers. Neither regime has kept pace with the rapid growth of the massive multinational companies in domestic communications. It follows that neither regime provides a model that properly addresses the unique privacy concerns of bulk data collection by multinational corporations who operate outside Australian jurisdiction.

28. It is insufficient for the Statement of Compatibility with Human Rights in the EM to state that the privacy risks are dealt with by the criteria applied by issuing authorities[12] or that handling rules for information obtained under an IPO provide privacy protections.[13] There are equally grave privacy risks associated with the acquisition, handling, and distribution of Australian's personal information by third parties *before* its transfer to Australia, which are not addressed at all in the EM.

29. The IPO framework involves the use of a domestically issued Australian warrant to obtain an order requiring a foreign communications provider to provide data, including personal information, without the involvement of any foreign law enforcement or government authorities. The involvement of foreign authorities would have acted as a safeguard on Australian requests, ensuring the legality of both government's actions and those of the telecommunications provider under the domestic laws of that foreign country.[14]

30. It has been observed that:

> *"A critical human rights protection in the Mutual Legal Assistance Treaty (MLAT) process is a requirement that a U.S. entity, namely the DOJ and a judge, review a foreign request for content to ensure that it does not raise human rights concerns. Such a protection is critical because even generally rights-respecting jurisdictions may have particular laws or practices*

[11] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013, Chapter 2 and Recommendation 18
[12] Explanatory Memorandum, Statement of Compatibility with Human Rights at paras 12 - 17
[13] Ibid, para 59.
[14] When foreign police seek data stored in the U.S., the mutual assistance system requires them to adhere to the Fourth Amendment's warrant requirements, which operate as a significant procedural safeguard. Informal law enforcement cooperation known as 'police to police' assistance is also bypassed under the IPO framework.

that raise human rights concerns. The U.S.-U.K. Agreement jettisons this important protection by permitting providers to respond directly to requests from the U.K… This essentially leaves providers as the last line of defence and does not reflect the reality that many providers will not have the capacity or interest in conducting robust human rights reviews of requests received."[15]

31. Similar concerns have been raised about the potential for this change in approach to encroach on privacy rights and freedoms. For example, the European Parliament has expressed the view:

"..that a more balanced solution would have been to strengthen the existing international system of MLATs with a view to encouraging international and judicial cooperation;"[16]

Comparison with the Australian regulatory framework

32. To appreciate the gap between current regulation of telecommunications interception and the regulation under the proposed model, it is necessary to briefly outline the standards to which communication providers are subject in Australia.

33. Australia's telecommunication industry facilitates access to communications and data for law enforcement and national security purposes. These activities are primarily regulated under two pieces of legislation — the *Telecommunications Act* (1997) ('Telecommunications Act') administered by ACMA, and the TIA Act, which is administered by the Department of Home Affairs.

34. Australian telecommunications carriers and telecommunications service providers are required to be licensed within Australia and are subject to oversight by ACMA.[17] The Office of the Australian Information Commissioner also has a regulatory and oversight role in relation to the privacy aspects of these responsibilities.[18]

35. The statutory obligations owed by industry include the protection of customer information under Part 13 of the Telecommunications Act, which provides that:

Carriers, carriage service providers, number-database operators, emergency call persons and their respective associates must protect the confidentiality of information that relates to:

(a) the contents of communications that have been, or are being, carried by carriers or carriage service providers; and
(b) carriage services supplied by carriers and carriage service providers; and
(c) the affairs or personal particulars of other persons.

- *The disclosure or use of protected information is authorised in limited circumstances (for example, disclosure or use for purposes relating to the enforcement of the criminal law).*

[15] Human Rights Watch *Groups Urge Congress to Oppose US-UK Cloud Act Agreement,* October 29, 2019 available at https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement
[16] European Parliament resolution of 5 July 2018 on the adequacy of the protection afforded by the EU-US Privacy Shield (2018/2645(RSP)) available at https://www.europarl.europa.eu/doceo/document/TA-8-2018-0315_EN.pdf?redirect
[17] https://www.acma.gov.au/about-carriers-and-carriage-service-providers
[18] https://www.oaic.gov.au/privacy/other-legislation/telecommunications/

- *An authorised recipient of protected information may only disclose or use the information for an authorised purpose.*

- *Certain record-keeping requirements are imposed in relation to authorised disclosures or uses of information.*[19]

36. Compliance with the Australian regulatory framework is also seen as necessary for larger offshore companies such as Facebook, Google and Twitter (referred to by the PJCIS as 'ancillary service providers). In 2013 the PJCIS recommended that it be made clear that these companies were subject to Australia's regulatory regime:

> *The Committee recommends that the* Telecommunications (Interception and Access Act) 1979 *and the* Telecommunications Act 1997 *be amended to make it clear beyond doubt that the existing obligations of the telecommunications interception regime apply to all providers (including ancillary service providers) of telecommunications services accessed within Australia. As with the existing cost sharing arrangements, this should be done on a no-profit and no-loss basis for ancillary service providers*.[20]

37. Chapter 7 of the PJCIS *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* discusses similar concerns about carriers being subject to oversight. The PJCIS concluded:

> *…On the basis of the evidence received, the Committee considers it would be appropriate to require all providers to be subject to either the Australian Privacy Principles or binding rules of the Australian Privacy Commissioner.*[21]

38. In March 2019, the Attorney-General and the Minister for the Arts issued a joint media release[22] which included the following statements:

> *"The tech industry needs to do much more to protect Australians' data and privacy," Minister Fifield said.*
>
> *"Today we are sending a clear message that this Government will act to ensure consumers have their privacy respected and we will punish those firms and platforms who defy our norms and our laws."*
>
> *The amendments to the Privacy Act will:*
>
> - *Increase penalties for all entities covered by the Act, which includes social media and online platforms operating in Australia, from the current maximum penalty of $2.1 million for serious or repeated breaches to $10 million or three times the value of any benefit obtained through the misuse of information or 10 per cent of a company's annual domestic turnover – whichever is the greater*

---

[19] This summary is found at s.270 of the Telecommunications Act
[20] *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation,* Recommendation 14
[21] Parliamentary Joint Committee on Intelligence and Security *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* at 7.122
[22] *Tougher penalties to keep Australians safe online* dated 24 March 2019, available at https://www.attorneygeneral.gov.au/media/media-releases/tougher-penalties-keep-australians-safe-online-24-march-2019

- *Provide the Office of the Australian Information Commissioner (OAIC) with new infringement notice powers backed by new penalties of up to $63,000 for bodies corporate and $12,600 for individuals for failure to cooperate with efforts to resolve minor breaches*
- *Expand other options available to the OAIC to ensure breaches are addressed through third-party reviews, and/or publish prominent notices about specific breaches and ensure those directly affected are advised*
- *Require social media and online platforms to stop using or disclosing an individual's personal information upon request*
- *Introduce specific rules to protect the personal information of children and other vulnerable groups.*

"This penalty and enforcement regime will be backed by legislative amendments which will result in a code for social media and online platforms which trade in personal information. The code will require these companies to be more transparent about any data sharing and requiring more specific consent of users when they collect, use and disclose personal information," the Attorney-General said.

39. Notwithstanding the PJCIS views and the government's announcement, it remains unclear whether the CLOUD Act and the IPO framework will provide such protections, including effective remedies, should Australian's data be collected, held, or used offshore in ways that depart from Australian privacy standards. As things stand presently, IPOs will be able to be issued in respect of *designated communications providers* which have not complied with these codes. Offshore communications providers cannot be expected to elevate users' rights, or government regulatory interests, above their commercial objectives. As noted by the ACCC,[23] "*The fundamental business model of both Google and Facebook is to attract a large number of users and build rich data sets about their users.*" which they then monetise.[24]

40. To the extent these corporations are answerable to the regulatory framework of the US Government, different standards apply to those expected in Australia. Their subsidiary companies may not even be based in the US. There are widely held concerns about the efficacy of the US accountability framework,[25] and the practices of the companies themselves.[26] As observed in the ACCC's recent Digital Platforms Inquiry:[27]

The ubiquity of the Google and Facebook platforms has placed them in a privileged position. They act as gateways to reaching Australian consumers and they are, in many cases, critical and unavoidable partners for many Australian businesses, including news media businesses. Dominant firms, of course, have a special responsibility that smaller, less significant businesses do not have. The opaque operations of digital platforms and their presence in inter-related markets mean it is difficult to determine precisely what standard of behaviour these digital platforms are meeting.

---

[23] ACCC Digital Platforms Inquiry, Final Report, page 7
[24] ACCC Digital Platforms Inquiry, Final Report, page 60.
[25] https://www.usatoday.com/story/opinion/2020/04/08/trump-tries-muzzle-governments-independent-watchdogs-editorials-and-debates/2965438001/
[26] See the Guardian newspaper article on Facebook's privacy problems https://www.google.com.au/amp/s/amp.theguardian.com/technology/2018/dec/14/facebook-privacy-problems-roundup and similar concerns expressed in the Irish Times: https://www.google.com.au/amp/s/www.irishtimes.com/business/technology/tide-turns-on-social-media-giants-as-privacy-concerns-rise-in-us-1.3974302%3fmode=amp
[27] ACCC Digital Platforms Inquiry, Final Report, page 1

41. Many people who might otherwise support the Bill may not be aware that the USA continues to operate without comprehensive privacy legislation, relying instead on a patchwork of sectoral laws.[28]

42. This risk is exacerbated by the lack of Australian jurisdiction over offshore communications providers. The restrictions on carriers and third parties contained in the TIA Act (e.g. the offences at ss. 7, 63 and 133, which collectively preserve the integrity of data and protect individual privacy rights) do not capture extra-territorial conduct.[29]

43. The Bill raises issues with the right to an effective remedy for breaches of fundamental rights, a right which is recognised under Article 2(3) of the ICCPR. Although this right is discussed in the Statement of Compatibility with Human Rights section of the EM (at paragraphs 75 – 80), the EM does not acknowledge that individuals may not have any remedy in respect of offshore activities conducted pursuant to, or resulting from, an IPO. The EM treats these offshore activities as separate and distinct from the operation IPO framework, which is precisely why there is an accountability issue with its design.

Recommendation 1

The Bill should include protections against the collection and use of data which has been obtained or used by private industry in contravention of Australian privacy principles.

Privacy Risk 2: Exponential increase in the scale of commercial exploitation of personal information

44. The IPO framework draws heavily on the data gathering capabilities of multinational companies such as Facebook and Google, together with the increasing use of those services by Australian consumers. The statutory thresholds for law enforcement access to these emerging capabilities cannot be assessed against a known impact on user privacy, because the evolution of technology outpaces the ability of regulators to assess and consider its privacy impact.

45. As the ACCC noted:

> *The ubiquity of digital platforms in the daily lives of consumers means that many are obliged to join or use these platforms and accept their non-negotiable terms of use in order to receive communications and remain involved in community life*.[30]

46. It is therefore misleading for the Minister for Home Affairs to state that:

> *The Minister for Home Affairs Peter Dutton said the Bill was an important step towards standing up agreements with close partner countries such as the United States for faster authorised access to electronic information.*

---

[28] See *Comments of the Electronic Privacy Information Centre on the Office of the High Commissioner for Human Rights call for inputs to a report on "the right to privacy in the digital age"* April 6, 2018, pages 7 and 8, available at https://epic.org/privacy/intl/Comments-OHCHR-Digital-Age.pdf

[29] See s. 105(5) of the TIA Act.

[30] ACCC Digital Platforms Inquiry, Final Report, page 22

> *"The global connectivity of the internet means evidence once stored in Australia and available under a domestic warrant is now distributed over many different services, in different countries," Mr Dutton said.* [31]

47. The statement misleads because it suggests the issue is simply one of data distribution and speed of access, rather than the changing nature of the material that is being stored (for example, the way that a company such as Google builds data profiles about their customers). The volume and of personal data collected and held offshore, as well as the opportunities to interrogate and leverage such data for commercial purposes, are expected to increase. As an example, the Digital Platforms Inquiry advised that:

> *Despite consumers being particularly concerned by location tracking, online tracking for targeted advertising purposes, and third-party data-sharing, these data practices are generally permitted under digital platforms' privacy policies.*[32]

Example – use of fingerprint data

48. The potential privacy impacts of the Bill can be illustrated with fingerprint records. There is increasing use of fingerprint recognition technologies in everyday transactions – from opening doors to opening mobile telephones. This is an emerging technology, and its use and regulation should be subject to careful assessment and informed public discussion. If the Government intended to collect, or allow the collection of, a large database of individuals' fingerprint data, the Australian public would expect that database to be subject to close Australian regulation and oversight – for both privacy and security reasons.

49. The way the IPO framework interacts with fingerprint data arises from the definition of 'stored communication' in Schedule 1 of the Bill. It has been significantly expanded from the definition of that term in the TIA Act, and relevantly includes two new limbs:

> *(f) material that:*
>
> *(i) has been uploaded by an end-user for storage or back-up by a storage/back-up service provided by a storage/back-up service provider; and*
>
> *(ii) is held on equipment that is operated by, and is in the possession of, the storage/back-up service provider.*
>
> *(g) material that:*
>
> *(i) is accessible to, or deliverable to, one or more of the end-users using a general electronic content service provided by a general electronic content service provider; and*
>
> *(ii) is held on equipment that is operated by, and is in the possession of, the general electronic content service provider.*

50. The term "uploaded" is defined in Clause 10 of the Schedule, to mean:

---

[31] See MHA website at: https://minister.homeaffairs.gov.au/peterdutton/Pages/international-crime-cooperation.aspx. The statement is repeated at paragraph 3 of the EM.
[32] ACCC Digital Platforms Inquiry, Final Report, para 7.2

10 Uploaded material

For the purposes of this Schedule, if:

(a) a person uses a device; and

(b) the device has software that automatically uploads material for storage or back-up by a storage/back-up service; and

(c) as a result, material is automatically uploaded for storage or back-up by the storage/back-up service;

the person is taken have to uploaded the material for storage or back-up by the storage/back-up service.

51. Most of the processes within modern communications devices are automatic. These features operate without a person's knowledge or conscious choice after they consent to the terms of a user agreement.[33] And if a user consents to it, the extent to which software may be programmed to automatically accumulate user data and send it offshore is entirely outside of the Government's control.

52. As noted by the ACCC, even where users opt out of automatic surveillance features such as location tracking, their location information may still be stored.[34]

53. The ACCC's view is that few consumers are fully informed of, fully understand, or effectively control, the scope of data collected and the bargain they are entering into with digital platforms when they sign up for, or use, their services.[35] As observed by the ACCC in the Digital Platforms Inquiry report:

> *The collection of user data by both major digital platforms (and other digital platforms) also extends far beyond the collection of data provided or observed via a user's interaction with the owned and operated apps and services. Data collected from the user's interaction with vast numbers of other websites and apps is combined with the data from the owned and operated platforms, and, in Google's case, with data collected from a user's device, where the device uses the Android mobile operating system.[36]*
>
> *….*
>
> *The ACCC considers that Australian consumers are better off when they are both sufficiently informed about the collection and use of their data and have sufficient control over their data. Transparency over the collection and use of data is important so that consumers have the opportunity to understand what data they are providing to others and how it is being used.*
>
> *However, this transparency is not enough. Consumers, once they understand what is being collected and how it is used, must be able to exercise real choice and meaningful control.[37]*

[33] See Chapter 7 of the ACCC's Digital Platforms Inquiry Final Report for a discussion of concerns about these agreements. Notwithstanding concerns raised in that report, it seems certain that automatic monitoring of users' activities is going to be an ongoing feature of modern electronic devices.
[34] Digital Platforms Inquiry, Final Report, Box 7.16
[35] ACCC Digital Platforms Inquiry, Final Report, June 2019, page 2
[36] Digital Platforms Inquiry, Final Report, page 7
[37] Ibid, page 22.

54. Due to the breadth of the revised definition of 'stored communication', the data captured by a fingerprint reader and sent over the internet offshore would fall within its scope, even though such information is not traditionally regarded as a 'communication' or a 'message'. The IPO framework will provide a means to acquire fingerprints from an offshore database held by a private company (e.g. a US-based technology company). This weakens privacy protections for fingerprint acquisition elsewhere in Australian law – for example, the requirements set out in Part IAA of the *Crimes Act 1914* (Cth).

55. While enforcement agencies should have powers to detect and uncover domestic criminal activity, providing those agencies access to data holdings which exploit users' ignorance about the use of their personal information will not encourage effective consumer protections or privacy rights.

56. The current design of the IPO framework gives significant autonomy to the private companies that control the user data. This design feeds, rather than fetters, this increase in the commercialisation of private data, and does so in ways that extend beyond Australia's effective control. To the extent this concern signals a need for government action, it is entirely consistent with that of the ACCC Digital Platforms Inquiry, which concluded:

> *The benefits that digital platforms have brought to consumers and businesses have not come without costs and consequences. It is these costs and consequences that governments must now grapple with, both in Australia and in other countries.*[38]

57. The original primary purpose of telecommunications legislation was the protection of privacy, with narrowly cast exceptions.[39] Given advancements in technology and social acceptance of technology with surveillance applications, government regulation is the only method through which this protection can be achieved. As Sharon Rodrick explained in 2009:

> *Notwithstanding the pervasive threat of terrorism and the increased sophistication in criminal techniques, it is argued that the Australian Government has a responsibility to continue to protect the privacy of its citizens' communications. Indeed, the escalation in the volume and form of telecommunications information, coupled with the unremitting development of intrusive and sophisticated electronic surveillance devices and techniques, makes it not only imperative that privacy concerns continue to be accommodated in legislative regimes that facilitate access to telecommunications for national security and law enforcement purposes, but that they are restored to a place of primacy. Since there are 'no longer any technical barriers to the kind of Big Brother surveillance society envisioned by George Orwell', the* only *barriers that remain are 'political and legal'.* [40]

Recommendation 2

The passage of the Bill should be contingent on the amendments to the Privacy Act which were announced in March 2019, together with the Government's formalisation of the agreed code for social media and online platforms which trade in personal information online.

[38] ACCC Digital Platforms Inquiry, Final Report, page 3
[39] The *Telephonic Communications (Interception) Act 1960* (Cth) made telephone interception an offence, with narrow exceptions in which interception could lawfully occur for national security purposes.
[40] Rodrick, Sharon --- "*Accessing Telecommunications Data for National Security and Law Enforcement Purposes*" [2009] FedLawRw 15; (2009) 37(3) Federal Law Review 375

The Bill should not be passed unless and until the privacy gaps in current law (being those referred to by the Attorney-General and the Minister for Communication and the Arts in March 2019) have been rectified.

Privacy Risk 3: Obscurity

58. A consistent theme that has emerged in discussion of TIA Act reform is the complexity of the legislation and the obscurity of its language. Unless Australians can understand the operation of the TIA Act and its implications for their privacy, their rights cannot be protected.

59. This risk was identified in a Privacy Impact Assessment conducted at the request of AGD in 2012.[41] The report noted:

> *3.1.3 TIA Act structural and drafting issues*
>
> *It is well recognised that TIA Act is lengthy, opaque, overly complex and confusing in application. In its discussions with AGD and stakeholders IIS was advised that the changing environment and complexity of drafting makes it increasingly difficult to know if and when the TIA Act may be used.*
>
> *The simplifying and streamlining aims of the reform process align with the Government's broader interest in improving the clarity of Commonwealth legislation. This 'Clearer Laws agenda' forms part of the Government's Strategic Framework for Access to Justice, which was announced by the Attorney-General on 17 May 2010.*[42]

60. The PJCIS reached a similar conclusion in 2013. The *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation* stated:

> *2.167 The Committee received extensive evidence from interception agencies, privacy advocates and legal practitioners about the complexity of the TIA Act. Indeed, the Committee's consideration of the statutory framework supports the conclusion that it is so complex as to be opaque in a number of areas. That this is the case in legislation which strives to protect the privacy of communications and enabling legitimate investigative activities is of concern*.[43]

61. The Report recommended, *inter alia*, that the TIA Act:

> *..be comprehensively revised with the objective of designing an interception regime which is underpinned by the following: clear protection for the privacy of communications; provisions which are technology neutral; maintenance of investigative capabilities, supported by provisions for appropriate use of intercepted information for lawful purposes; clearly*

---

[41] Information Integrity Solutions, Preliminary Report *Telecommunications (Interception and Access) Act 1979* Reform, 2011, available at: https://www.ag.gov.au/RightsAndProtections/FOI/Documents/Privacy%20Impact%20Assessment%20Preliminary%20Report%20Telecommunications%20(Interception%20and%20Access)%20ACT%201979%20Reform.doc

[42] The Attorney-General's speech, and references to the strategic framework are available at http://www.ema.gov.au/www/ministers/mcclelland.nsf/Page/Speeches_2010_17May2010-SpeechattheLaunchofNationalLawWeek-ImprovingAccesstoJustice

[43] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013 paragraph 2.167

articulated and enforceable industry obligations; and robust oversight and accountability which supports administrative efficiency.

62. The Committee also noted that the legislation could be significantly improved by "*providing clear direction on the protections afforded to telecommunications users, and the scope of the powers provided to agencies able to undertake telecommunications interception and access to stored communications and telecommunications data.*"[44]

63. The TIA Act reform recommendations made in the PJCIS 2013 inquiry were revisited in 2015 in the PJCIS *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*. Recommendation 1 was that:

The Committee recommends that the Government provide a response to the outstanding recommendations from the Committee's 2013 Report of the Inquiry into Potential Reforms of Australia's National Security Legislation by 1 July 2015.

64. The Government committed to writing to the Committee outlining its approach to TIA reform by 1 July 2015.[45] It is unclear if that response was provided, as it is not on the Committee's inquiry homepage.

65. These important objectives will not be met under the CLOUD Act and the IPO framework, as the expanded powers are deliberately open-ended – for example in the range of individuals and companies[46] that could be subject to an IPO, and the nature of the data that would be able to be acquired.[47]

66. Under the IPO framework, interception and data acquisition powers would no longer be defined by the capabilities of Australia's agencies and telecommunications carriers but would be defined by the future capabilities of multinational companies operating under foreign law - unknown and inaccessible to most Australians. This adds significant obscurity to an already complex and difficult area of law.

Recommendation 3

The Committee should examine the Government's response to Recommendation 1 of the *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* to ensure that those reforms are being progressed, so that the IPO framework does not exacerbate systemic weaknesses in the outdated regime.

[44] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Canberra, May 2013 paragraph 2.170
[45] Government response to Recommendation 1, available at the Inquiry homepage https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention
[46] See the definition of 'designated communications provider' discussed at para 59(k) of the EM.
[47] See the expanded definition of 'stored communication' in Clause 2 of Schedule 1

Specific Recommendations on the Bill

Title of the TIA Act

67. Item 14 of the Bill proposes changing the long title of the TIA Act by substituting the word 'other' for 'related' in the phrase '*and for related purposes*'. While necessary, this change does not go far enough. The TIA Act is no longer concerned with prohibiting interception, or permitting access to telecommunications *content*,[48] but is mainly concerned with obtaining *data* that is exchanged over the internet, consciously or automatically, by end users.

68. The purpose and scope of the TIA Act should be clear from its title.

Recommendation 4

The short title of the *Telecommunications (Interception and Access) Act 1979* should be changed to the *Telecommunications and Internet Data Interception Act 2020*.

The long title of the *Telecommunications (Interception and Access) Act 1979* should be changed from:

An Act to prohibit the interception of, and other access to, telecommunications except where authorised in special circumstances or for the purpose of tracing the location of callers in emergencies, and for related purposes.

To:

An Act to regulate law enforcement and national security interception of telecommunications and internet data, to regulate telecommunications industry assistance with such interception, and for related purposes.

Purpose of the TIA Act

69. In 2013, the PJCIS recommended that the TIA Act include an objects clause that specifically referred to the protection of the privacy of communications.[49] This recommendation has not been adopted notwithstanding several subsequent amendments to the TIA Act – indicating a shift in Government focus and attention to that of data acquisition, rather than privacy protection.

70. The Minister for Home Affairs has responsibility for the TIA Act, and accordingly also has responsibility for the privacy objectives of the TIA Act. According to the Home Affairs website:

> *The TIA Act protects the privacy of Australians by prohibiting interception of communications and access to stored communications. The privacy of Australians is also protected by*

[48] This is a feature of many recent Parliamentary submissions calling for increased access to telecommunications data – that agencies' ability to reliably obtain the content of communications under a warrant issued under the TIA Act is diminishing.

[49] Parliamentary Joint Committee on Intelligence and Security, *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, Recommendation 1

the Telecommunications Act 1997, which prohibits telecommunications service providers from disclosing information about their customers' use of telecommunications services. [50]

71. The Minister for Communication and the Arts administers the *Telecommunications Act 1997*.

72. This structure is inadequate to protect the rights of Australian telecommunication users. Dividing privacy responsibility across two different pieces of legislation undermines the effective consideration of privacy. This is further evidenced by the fact that some privacy responsibilities are carved out and given to the Australian Information Commissioner. [51] It is entirely unclear who speaks for privacy.

73. Further uncertainty is created by the regulation of two different types of information – personal information and electronic communications - for different purposes and to different standards.[52]

74. This division of responsibilities is not only a privacy and security risk, these regulatory gaps empower multinational corporations who are able to monetise their trade in Australians' personal data.[53]

75. The Minister for Home Affairs cannot simultaneously protect the privacy of Australians and promote extensions of surveillance powers which encroach upon those rights. This is a classic example of the fox guarding the henhouse.

76. The TIA Act's primary objective is not (or is no longer[54]) to prohibit the interception of telecommunications and to promote privacy. To the extent it still serves this function (e.g. through the interception offence at s. 7), its operation is now confusing and unwieldy. Case law involving this protection indicates that this area of law is poorly understood and badly in need of reform, particularly in the digital age.[55]

77. These issues would be addressed, and the privacy purposes served by this prohibition would operate more clearly and distinctly if they were relocated into privacy-based legislation, which clearly articulated societal expectations about the handling of telecommunications data outside a warrant-based interception framework.

78. That Act should be the responsibility of one Minister, who should not also have responsibility for Australia's national security and law enforcement agencies or outcomes.

Recommendation 5

The objectives of the TIA Act should no longer include a prohibition of telecommunications interception and privacy protection. It should only regulate interception and access. The

[50] https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/telecommunications-interception-and-surveillance
[51] E.g. s. 180(5) of the TIA Act. See further information at the Information Commissioner's website https://www.oaic.gov.au/privacy/other-legislation/telecommunications/
[52] See Australian Law Reform Commission Report *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108) available at https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/73-other-telecommunications-privacy-issues/collection/ at 71.32
[53] ACCC Digital Platforms Inquiry, Chapter 2.
[54] For a history of the TIA Act's functions, see Rodrick, Sharon --- "*Accessing Telecommunications Data for National Security and Law Enforcement Purposes*" [2009] FedLawRw 15; (2009) 37(3) Federal Law Review 375
[55] E.g. see *Rayney and Legal Practice Board of Western Australia* [2016] WASAT 7 (10 February 2016)

privacy objectives should instead be dealt with in separate privacy-based legislation administered outside of the Home Affairs portfolio.

Expanded definition of "stored communication"

79. The term 'stored communication' is defined in both the TIA Act and the Bill. The definition in the Bill (i.e. the definition used in the IPO framework) is significantly broader:

TIA Act s.5 definition:

stored communication *means a communication that:*

(a) is not passing over a telecommunications system; and

(b) is held on equipment that is operated by, and is in the possession of, a carrier; and

(c) cannot be accessed on that equipment, by a person who is not a party to the communication, without the assistance of an employee of the carrier.

Bill clause 2 definition:

stored communication *means:*

(a) a communication that:
- *(i) has been carried by a carriage service; and*
- *(ii) is not being carried by a carriage service; and*
- *(iii) is held on equipment that is operated by, and is in the possession of, the carriage service provider who supplied the carriage service; or*

(b) a communication that:
- *(i) has been carried by a carriage service; and*
- *(ii) is not being carried by a carriage service; and*
- *(iii) is held on equipment that is operated by, and is in the possession of, the carrier who owns or operates a telecommunications network used to supply the carriage service; or*

(c) a message that:
- *(i) has been sent or received using a message/call application service provided by a message/call application service provider; and*
- *(ii) is held on equipment that is operated by, and is in the possession of, the message/call application service provider; or*

(d) a recording of a voice call that:
- *(i) has been made or received using a message/call application service provided by a message/call application service provider; and*
- *(ii) is held on equipment that is operated by, and is in the possession of, the message/call application service provider; or*

(e) a recording of a video call that:
- *(i) has been made or received using a message/call application service provided by a message/call application service provider; and*
- *(ii) is held on equipment that is operated by, and is in the possession of, the message/call application service provider; or*

(f) material that:
- *(i) has been uploaded by an end-user for storage or back-up by a storage/back-up service provided by a storage/back-up service provider; and*
- *(ii) is held on equipment that is operated by, and is in the possession of, the storage/back-up service provider; or*

(g) material that:

(i) is accessible to, or deliverable to, one or more of the end-users using a general electronic content service provided by a general electronic content service provider; and

(ii) is held on equipment that is operated by, and is in the possession of, the general electronic content service provider.

80. The term 'uploaded' is defined in Clause 10 of the Bill to include material that is automatically uploaded by software. Paragraph 91 of the EM does not refer to the fact that the new definition of 'stored communication' will capture data that is automatically uploaded by software, rather than consciously sent by an end-user.

81. The revised definition of 'stored communication' includes 'material' that would not fit the natural meaning of the term 'communication' as it applies to a human interaction, or even the definition of 'communication' in s.5 of the TIA Act, which is linked to the concepts of 'conversation' and 'message':

communication includes conversation and a message, and any part of a conversation or message, whether:

(a) in the form of:
  (i) speech, music or other sounds;
  (ii) data;
  (iii) text;
  (iv) visual images, whether or not animated; or
  (v) signals; or
(b) in any other form or in any combination of forms.

82. The EM does not explain the significance of the change in this definition. Paragraph 59(nn) misleadingly states that the term has a meaning 'similar to *stored communications* as defined in subsection 5(1) of the TIA Act'. Moreover, the examples provided in the EM at paragraphs 134 and 145-148 are conventional communications that are consciously sent by a person to another person or location. The examples do not reveal the extent of these new powers.

83. The net result is that despite using similar terminology, the Bill will significantly expand the scope of data that can be acquired - for example all of the information that a mobile phone learns of its user's activities and automatically backs up.

84. It is unclear whether the Bill would also capture data automatically uploaded by devices in the person's possession – such as their car or a networked infrastructure device such as Google Home™. Similarly, it is not clear if it would extend to other interactions a person has with their environment – such as fingerprint swipe access to an office building. The term 'end-user' is undefined in the Bill, further adding to this uncertainty.

85. When compared with the surveillance powers under the Commonwealth surveillance devices regime, the intrusive nature of these powers and their comparative lack of regulation and accountability protections is immediately apparent. Section 49 of the *Surveillance Devices Act 2004* outlines the reporting requirements for each warrant issued to, and authorisation given by, an agency. This section states the chief officer must, as soon as practicable after a warrant ceases to be in force, provide the Minister with a report, a copy of the warrant and other specified documents. Where a warrant or authorisation is executed, the agency is required to provide additional details in the report to the Minister.

86. The details that must be reported on indicate how seriously the privacy implications are viewed:

> *(2) In the case of a surveillance device warrant, or an authorisation referred to in paragraph (1)(b) or (c), the report must:*
>
> *(a) state whether the warrant or authorisation was executed; and*
>
> *(b) if so:*
>
> *(i) state the name of the person primarily responsible for the execution of the warrant or authorisation; and*
>
> *(ii) state the name of each person involved in the installation, maintenance or retrieval of the surveillance device; and*
>
> *(iii) state the kind of surveillance device used; and*
>
> *(iv) state the period during which the device was used; and*
>
> *(v) state the name, if known, of any person whose conversations or activities were overheard, recorded, monitored, listened to or observed by the use of the device; and*
>
> *(vi) state the name, if known, of any person whose location was determined by the use of a tracking device; and*
>
> *(vii) give details of any premises on which the device was installed or any place at which the device was used; and*
>
> *(viii) give details of any object in or on which the device was installed and any premises where the object was located when the device was installed; and*
>
> *…..*

87. Notwithstanding the proposed expanded scope of the power to access stored communications under the Bill, the threshold for obtaining stored communications remains a 3 year offence (a 'serious category 1 offence').[56] Given the expansion of the power, this penalty threshold is now too low.

88. The simplest and most appropriate solution is not to expand the scope of the existing 'stored communications' definition, until such time as the identified privacy and accountability concerns with the proposal have been addressed.

Recommendation 6

The definition of 'stored communication' in the Bill should be the same as that used in the *Telecommunications (Interception and Access) Act 1979.*

89. If this recommendation is not adopted, the EM should be re-written so that it is clear what types of data a stored communications IPO is able to capture, how this data differs from telecommunications data and intercepted content, and why this expanded capture of data is justified.

[56] EM at paragraph 149.

Scope of stored communications IPO

90. Although there are merits in relying on the existing TIA Act framework, including thresholds for issue, there are also dangers that they are not fit for purpose in the IPO context. Previous PJCIS inquiries concerning the TIA Act have included detailed consideration of concerns raised about those thresholds. Those reports reveal significant concern about the lack of concrete factors that determine whether an application should be granted (in other words, that they are merely a box ticking exercise).

91. These concerns are pertinent when considered against the application process for a stored communications IPO, in Division 3 of Part 2 of the Bill. Under that application process, the applicant must satisfy the issuing authority that:

    a. there are reasonable grounds for suspecting that the designated communications provider holds any of the types of stored communications contained in the definition, and
    b. that information that would be likely to be obtained by making a copy of the stored communications would be likely to assist in connection with the investigation of a serious category 1 offence, or serious category 1 offences, in which the relevant person is involved.

92. The issuing authority must have regard to matters including:

    a. how much the privacy of any person or persons would be likely to be interfered with,
    b. the gravity of the conduct constituting the offence, and
    c. how much the information would be likely to assist in connection with the investigation

93. The applicant is not required to specify the stored communications sought under the IPO. If the designated communications provider is a large provider (e.g. Google or Apple) there is a wide range of historic data that could be captured.[57] Although it may be expected that the scope of this data would be limited under the Bill, subclause 39(2)(e) states the IPO requires the designed communications provider to:

    (e) make a copy of any such stored communications

94. It is unclear how the issuing authority would be able to make an informed assessment of the issuing criteria (e.g. the degree of interference with a person's privacy) if the type and range of data are not specified in the application or in the IPO itself.

95. Given Division 3 does not otherwise mention the scope of the IPO, if the issuing authority had concerns about the scope of the order (e.g. because it may pick up privileged communications with a lawyer), it is unclear how the issuing authority could impose conditions restricting its scope.[58]

Recommendation 7

[57] It follows that the expression 'the stored communications' in paragraph 150 of the EM should be changed to 'any stored communications'.
[58] *cf* s. 17(1)(b)(xi) and 18(1) of the *Surveillance Devices Act 2004 (Cth)*

The applicant for a stored communications IPO under clause 39 of the Bill should be required to specify the stored communications sought under the order (e.g. by type and date range) and justify why obtaining that specific set of data would be likely to assist in the investigation of the serious offence.

Recommendation 8

An IPO for stored communications issued under clause 40 of the Bill should specify what stored communications are to be provided by the designed communications provider under the order (e.g. by type and date range).

Recommendation 9

An IPO for stored communications issued under clause 40 of the Bill should include the ability of the issuing authority to impose restrictions on the scope of the order.

Definition of serious category 1 offence

96. It is unclear why the word 'serious' appears in the term 'serious category 1 offence' in Clause 2 of the Bill. 'Serious offence' is separately defined in s. 5D of the TIA Act and is used to define offences that can be subject to interception powers. The use of the word 'serious' is unnecessary and confusing.

Recommendation 10

The term 'serious category 1 offence' should be replaced with the term 'category 1 offence' throughout the Bill.

Legality of foreign data acquisition

97. Through the IPO framework Australian agencies may acquire data, including personal information, which has been acquired or retained unlawfully by a private corporation in a foreign country.[59] If the data is transferred to Australia under an IPO, it could be used lawfully in Australian proceedings (a form of 'data laundering'). The proposed IPO framework contains no procedural protections to prevent this occurring. Unlike the MLAT process which involves foreign officials in its execution, under the IPO framework there is no basis for a foreign government to check whether the service provider's data holdings are compliant with their domestic law.

98. Concerns about the legality of Google's practices were noted in the ACCC report, which observed:

> *Google's location tracking practices and representations are currently facing class-action lawsuits for potential violation of the US State of California's privacy laws. They are*

[59] For a description of US legislative issues with the protection of consumer's data, including the Cambridge Analytics breach, see the *Comments of the Electronic Privacy Information Centre on the Office of the High Commissioner for Human Rights call for inputs to a report on "the right to privacy in the digital age"* April 6, 2018, pages 7 and 8, available at https://epic.org/privacy/intl/Comments-OHCHR-Digital-Age.pdf

reportedly under investigation by the US State of Arizona Attorney-General and are subject to complaints by the Norwegian Consumer Council and six other European consumer agencies relating to their compliance with the GDPR. The latter follows the release of the Norwegian Consumer Council's report 'Every step you take' in November 2018 relating to Google's tracking practices.

99. The Bill should not permit Australian Government agencies to take advantage of practices that are unlawful under Australian legal standards, or which would be prohibited if they were to occur in Australia or in the foreign jurisdiction. The Bill should ensure that unlawfully acquired or retained data cannot be obtained from a foreign jurisdiction under an IPO.

Recommendation 11

The matters to which an issuing authority must be satisfied of before issuing an IPO should include whether the data being sought was acquired or retained in accordance with the foreign country's domestic laws.

Definition of 'designated communications providers'

100. The term '*designated communications provider*' is defined broadly in Clause 2 of the Bill to include a range of entities that meet subsidiary definitions (for example, carriers and carriage service providers).

101. The word 'designated' in this defined term is misleading, as no designation of the communication providers actually occurs (*cf* the term '*designated international agreement*' and the process for Ministerial designation of agreements in Clause 3 and the Regulations). It suggests a degree of oversight and regulation that does not actually take place.

102. This issue is compounded by the breadth of activity described in the component terms like '*carrier*', which includes individuals as well as bodies corporate. The result is that a wide range of communications providers are captured. Contrary to the natural meaning of the term 'designated', the number and nature of those providers is unlimited.

103. The structure of the Bill and its lack of procedural protections expose Australians to significant risks of data misuse. The private entities and individuals who may collect Australians' personal data may do so unlawfully or unethically, and there is no protection against illegally acquired data being sought out and used by Australian agencies under an IPO. Describing such communication providers as 'designated' gives a misleading impression of propriety.

Recommendation 12

The word 'designated' should be removed from the term *designated communications provider* throughout Bill.

Recommendation 13

As a precondition for issuing an IPO, the Issuing Authority should be satisfied that the communications provider subject of the IPO has a lawful right of access to, or the retention of, the type of data sought under that foreign country's laws, including in respect of applicable privacy laws and protections.

Compliance with the designated international agreement

104. The Bill will establish an "Australian Designated Authority" to review each IPO's compliance with the terms of the nominated *designated international agreement*. This review happens after an IPO is issued, but before it is executed.[60] If the order is not compliant, is it cancelled. The Issuing Authority is not notified of this cancellation.

105. The Bill effectively inverts the conventional process for the issue of law enforcement warrant powers, which is that an agency's application is made against defined statutory criteria, and its satisfaction of those criteria is reviewed by an independent officer. The desirability of this design is evident from the following passages in the High Court's majority judgment in *Grollo v Palmer*:[61]

> *20. Yet it is precisely because of the intrusive and clandestine nature of interception warrants and the necessity to use them in today's continuing battle against serious crime that some impartial authority, accustomed to the dispassionate assessment of evidence and sensitive to the common law's protection of privacy and property (both real and personal), be authorised to control the official interception of communications. In other words, the professional experience and cast of mind of a Judge is a desirable guarantee that the appropriate balance will be kept between the law enforcement agencies on the one hand and criminal suspects or suspected sources of information about crime on the other. It is an eligible Judge's function of deciding independently of the applicant agency whether an interception warrant should issue that separates the eligible Judge from the executive function of law enforcement. It is the recognition of that independent role that preserves public confidence in the judiciary as an institution.*
>
> *21. In other countries the same view has been taken of the desirability, if not the necessity, for judicial issuing of a warrant to authorise secret surveillance of suspects in criminal cases. In such cases, the European Court of Human Rights said in* Klass v Federal Republic of Germany*:*
>
> *" The Court considers that, in a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge."*
>
> *In the United States, the Fourth Amendment protection "against unreasonable searches and seizures" has been held to require prior judicial warrant authorising electronic surveillance. In United States v United States District Court for the Eastern District of Michigan, the Court said:*
>
> *"The Fourth Amendment contemplates a prior judicial judgment, not the risk that executive discretion may be reasonably exercised."*
>
> (Footnotes omitted)

106. The EM contains no explanation for the compliance assessment occurring *after* the issue of an IPO, nor why is it performed by a government agency rather than by the independent issuing authority.

---

[60] Subclause 111(1)(b)
[61] *Grollo v Palmer* [1995] HCA 26

Recommendation 14

Every IPO application should be required to state that the order sought will comply with the terms of the relevant *designated international agreement* under which it will be executed. The Issuing Authority should be independently satisfied the IPO complies with the *designated international agreement* before the IPO is issued.

Control Order monitoring powers

107. As introduced, Control Orders did not contain any monitoring powers. They relied upon the deterrent effect of an offence provision[62] and compliance with conditions that involved interaction with law enforcement officers – such as reporting requirements.[63]

108. In 2015, AGD successfully argued that the addition of monitoring powers was necessary to ensure that Control Orders could achieve their purpose.[64] The new monitoring regime was said to allow monitoring to prevent breaches of control orders and to detect and prevent preparatory acts, planning and terrorist acts, as well as support and facilitation of terrorism or hostile activities in foreign countries.[65] The PJCIS accepted that argument, observing in respect of the TIA Act powers that:

> *3.134 The power to intercept communications is vital to ensuring compliance with certain conditions that may be imposed under a control order, such as restrictions or prohibitions on communicating or associating with specified individuals, accessing or using specified telecommunications or technology, and carrying out specified activities, can be effectively monitored.*

109. The TIA Act's Control Order monitoring powers are currently limited to an application for an interception warrant.[66] The TIA Act does not permit applications for stored communications or telecommunications data for Control Order monitoring purposes. This appears to be a deliberate choice, given the purpose of monitoring compliance with the terms of a Control Order is a prospective and preventative activity, not an investigative activity, and does not obviously require access to historic telecommunications records. [67] Plainly, a person cannot breach a Control Order through conduct that occurred before the Control Order came into force.

110. The Control Order monitoring powers are complemented by increasingly restrictive measures that courts have been willing to apply to subjects under s. 104.5 of the *Criminal Code* – including limiting the subject's internet communications and access to programs and devices. [68]

---

[62] *Criminal Code* s. 104.27
[63] Criminal Code s. 104.5
[64] *Counter-Terrorism Legislation Amendment Bill (No.1) 2015* - see PJCIS report on the Bill at https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/CT_Amendment_Bill_2015
[65] AGD submission to the PJCIS inquiry on the Counter-Terrorism Legislation Amendment Bill (No.1) 2015.
[66] See TIA Act and paragraph 221 of the EM.
[67] See the Explanatory Memorandum to the Counter-Terrorism Legislation Amendment Bill (No. 1) 2015 at paragraphs 189 and 551.
[68] See for example, controls 16 -20 of the Control Order imposed in *McCartney v Abdirahman-Khalif* [2019] FCA 2218 (22 November 2019) and compare this against the content of earlier Control Orders.

111. The Bill proposes extending Control Order monitoring powers beyond interception, to also permit the acquisition of stored communications and telecommunications data. The powers will enable the acquisition of data that came into existence before the Control Order came into force, because the terms of an IPO are not limited by date range.[69]

112. The risk of the person not complying with the Control Order is already effectively dealt with under the existing regime. The additional powers in the Bill seem unnecessary and are not accompanied by clear justification. It is important to recall that Control Orders are designed to be obtained in circumstances where a person has not committed a criminal offence.

113. The Committee should consider firstly, exactly what types of data the Government proposes to acquire under the new powers in the Bill, and secondly, consider whether the combined effect of all the proposed and existing restrictions is proportionate to the risk being guarded against.[70] It would be entirely appropriate to ask the Independent National Security Legislation Monitor to inquire into these proposals.

114. A relevant consideration is whether future Control Orders may not be issued by a court simply because the extent of intrusion into the subject's privacy available to authorities under monitoring powers outweighs the appropriateness of imposing the Order. Alternatively, the additional justification needed to persuade a court to impose a Control Order may dissuade an agency from applying for one in otherwise appropriate circumstances. Such outcomes would undermine the important protective function that Control Orders serve.

115. It would be appropriate to mirror the existing scope of the Control Order monitoring powers under the TIA Act until the Committee is satisfied that an expansion can be clearly justified (i.e. following a thorough inquiry and report). If such the expansion is justified, it should be referred to in an Explanatory Memorandum accompanying these proposals.

Recommendation 15

The powers in Part 3 of the Bill should be limited to only interception orders and should only permit the interception of communications which are made while a Control Order or a succeeding Control Order is in force.

[69] See clauses 69 and 79

[70] See the Law Council's submission to the Independent National Security Monitor's Report on Stop, search and seizure powers, declared areas, control orders, preventive detention orders and continuing detention orders, dated 12 May 2017, available at https://www.lawcouncil.asn.au/tags/submissions